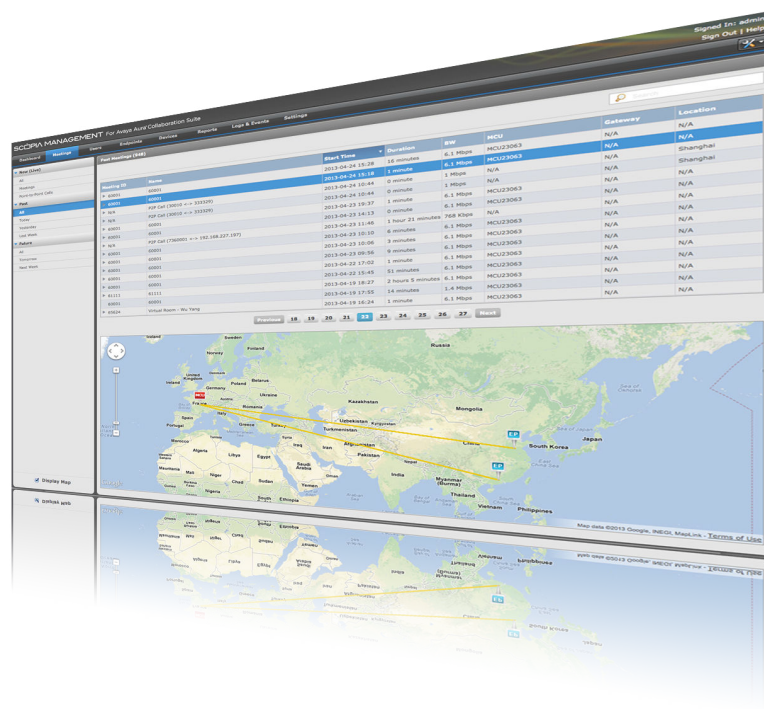




Administrator Guide for Avaya Scopia® Management for Aura Collaboration Suite



Version 8.3
For Solution 8.3
July 2014

© 2000-2014 Avaya Inc. All intellectual property rights in this publication are owned by Avaya Inc. and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. Avaya Inc. retains all rights not expressly granted.

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

This publication is AVAYA Confidential & Proprietary. Use pursuant to your signed agreement or Avaya policy. No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by Avaya Inc.

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

Avaya Inc. reserves the right to revise this publication and make changes without obligation to notify any

person of such revisions or changes. Avaya Inc may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

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

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

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

Administrator Guide for Avaya Scopia® Management for Aura Collaboration Suite Version 8.3, July 17, 2014

<http://support.avaya.com>

Table of Contents

Chapter 1: Getting Started with the Avaya Scopia® Management

About Avaya Scopia® Management for Aura Collaboration Suite	8
Planning your Avaya Scopia® Management Deployment	11
Implementing Port Security for Avaya Scopia® Management	11
Ports to Open on Avaya Scopia® Management	12
Minimum Requirements for Scopia® Management	16
Planning the Topology of the Avaya Scopia® Management	21
Planning Licenses for Integration with Aura Collaboration Suite	22
Deploying Scopia® User and Endpoint Licenses in Scopia® Management	25
Planning User Access to Videoconferences	26
Installing the Scopia® Plug-in for Microsoft Exchange	28
Localized Languages in Scopia® Management	32
Accessing Avaya Scopia® Management	32
Accessing the Administrator Portal to Manage your Video Network	33
Accessing the User Portal to Manage your Videoconferences	34
Enabling Single Sign-on for Scopia® Management	35
Enabling Single Sign-on for Scopia® Add-in for Microsoft Outlook	36
Initial Configuration Workflow	36
Initial Workflow for your Organization	37

Chapter 2: Defining Locations in your Deployment

Adding or Modifying a Location	38
Defining Bandwidth Limits for a Location	39

Chapter 3: Defining your Video Network Devices

Device Configuration Workflow	42
Adding Video Network Devices in Scopia® Management	44
Planning and Configuring Gatekeepers in Scopia® Management	47
About the Scopia® Management's Internal Gatekeeper	48
Defining the Gatekeeper's Dial Plan in Avaya Scopia® Management	49
Defining Scopia® Management as the Gatekeeper's Authorization Server	51

Adding a Lync Server, an OCS or a SIP Server in Scopia® Management	53
Planning and Configuring MCUs in Scopia® Management	57
Configuring the MCU from Scopia® Management	58
Modifying an MCU's Location or Organization	61
Downloading MCU Meeting Types to Scopia® Management	62
Synchronizing MCU Meeting Types with Scopia® Management	63
Defining a Default and Fallback Meeting Type	65
Modifying an MCU Meeting Type in Scopia® Management	66
Searching for a Meeting Type	68
Deleting a Meeting Type from Scopia® Management	69
Increasing MCU Capacity by Cascading Multiple MCUs	69
Enabling Auto-Attendant Support	72
Integrating the Avaya Aura Conferencing Server	75
Planning and Configuring a Scopia® Desktop server in Scopia® Management	76
Adding and Modifying Scopia® Desktop server in Avaya Scopia® Management	76
Planning and Configuring Gateways in Scopia® Management	78
Configuring the Avaya Scopia® TIP Gateway or Scopia® Video Gateway in Scopia® Management	79
Configuring a Scopia® Gateway in Scopia® Management	82
Registering a Gateway with a Gatekeeper	86
Remotely Configuring Avaya Scopia® PathFinder server	87
Planning and Configuring Endpoints in Scopia® Management	89
Importing H.323 Endpoints from the Gatekeeper	91
Importing H.323 Endpoints from an External LDAP Server	94
Importing Endpoints from the H.350 Search Base	97
Adding Endpoints in Scopia® Management Manually	99
Adding H.323 IP Endpoints	100
Adding SIP IP Endpoints	102
Adding Telepresence Systems in Scopia® Management	104
Adding ISDN/PSTN H.320 Endpoints	109
Adding Mobile Endpoints	110
Planning and Configuring Telepresence in Scopia® Management	111
Understanding Telepresence Systems	112
Hosting Telepresence Meetings	113
Calculating Resources for Telepresence	113
Scheduling Telepresence Systems	113
Managing Endpoints using Scopia® Management	113
Replicating Endpoint Settings on Multiple Endpoints	115
Using Scopia® Management's Endpoint Directory as a Corporate Address Book	118
Configuring Corporate Address Books	119

Configuring Endpoints to be Displayed in the Corporate Address Book	120
Managing your Endpoint's User Directory with LDAP	120
Configuring Endpoints to use an LDAP Directory	121
Configuring Third-Party Endpoints to use Scopia® Management as LDAP Directory	124
Configuring Presentation Layouts for Single-Screen Endpoints	127
Organizing Endpoints into Groups with Labels	129

Chapter 4: Securing your Video Network

Securing Web Access to Scopia® Management Using HTTPS	133
Installing Certificates with Unique Keys on the Tomcat Web Server	134
Configuring the Tomcat Web Server to Use HTTPS	136
Connecting Scopia® Management to WebLM Securely with HTTPS	137
Securing the Connection between Scopia® Management and an LDAP Server	139
Securing Your Video Network Using TLS	139
Planning the Required Certificates for TLS	142
Creating and Uploading Scopia® Management's Certificate for Videoconferencing Components .	148
Creating and Uploading the Scopia® Management's Certificate for Scopia® Desktop server	153
Uploading Root and Intermediate Certificates for Scopia® Video Gateway, Avaya Scopia® TIP Gateway or Other Devices	155
Enabling the TLS Connection in Scopia® Management	158

Chapter 5: Defining and Managing Video Users

Managing User Profiles	161
Creating or Modifying a User Profile	162
Defining Scopia® Desktop Bandwidth for a User Profile	164
Customizing a User Profile	165
Deleting a User Profile	167
Managing User Groups	168
Creating a User Group	169
Modifying a User Group	169
Removing a User Group	170
Managing Video Users	171
Managing Users from the LDAP Server	171
Connecting Scopia® Management with the LDAP Server	172
Scopia® Management LDAP Information Attributes	174
Downloading Users from the LDAP Server	175
Synchronizing Users from the LDAP Server	177

Managing Users with a Local User Directory	178
Creating a User within Scopia® Management	178
Removing a User	180
Modifying a User	181
Assigning Groups to Multiple Users	182
Searching for a User	183
Managing Virtual Rooms	184
Downloading Virtual Rooms from the LDAP Server	184
Creating or Modifying a Virtual Room for a Scopia® Management User	187
Creating an Invitation Template	189

Chapter 6: Scheduling Your Videoconference from the Scopia® Management User Portal

Configuring Advanced Meeting Properties in the User Portal	199
--	-----

Chapter 7: Real-time Monitoring

Managing Alarm Notifications	205
Configuring the Log Level	206
Sending Trap Messages	206
Forwarding Traps to a Third-party Trap Server	207
Removing Trap Forwarding to a Third-party Trap Server	207
Sending Email Alerts	208
Creating or Modifying an Alert Recipient Profile	208
Removing an Alert Recipient Profile	209
Monitoring Network Devices via Scopia® Management	210
About Management Status of Network Devices	211
Monitoring Network Events and Alarms	211
Changing the Severity Level of Alarms	213
Monitoring Meetings and Calls	213
Monitoring Ongoing Meetings or Calls	214
Monitoring Bandwidth and Port Utilization	216
Checking the Status of Meetings	217
Disconnecting Calls or Meetings	217
Downgrading the Meeting Bandwidth	218

Chapter 8: Maintaining your Videoconferencing Network

High Availability of Scopia® Management	221
Creating a Redundant Secondary Server for Scopia® Management	223
Creating an Off-Site Backup Server for Scopia® Management	228
Monitoring Redundancy Status	230
Manually Promoting the Off-Site Backup Server	233
Restoring Primary Server from Off-Site Backup Server	236
Disabling Redundancy	237
Upgrading, Backing up and Restoring Scopia® Management Data	239
Backing Up Scopia® Management Manually	239
Backing up Avaya Scopia® Management Automatically	240
Restoring a Scopia® Management Backup File	241
Upgrading Scopia® Management	243
Upgrading, Backing Up and Restoring Video Device Software	244
Editing Upgrade History of Video Devices	244
Upgrading the Software File of a Video Device	245
Removing a Software Upgrade File from a Video Device	248
Backing Up and Duplicating a Video Device Configuration	249
Updating License Keys of Avaya MCUs or Gateways	250
Restoring the Previous Software Version of a Network Device	250
Downgrading your Your Network Device	252
Daily Maintenance of your Video Network	252
Searching for a Video Device	252
Removing a Video Device from Scopia® Management	253
Preparing a Device for Maintenance	254
Managing Bandwidth in your Network	254
Defining Video Usage Defaults	254
Maintaining Scheduled Meetings	259
Searching for a Meeting	259
Modifying Upcoming Meetings	260
Retrieving the Customer Support Package	261
Uninstalling Avaya Scopia® Management	262

Chapter 9: Tracking System Usage with Reports

Generating a Report	266
---------------------------	-----

Chapter 1 | Getting Started with the Avaya Scopia® Management

This section provides an orientation for Scopia® Management, including its features, considerations for planning and implementing its deployment, and how to access Scopia® Management:

Navigation

- [About Avaya Scopia® Management for Aura Collaboration Suite](#) on page 8
- [Planning your Avaya Scopia® Management Deployment](#) on page 11
- [Localized Languages in Scopia® Management](#) on page 32
- [Accessing Avaya Scopia® Management](#) on page 32
- [Initial Configuration Workflow](#) on page 36

About Avaya Scopia® Management for Aura Collaboration Suite

Avaya Scopia® Management is an application to control your video network devices and schedule videoconferences.

The Aura Collaboration Suite enables any enterprise to gain full business collaboration utilizing audio, video or the web. The Aura Collaboration Suite is positioned for organizations which need robust collaboration capabilities, including industry leading HD video, plus audio and web conferencing.

The Scopia Solution is a component of the Aura Collaboration Suite. With this unified offering, every potential Avaya UC customer can access and utilize the Scopia® Solution premium collaboration experience.

Avaya UC customers can now enjoy the Scopia high-end video experience as one of their collaboration options within the Collaboration Suite.

The Scopia® Desktop and Scopia® Mobile Scopia® Users delivered with the Aura Collaboration Suite require Scopia Management for Aura Collaboration Suite.

The Aura Collaboration Suite is positioned for organizations which need robust collaboration capabilities, including industry leading HD video, plus audio and web conferencing. The Avaya Scopia® Management is specially tailored to fit this Unified Communications (UC) offering, along with other video infrastructure devices of the Scopia® Solution such as Scopia® Desktop for Aura Collaboration Suite and Scopia® Elite 6000 Series MCU. The Avaya Scopia® Management server software cannot be re-purposed for other video solutions which are not part of the Aura Collaboration Suite.

You can access Avaya Scopia® Management either from the administrator portal or the user portal ([Figure 1: Scopia® Management portals](#) on page 9). Administrators access the administrator portal to perform network-wide management. Meeting operators, organizers, and regular users access the user portal to perform scheduling and management relevant to them.

The system administrator defines different user profiles with varying permissions to determine the management tasks available for a specific user.

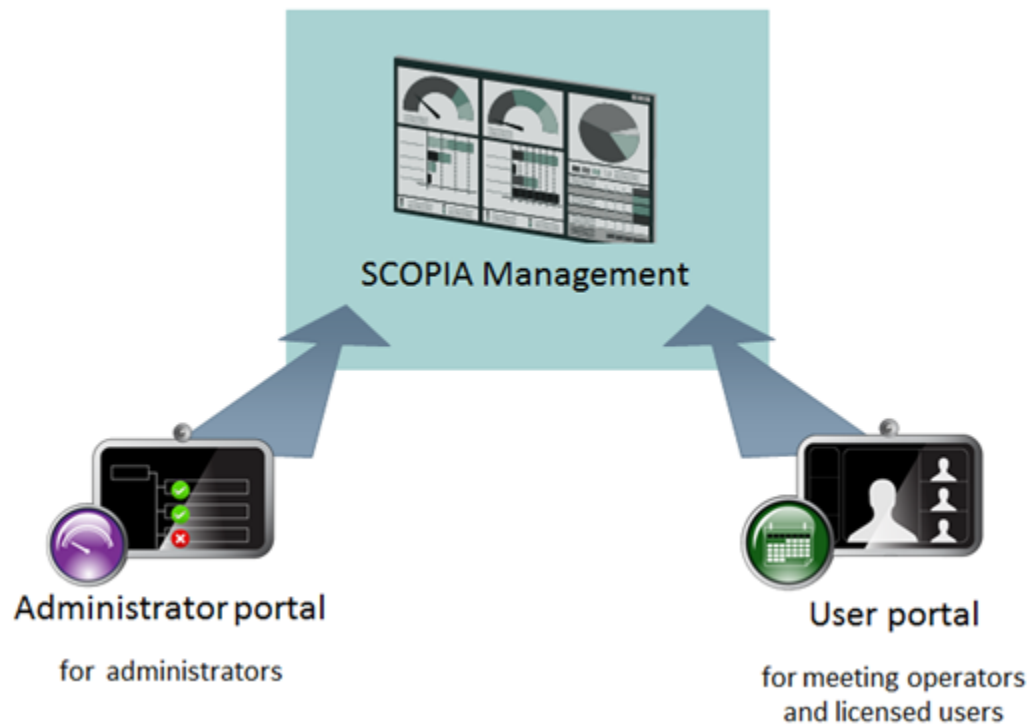


Figure 1: Scopia® Management portals

Scopia® Management sits at the core of your Scopia® Solution deployment and offers the following capabilities:

- Video network device management

Remotely configure, upgrade and monitor many of your video network devices via the administrator portal. These devices include Scopia® Elite MCU, Avaya Scopia® ECS Gatekeeper, and many gateways ([Figure 2: Managing all components of the Scopia® Solution](#) on page 10).

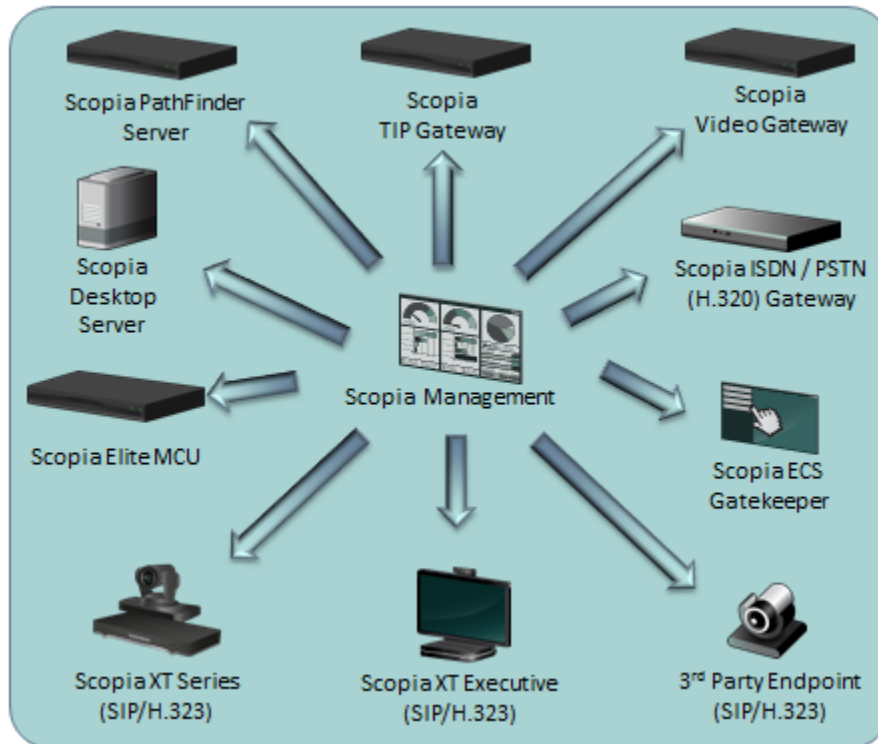


Figure 2: Managing all components of the Scopia® Solution

- Endpoint management

Remotely configure, upgrade and monitor both Scopia® Solution and third-party endpoints via the administrator portal.

Every dedicated endpoint requires a license to join a videoconference and to be defined and managed by Scopia® Management (see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22).

- Resources and bandwidth management

Configure your network devices and endpoints for effective bandwidth control. For example, you can determine when meetings are cascaded between multiple MCUs (for more information, see [Increasing MCU Capacity by Cascading Multiple MCUs](#) on page 69). You can also monitor in real-time from the administrator portal's dashboard, or generate reports to see network statistics for a given time period.

- User management

You can manage user access by creating profiles with a set of capabilities. You can also create virtual rooms and assign endpoints. Scopia® Management also integrates with existing directory servers such as Microsoft Active Directory, IBM Lotus Domino for easy user provisioning.

- Meeting management

Schedule, moderate, and reserve resources for your videoconferences via the user portal. Scopia® Management can also work with Microsoft Outlook or IBM Lotus Notes for an easy and intuitive calendar application scheduling.

Using one of the Scopia® Management plug-ins for Microsoft Outlook, you can easily schedule meetings with resources directly from Microsoft Outlook (2010 or later) or a calendar application on your mobile device (see [Planning User Access to Videoconferences](#) on page 26).

- Interface to unified communication solutions

Scopia® Management provides the interface to market leading unified communication solutions such as Avaya Aura Collaboration Suite, Microsoft Lync Server, Microsoft Office Communications Server, and IBM Lotus Sametime.

- SIP server integration

The smooth integration with third-party SIP servers leverages existing network call control for the videoconferencing system. The SIP server manages the call control and network usage, while the Scopia® Solution supplies the videoconferencing capabilities.

- Built-in gatekeeper

Scopia® Management is shipped with a built-in gatekeeper, Avaya Scopia® Gatekeeper, which supplies the correct destination IP and authorizes the appropriate bandwidth for the call. In this way, Scopia® Management can manage endpoint-initiated calls and point-to-point calls.

- Call authorization

Scopia® Management integrates with the gatekeeper to authorize calls based the settings you define for your network, such as user capabilities and allowed bandwidth.

Planning your Avaya Scopia® Management Deployment

When planning your Scopia® Management deployment, it is important to understand the minimum system requirements described in this section.

You can deploy Scopia® Management differently, depending on the needs of your organization. There are several solutions defined in the *Scopia® Solution Guide*, each with its own deployment scenario and network topology. Decide on the type of deployment you need based on your video requirements and your existing network topology.

The *Scopia® Solution Guide* details the considerations for choosing each of the deployments, and the locations to place each of the solution components within the network topology.

When planning your deployment, it is also important to consider port security (see [Implementing Port Security for Avaya Scopia® Management](#) on page 11) and whether to install redundant Scopia® Management servers for high availability ([High Availability of Scopia® Management](#) on page 221).

For installation procedures for each of the components of the Scopia® Solution, see the product's *Installation Guide*. For installation procedures for the Scopia® Management, see *Installation Guide for Avaya Scopia® Management*.

Navigation

- [Implementing Port Security for Avaya Scopia® Management](#) on page 11
- [Ports to Open on Avaya Scopia® Management](#) on page 12
- [Minimum Requirements for Scopia® Management](#) on page 16
- [Planning the Topology of the Avaya Scopia® Management](#) on page 21
- [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22
- [Planning User Access to Videoconferences](#) on page 26

Implementing Port Security for Avaya Scopia® Management

Avaya Scopia® Management is located in the enterprise (internal) network and is connected to the DMZ and public network via firewalls.

Avaya Scopia® Management can connect to H.323 endpoints in public and partner networks via Avaya Scopia® PathFinder, and to H.323 and SIP endpoints located in the enterprise network. For a list of TCP/IP/UDP ports supported by Avaya Scopia® Management, see [Ports to Open on Avaya Scopia® Management](#) on page 12.

For a list of TCP/IP/UDP ports supported by other Scopia® Solution products, see the *Port Security Reference Guide* or the product's *Installation Guide*.

Ports to Open on Avaya Scopia® Management

Avaya Scopia® Management is typically deployed in the enterprise network or the DMZ.

When opening ports to and from Scopia® Management, use the following as a reference:

- For ports both to and from Scopia® Management, see [Table 1: Bidirectional Ports to Open on Scopia® Management](#) on page 12.
- For outbound ports from Scopia® Management, see [Table 2: Outbound Ports to Open from Scopia® Management](#) on page 14.
- For inbound ports into Scopia® Management, see [Table 3: Inbound Ports to Open on Scopia® Management](#) on page 16.

! Important:

Choose the specific firewalls to open ports, depending on where your Avaya Scopia® Management and other Scopia® Solution products are deployed.

Table 1: Bidirectional Ports to Open on Scopia® Management

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
23	Telnet (TCP)	Sony PCS address book, MCM, Endpoints	Enables you to use Sony PCS address book, retrieve element logs, and control MCM and endpoints.	Cannot use Sony PCS address book feature or retrieve logs from various devices (such as MCM).	Recommended
80	HTTP (TCP)	Web client	In: Provides access to the Scopia® Management web user interface. When installed with the gatekeeper, this port defaults to 8080. Out: Provides access to the Scopia® Management web user interface, TANDBERG MXP management (XML API via HTTP) and Scopia® Elite MCU.	Cannot manage TANDBERG MXP and Scopia® Elite MCU from the Scopia® Management administrator portal.	Mandatory You can configure this port during installation (see <i>Installation Guide for Avaya Scopia® Management</i>).

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
161	SNMP (UDP)	Any managed element	Enables SNMP configuration	Cannot operate the SNMP service with devices, and forward trap events do not function.	Mandatory
162	SNMP (UDP)	Any third-party SNMP manager	Enables sending SNMP trap events from any managed element	Cannot operate the SNMP service with devices, and forward trap events do not function.	Recommended
389	LDAP (TCP)	LDAP servers	Enables connection to LDAP servers	Cannot work with LDAP Servers	Mandatory for LDAP authentication
3336	XML (TCP)	Scopia® Management/ Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU	Enables communication between Scopia® Management and the Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU via the moderator's XML API (used for managing meetings via Scopia® Management)	Scopia® Management cannot connect to the Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU via the XML API	Mandatory if deployed with Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU
3342	SOCKS (TCP)	Scopia® Management	Enables synchronization between multiple redundant Scopia® Management installations	Cannot operate redundancy	Mandatory in deployments with a redundant Scopia® Management server.
3346	XML (TLS)	Scopia® Management	Enable secure XML Connection to Scopia® Management	Cannot open secure XML connection to Scopia® Management	Mandatory for any XML secure clients
5060	SIP (TCP/ UDP)	B2B/ Other SIP components	Enables SIP signaling	Cannot connect SIP calls	Mandatory
5061	SIP (TLS)	B2B/ Other SIP components	Enables secure SIP signaling	No TLS connection available	Mandatory
5432	TCP	Scopia® Management	Enables master/slave data synchronization (used for Scopia® Management redundant deployments with an internal database)	Cannot synchronize data between the master and slave servers	Mandatory for redundancy deployments with an internal database

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
7800-7802	UDP	Scopia® Management	Enables data synchronization between redundant Scopia® Management servers	Redundancy functionality is not available	Mandatory for redundancy deployments
8011	HTTP (TCP)	Web client	Provides access to the internal ECS web user interface	Scopia® Management client cannot access internal ECS web user interface	Mandatory for accessing the ECS web user interface

Table 2: Outbound Ports to Open from Scopia® Management

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
7	Echo (TCP)	Video Network Devices	Detects online status of video network devices	Cannot detect online status of video network devices	Mandatory
21	FTP (TCP)	Scopia® Management	Enables downloading logs from ECS or other devices that allow logs to be downloaded via FTP. Enables importing and exporting TANDBERG Local Address Book. Enables software upgrade.	Cannot download logs from ECS or from other devices via FTP, import or export TANDBERG Local Address Book, or perform software upgrades.	Mandatory
22	SSH (TCP)	Scopia® Management	Detects LifeSize endpoints. Enables downloading Avaya Scopia® PathFinder server logs. Detects and manages Scopia® VC240.	Cannot detect LifeSize endpoints, download Avaya Scopia® PathFinder server logs, or detect/ manage Scopia® VC240	Mandatory
24	Telnet (TCP)	Polycom endpoints	Enables you to control Polycom endpoints	Cannot control Polycom endpoints	Optional
25	SMTP (TCP)	SMTP server	Enables connection to SMTP server for sending email notifications	Cannot send email notifications	Mandatory
53	DNS (UDP)	DNS server	Enables DNS queries	Cannot parse domain names	Mandatory
445	NTLM (TCP/UDP)	Active Directory Server	Enables connection to the Active Directory Server	NTLM SSO does not function	Mandatory
636	LDAP over SSL	Directory Server	Enables connection to the Directory Server	Cannot connect to the Directory Server	Mandatory
3089	TCP	Avaya Scopia® PathFinder	Detects endpoints via Avaya Scopia® PathFinder	Cannot detect endpoints via Avaya Scopia® PathFinder	Mandatory

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3338	XML (TCP)	MCU/ Scopia® Video Gateway / TIP Gateway /SIP Gateway	Enables connection to MCU/ Scopia® Video Gateway/ TIP Gateway/ SIP Gateway via the administrator's XML API (used for configuring devices via Scopia® Management)	Cannot perform configuration for MCU/ Scopia® Video Gateway/ TIP Gateway/ SIP Gateway via the XML API	Mandatory if deployed with MCU/ Scopia® Video Gateway/ TIP Gateway/ SIP Gateway
3339	XML (TCP)	B2B	Enables you to use the Scopia® Management XML API	Cannot communicate with the B2BUA component via Scopia® Management XML API	Mandatory
3340	TCP/TLS	Scopia® Desktop	Enables connection to Scopia® Desktop	Scopia® Desktop cannot use Scopia® Management to place or manage calls	Mandatory if deployed with Scopia® Desktop
3346	XML (TLS)	Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU	Enables secure connection to the Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU via the moderator's XML API (used for managing meetings via Scopia® Management)	Cannot securely connect to the Scopia® Video Gateway/ TIP Gateway/ SIP Gateway / MCU via the XML API	Mandatory for a secure XML API connection with Scopia® Video Gateway/ TIP Gateway/ SIP Gateway / MCU
3348	XML (TLS)	Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU	Enables secure connection to Scopia® Video Gateway/ TIP Gateway/ SIP Gateway/ MCU via the administrator's XML API (used for configuring devices via Scopia® Management)	Cannot securely connect to the Scopia® Video Gateway/ TIP Gateway/ SIP Gateway / MCU via the administrator's XML API	Mandatory for a secure XML API connection with Scopia® Video Gateway/ TIP Gateway/ SIP Gateway / MCU
8089	XML (TCP)	Avaya Scopia® PathFinder server	Enables connection to Avaya Scopia® PathFinder server (v7.0 and later) via Avaya Scopia® PathFinder server XML API	Cannot connect to Avaya Scopia® PathFinder server via Avaya Scopia® PathFinder server XML API	Optional
50000	Telnet (TCP)	Sony endpoints	Enables you to control Sony endpoints	Cannot control Sony endpoints	Optional

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
55003	TCP	XT Series	Enables connection to the XT Series	Cannot connect to the XT Series	Mandatory if deployed with XT Series
63148	DIOP (TCP)	Domino server	Enables connection with the Domino server	Cannot connect to the Domino Server	Mandatory if Scopia® Management works with Domino Server

Table 3: Inbound Ports to Open on Scopia® Management

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
443	HTTPS (TCP)	Web client	Enables Tomcat to run over SSL	Cannot access Scopia® Management web user interface via HTTPS	Mandatory if using HTTPS
3341	TCP	IBM Sametime	Enables connection to IBM Sametime application	Cannot work with IBM Sametime	Mandatory if Scopia® Management works with IBM Sametime
8080	HTTP (TCP)	Web client	Provides access to the Avaya Scopia® PathFinder and Scopia® Management web user interface	Cannot access the Avaya Scopia® PathFinder web user interface	Mandatory if deployed with Avaya Scopia® PathFinder or Scopia® Management internal Gatekeeper. You can configure this port during installation (see <i>Installation Guide for Avaya Scopia® Management</i>).
9443	HTTPS (TCP)	Web client	Enables Tomcat to run over SSL	Cannot access Scopia® Management web user interface via HTTPS	Mandatory if using HTTPS. You can configure this port as part of setting up HTTPS (see Configuring the Tomcat Web Server to Use HTTPS on page 136).

Minimum Requirements for Scopia® Management

Minimum Server Hardware Requirements

This section describes the minimum hardware requirements of the Avaya Scopia® Management server. The hardware specifications use the CPU passmark as a measure of computers across different models and companies. For more information, and to find out the CPU mark of your system, go to

<http://www.cpubenchmark.net>. The RAM and hard disk sizes must be dedicated solely to Scopia® Management. Avaya Scopia® Management and Scopia® Desktop are installed on separate servers.

! Important:

Make sure the duplex settings of your NIC is correct.

Table 4: Matching hardware server specifications with your product

Product	Max capacity (ports)	Minimum hardware requirements	Can support virtual machine? (VMWare or Microsoft HyperV)
Medium Enterprise edition Scopia® Management and Scopia® Desktop run on different servers.	1000	CPU: Intel Xeon X3430 at 2.40GHz (4 virtual cores) RAM: 4Gb Disk space: 80Gb NIC: 1000Mb	✓
Large Enterprise edition Server runs Scopia® Management and Avaya Scopia® Gatekeeper.	2000	CPU: Intel Xeon E3-1220 at 3.10GHz (4 virtual cores) RAM: 8Gb Disk space: 80Gb NIC: 1000Mb	✓

Operating Systems

Avaya Scopia® Management support the following server operating systems:

- Microsoft Windows 2003 R2 Standard/Enterprise Edition, SP1 & SP2 (32 and 64 Bit)
- Microsoft Windows 2008 Standard/Enterprise Edition, SP1 & SP2 (32 and 64 Bit)
- Microsoft Windows 2008 R2 Standard/Enterprise Edition, SP1 (64 Bit)
- Microsoft Windows 2012 Standard/Enterprise Edition (64 Bit)
- Microsoft Windows 2012 R2 Standard/Enterprise Edition (64 Bit)

! Important:

Scopia® Management relies on the Windows operating system to send and receive SNMP messages to enable the internal gatekeeper to function properly. Be sure to install or enable the Windows **SNMP Service** as one of the services running on the server.

Scopia® Management also supports VMware vSphere versions 4,5, and 5.1, and Microsoft Hyper-V Server. The virtual server operating system specifications include:

- Windows 2003 Server R2 SP2 - Enterprise (32 bit and 64 bit) - VMware vSphere only
- Windows 2008 Server SP2 - Enterprise (32 bit and 64 bit)

- Windows 2008 Server R2 - Enterprise (64 bit)
- Windows 2012 Server - Microsoft Hyper-V Server only

Redundancy Requirements

High availability and service preservation for Scopia® Management is based on either two or three redundant servers.

You can deploy two Avaya Scopia® Management servers in the same location, one as the primary server and the other as a secondary server (local redundancy). If the primary server fails, the secondary server automatically takes over. For increased reliability, deploy a third server as an off-site backup (geographic redundancy). For details, see [High Availability of Scopia® Management](#) on page 221.

For existing redundant deployments, install Scopia® Management on an additional server. For new redundant deployments, install Scopia® Management on two or three separate servers, depending on the redundancy method.

For servers running Windows Server 2008, install WinPcap version 4.1.2 to enable the network switch update its cache with the new MAC address of the active server, if a failover occurs.

Supported User Directories (LDAP)

Scopia® Management interoperates with a number of LDAP servers:

- Microsoft Active Directory Server for Windows 2003 Server
- Microsoft Active Directory Server for Windows 2003 R2 Server
- Microsoft Active Directory Server for Windows 2008 Server
- Microsoft Active Directory Server for Windows 2008 R2 Server
- Microsoft Active Directory Server for Windows 2012 Server
- Lotus Domino Server version 8.0
- Lotus Domino Server version 8.5, 8.5.1, 8.5.2, 8.5.3

Databases

Avaya Scopia® Management uses its own internal database.

Supported Web Browsers

The following browsers are supported by Scopia® Management:

- Internet Explorer 9, 10 and 11
- Firefox 12 and higher
- Safari 6 on Mac OS
- Google Chrome 20 and higher

Supported Mail Programs

Scopia® Management Outlook Add-on supports these versions of Microsoft Outlook:

- Microsoft Outlook 2007 on Windows XP
- Microsoft Outlook 2007 on Windows 7
- Microsoft Outlook 2007 on Windows 7 x64
- Microsoft Outlook 2010 on Windows 7
- Microsoft Outlook 2010 on Windows 7 x64
- Microsoft Outlook 2013 on Windows 8/8.1
- Microsoft Outlook 2013 on Windows 8/8.1 x64

Scopia® Management supports these versions of Microsoft Exchange:

- Microsoft Exchange 2007
- Microsoft Exchange 2010
- Microsoft Exchange 2013

Supported Endpoints and Video Network Devices

Scopia® Management supports these video network infrastructure devices:

- Avaya Aura Session Manager
- Avaya Aura Communication Manager
- Scopia® Elite MCU
- Scopia® Desktop
- Scopia® Video Gateway
- Avaya Scopia® Gateway
- Avaya Scopia® ECS Gatekeeper
- Cisco IOS H.323 Gatekeeper
- Cisco Unified Communications Manager
- Cisco TelePresence Video Communications Server (VCS)
- Microsoft Lync Server 2010, Microsoft Office Communicator Server (OCS) 2007 and 2007 R2
- IBM Lotus Sametime 8.5.1/8.5.2
- Broadsoft IP Centrix

Scopia® Management can also manage a broad range of endpoints, including:

- Scopia® Solution endpoints
 - Avaya Scopia® XT Series
 - Scopia® VC240
- Polycom endpoints
 - VSX 3000/5000/6000/6000A/7000/7000E/7000S/8000
 - HDX 4000/7000/8000/9001/9002/9004

- Tandberg endpoints
 - MXP 990/880/770/550/1500
 - MXP EDGE 75/85/95
 - MXP CENTRIC 1700/1000
 - MXP PROFILE 6000
- LifeSize endpoints
 - Passport
 - Express 220
 - Team 220
 - Room 200
 - LGExecutive

Each endpoint model series supports Scopia® Management features to different extents (see [Table 5: Supported features with various endpoint models](#) on page 20).

Every dedicated endpoint requires a license to join a videoconference and to be defined and managed by Scopia® Management (see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22).

Table 5: Supported features with various endpoint models

Feature	XT Series	Scopia® VC240	Polycom VSX and HDX	Tandberg MXP Series	LifeSize endpoints
Monitoring	✓	✓	✓	✓	✓
Traps and Alarms	✓	✓	✓	✓	✓
Remote Configuration	✓	✓	✓	✓	✓
Mass Software/Firmware Update	✓	✓	✓	✓	X
Mass Configuration	✓	✓	✓	✓	X
Remote Reboot	✓	✓	✓	✓	✓
Auto-detect	✓	✓	X	X	X
Customer Data Records	✓	✓	✓	✓	✓
Graphical usage reports	✓	✓	✓	✓	✓
Limit maximum allowed bandwidth	✓	✓	✓	✓	✓
Populating the local endpoint directory	X	✓	X	✓	X
Corporate Directory	✓	✓	X	X	✓
Endpoint log retrieval	✓	X	X	X	X
Changing H.323 registration	✓	✓	✓	✓	✓
License Update	X	X	✓	✓	X

Planning the Topology of the Avaya Scopia® Management

This section describes the guidelines for deploying this and other Scopia® Solution components in your video network when you integrate with Aura Collaboration Suite.

You can deploy Scopia® Solution components either in a centralized or distributed solution:

- In a centralized topology ([Figure 3: Centralized Scopia® Solution deployment with Aura Collaboration Suite](#) on page 21), all the components are installed in the same location.

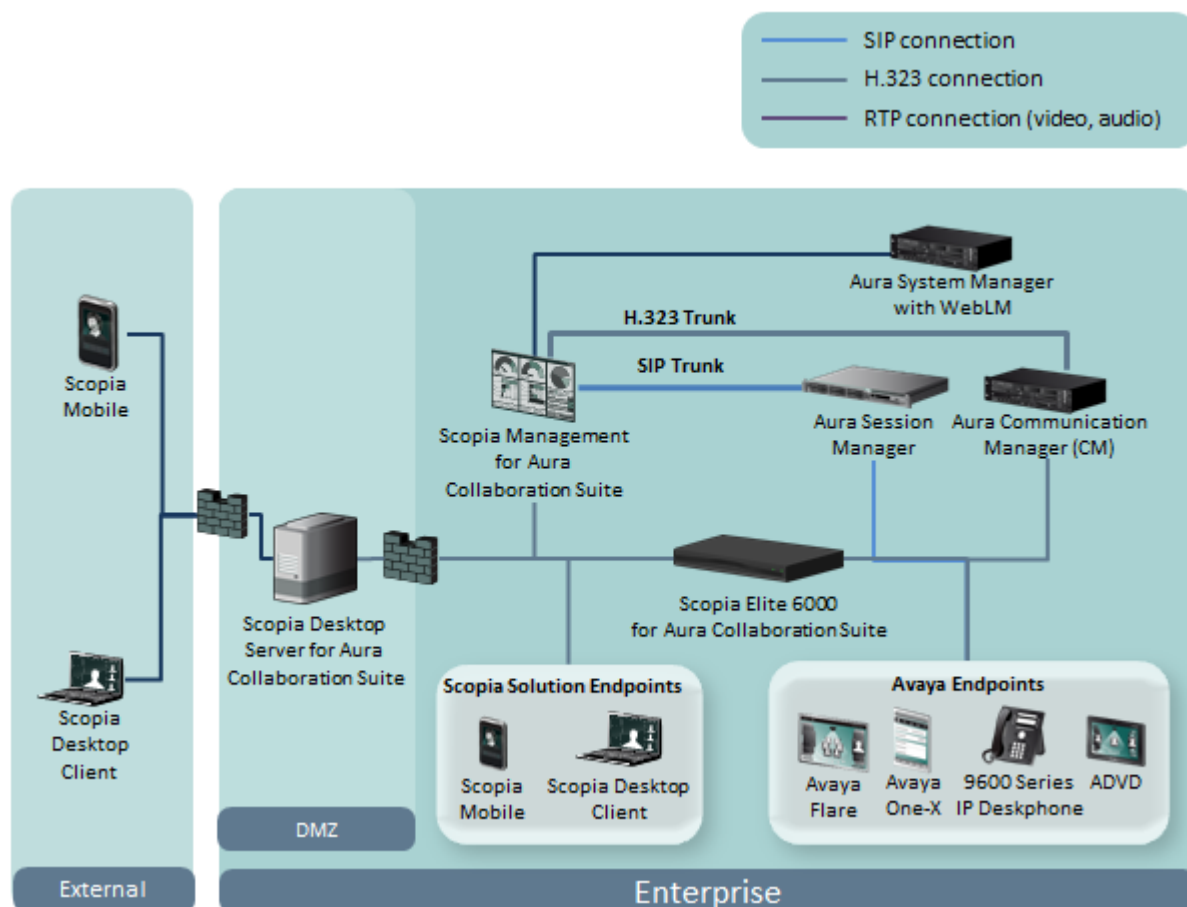


Figure 3: Centralized Scopia® Solution deployment with Aura Collaboration Suite

When deploying the Scopia® Solution for Aura Collaboration Suite, you gain state-of-the-art enterprise videoconferencing using Avaya Scopia® Desktop and Avaya Scopia® Mobile, while enabling these meetings to also include participants on Avaya UC devices such as Flare, One-X, IP Deskphone and ADVD.

The solution includes these mandatory components:

- Scopia® Elite 6000 Series MCU, responsible for combining images from different endpoints into a single continuous presence image to enable effective videoconferencing.
- Avaya Scopia® Management for Aura Collaboration Suite, which sits at the core of your Scopia® Solution and offers a comprehensive management solution for video communications where enterprises can efficiently control the videoconferencing network. The MCU can only function and connect calls when managed and controlled by Scopia® Management for Aura Collaboration Suite.

- Scopia® Desktop server for Aura Collaboration Suite, the desktop videoconferencing system turning PCs, Macs and mobile devices into videoconferencing endpoints. The Scopia® Desktop server brings together meetings with Scopia® Desktop Clients and Scopia® Mobile devices, passing their media connections to the MCU.

A SIP trunk connects the Aura Session Manager to Scopia® Management, while an H.323 trunk connects the Aura Communication Manager also to Scopia® Management. Scopia® Management synchronizes automatically and periodically with the Web License Manager (WebLM) installed on the Aura System Manager to manage the Collaboration Suite licenses. For detailed information on licenses, see *Administrator Guide for Avaya Scopia® Management for Aura Collaboration Suite*. You can also optionally add Aura Conferencing (AAC) to transmit media to the MCU.

- In a distributed topology (Figure 4: Additional components in other locations for a distributed deployment on page 22), you can add components in other locations to create a scalable and geographically distributed solution. You can deploy a full set of videoconferencing components in the headquarters, and distribute additional MCUs and Scopia® Desktop servers over several branches. Each branch can have one or more of these servers depending on the branch's requirements for videoconferencing capacity and high availability. To provide scalability and high availability with service preservation, you can also cluster the Scopia® Desktop servers behind a load balancer. The Scopia® Desktop servers are typically deployed in the DMZ to provide connection to participants from both the internal and external networks.

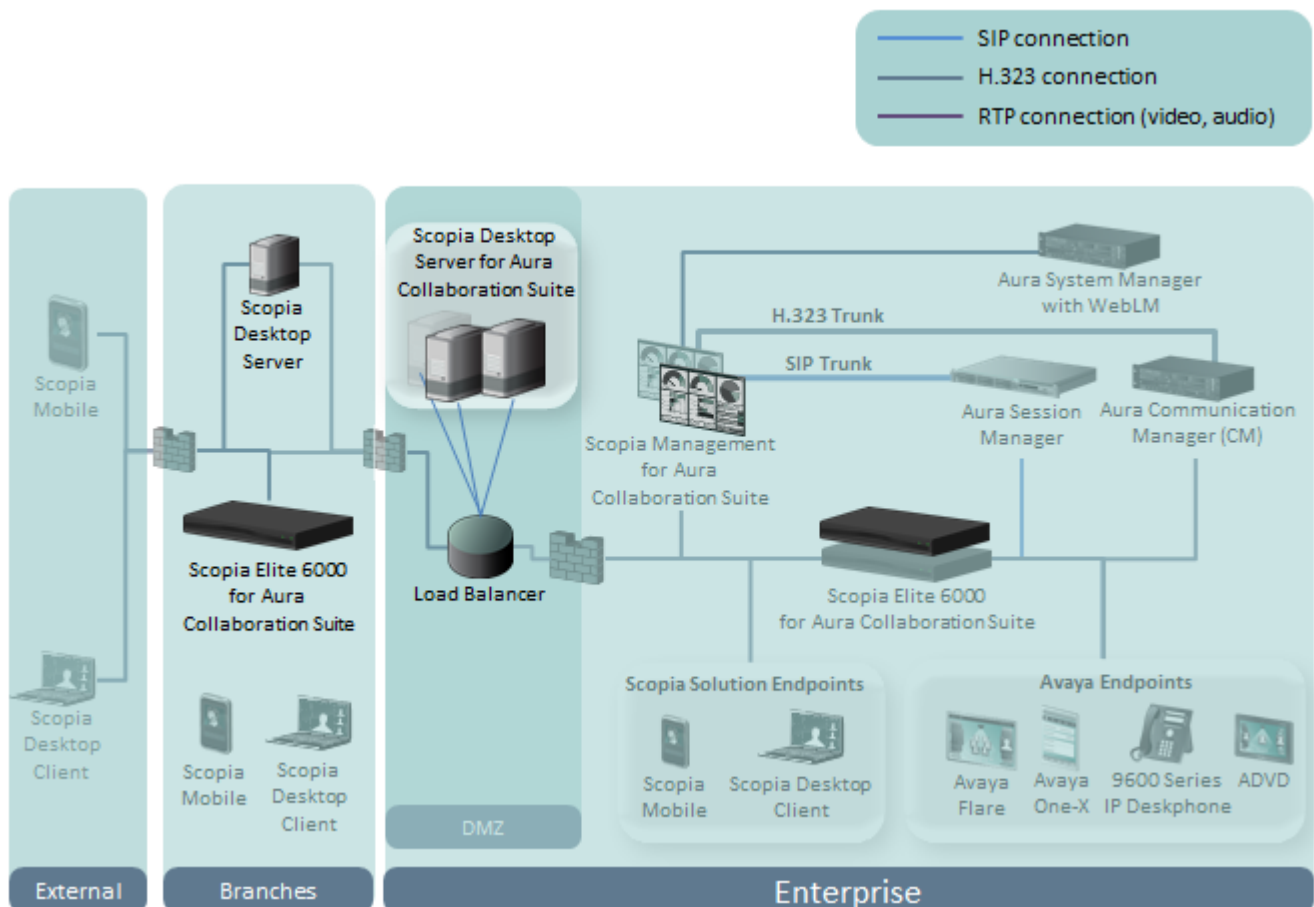


Figure 4: Additional components in other locations for a distributed deployment

For a detailed description of the Scopia® Solution components, refer to *Scopia® Solution Guide*.

Planning Licenses for Integration with Aura Collaboration Suite

As part of integrating Scopia® Solution with Aura Collaboration Suite, you must plan the number of licenses to purchase and allocate. There are four types of licenses:

- Scopia® User for Aura Collaboration Suite licenses offer complete functionality for users of Scopia® Desktop, Scopia® Mobile, and other supported UC clients.
- Guest user licenses are free, offering limited functionality guest Scopia® Desktop and Scopia® Mobile users.
- Scopia® Named Video Endpoint for Aura Collaboration Suite licenses offer complete functionality for dedicated video endpoints like the XT Series.

This license, which grants you the right to join videoconferences, is distinct and separate from other product-specific licenses which activate features in the XT Series.

- Scopia® Guest Video Endpoint for Aura Collaboration Suite licenses offer limited functionality to guest users on dedicated video endpoints. You purchase a pool of these licenses to allow a limited number of endpoints without a Scopia® Named Endpoint license to join a meeting, usually joining from an external network. When guest endpoints start or join a meeting, they are placed in the waiting room until the moderator joins the meeting.

Guest endpoints are not defined or managed in Scopia® Management.

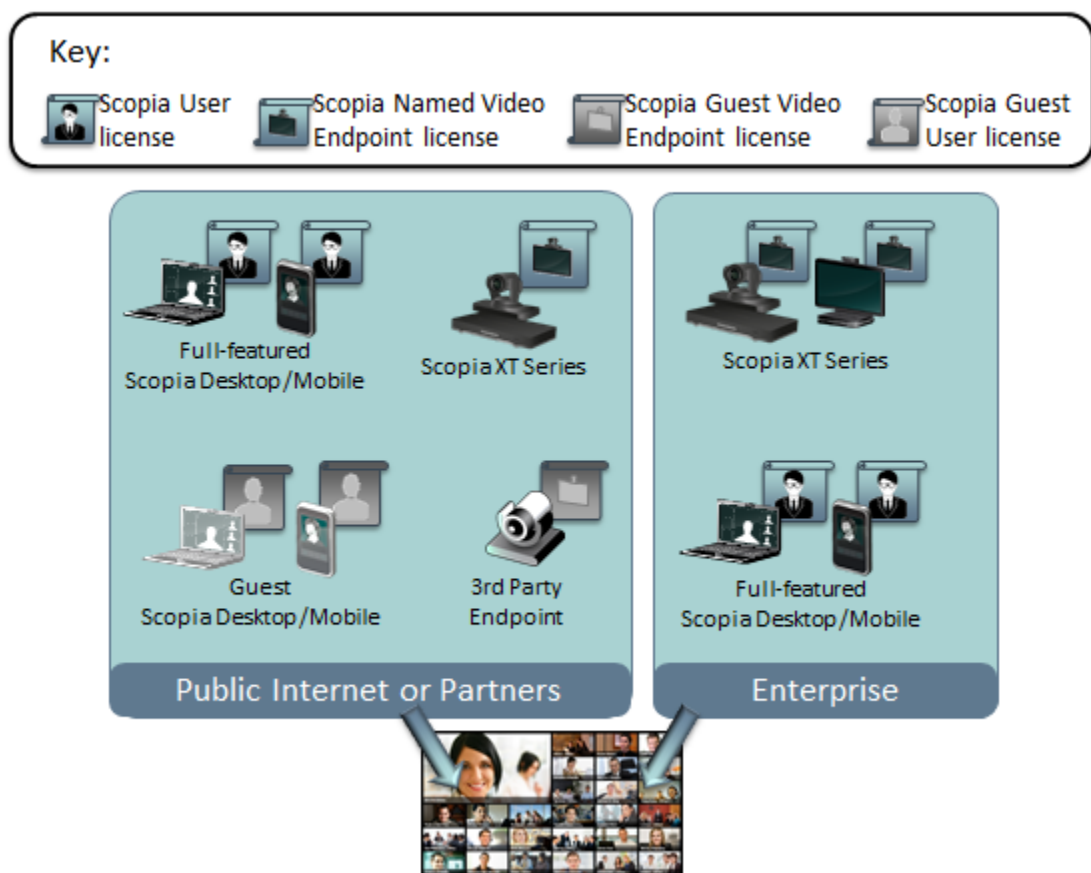


Figure 5: Types of licenses for connecting to videoconference

Table 6: Feature comparison between different Scopia® licenses

Feature	Scopia® User	Scopia® Named Endpoint	Scopia® Guest Endpoint	Guest Video User
Virtual room owner	Yes	N/A	N/A	No
Access Scopia® Desktop web portal	Yes	N/A	N/A	Yes
Start a videoconference	Yes	Yes	Yes, if license available	No
View participants list	Yes	Yes	Yes, if license available	Yes
Moderate the meeting	Yes	Yes	No	No
Share content	Yes	Yes	Yes, if license available	Yes
Schedule a meeting in Scopia® Management	Yes	Yes	No	No
Point-to-point meetings	Yes	Yes	Yes	N/A

If you have a personal endpoint like a Scopia® XT Executive, a Scopia® Named Endpoint license enables you to participate in meetings from that endpoint only. You cannot join from a computer (Scopia® Desktop) or a mobile device (Scopia® Mobile) unless you also have a Scopia® User license. Typically, you assign each member of your organization a Scopia® User license, and each dedicated endpoint a Scopia® Named Endpoint license (see [Table 7: Estimating the number of Scopia® licenses required](#) on page 25).

Table 7: Estimating the number of Scopia® licenses required

License	Number of Licenses
Scopia® User licenses	One license per employee
Scopia® Named Endpoint licenses	One license per dedicated endpoint
Scopia® Guest Endpoint licenses	One license per external dedicated endpoint that will join a meeting simultaneously.

You install licenses on the Avaya Web License Manager (WebLM) server, where Scopia® Management retrieves the license information and uses it to manage users and dedicated endpoints (see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25).

If you have an existing Aura Collaboration Suite and are integrating Scopia® Solution, you can use existing Aura Collaboration Suite licenses as Scopia® User licenses as well.

Deploying Scopia® User and Endpoint Licenses in Scopia® Management

About this task

As part of deploying your Scopia® Solution, you need to install the required Scopia® for Aura Collaboration Suite licenses for both users and dedicated endpoints in your organization.

If you have an existing Aura Collaboration Suite and are integrating Scopia® Solution, you can use existing Aura Collaboration Suite licenses for Scopia® Users as well.

Follow the workflow below to deploy both Scopia® User and video endpoint licenses, which requires first installing the licenses on the Avaya Web License Manager (WebLM) server, and then synchronizing with Scopia® Management. You can do this for all Scopia® licenses simultaneously.

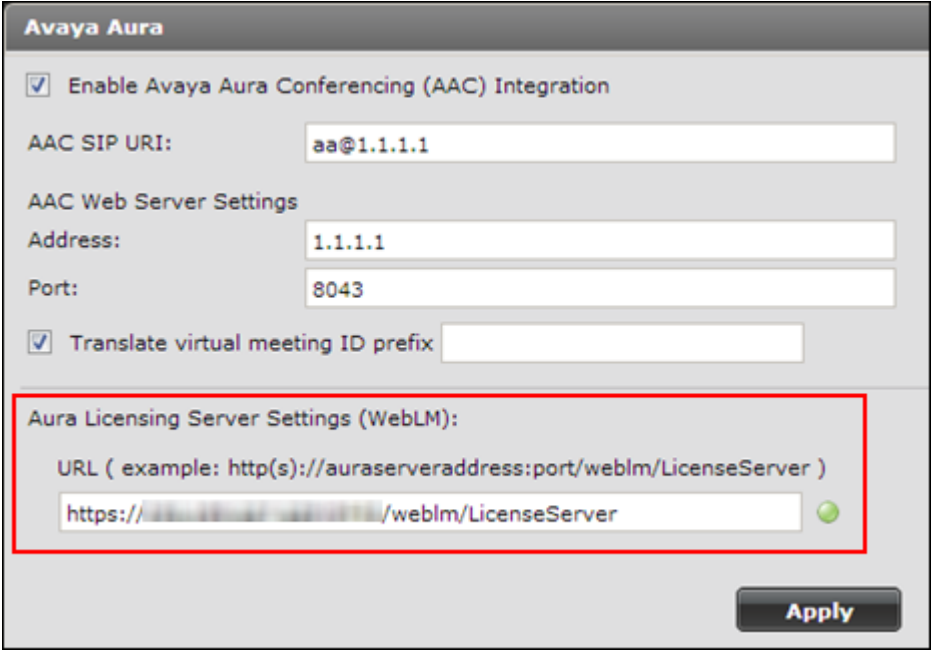
Before you begin

Assess which Scopia® licenses you need and how many (see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22).

After deploying the licenses, you can provision users and add endpoints in Scopia® Management. When performing the initial setup of Scopia® Management, we recommend following the [Initial Workflow for your Organization](#) on page 37.

Procedure

1. Purchase the required number of Scopia® licenses and upload them on the Avaya WebLM server located in the Avaya Aura System Manager (see the *Administering Avaya Aura System Manager* manual for details).
2. Configure the Scopia® Management connection with the WebLM server to import the licensing information:
 - a. In the Scopia® Management administrator portal, select **Settings > Unified Communications> Avaya Aura**.
 - b. Enter the URL of the Avaya WebLM server in the **Aura Licensing Server Settings (WebLM)** field.



The screenshot shows the Avaya Aura configuration window. The 'AAC Web Server Settings' section includes fields for 'Address' (1.1.1.1) and 'Port' (8043). The 'Aura Licensing Server Settings (WebLM)' section, highlighted with a red box, contains a 'URL' field with the value 'https://.../weblm/LicenseServer' and a green status icon. An 'Apply' button is located at the bottom right of the window.

Figure 6: Configuring connection with Avaya WebLM server

- c. Select **Apply**.

Scopia® Management automatically connects to the WebLM (indicated by the green  icon) and imports the number of available licenses.

3. Now that Scopia® Management is updated with the Aura Collaboration Suite licensing information, you can:
 - Assign Scopia® Named Endpoint licenses to endpoints by adding them to Scopia® Management (see [Planning and Configuring Endpoints in Scopia® Management](#) on page 89).
 - Other endpoints use the (temporary) Scopia® Guest Endpoint license and are not managed in Scopia® Management.
 - Assign licenses to specific users, or to user profiles so all members of the profile have a license (see [Creating or Modifying a User Profile](#) on page 162).

Planning User Access to Videoconferences

As part of deploying Scopia® Solution, you need to plan how users in your organization start videoconferences.

Users can either schedule a meeting in advance, and reserve the required video network resources, or they can start an instant meeting. Scheduling meetings with resources ensures a high quality user experience. If there are not enough resources during the videoconference, the system may either downgrade the video quality or block additional participants from joining.

Users can schedule meetings with resources in one of two ways:

- From Microsoft Outlook (2010 or later), using a Scopia® Management plug-in for Microsoft Outlook.
- From the Scopia® Management User Portal.

When scheduling from either one of these plug-ins for Microsoft Outlook, Scopia® Management reserves both the endpoint resources and their required MCU connections.

Users can start instant meetings in one of two ways:

- Dialing an endpoint directly from another endpoint. To dial more than one endpoint, users dial the MCU dial prefix and a virtual room number (personal or public).
- Dialing an endpoint from their virtual room in Scopia® Desktop Client, using the MCU dial prefix.

You set up the MCU prefix and virtual room numbers according to your organization's dial plan.

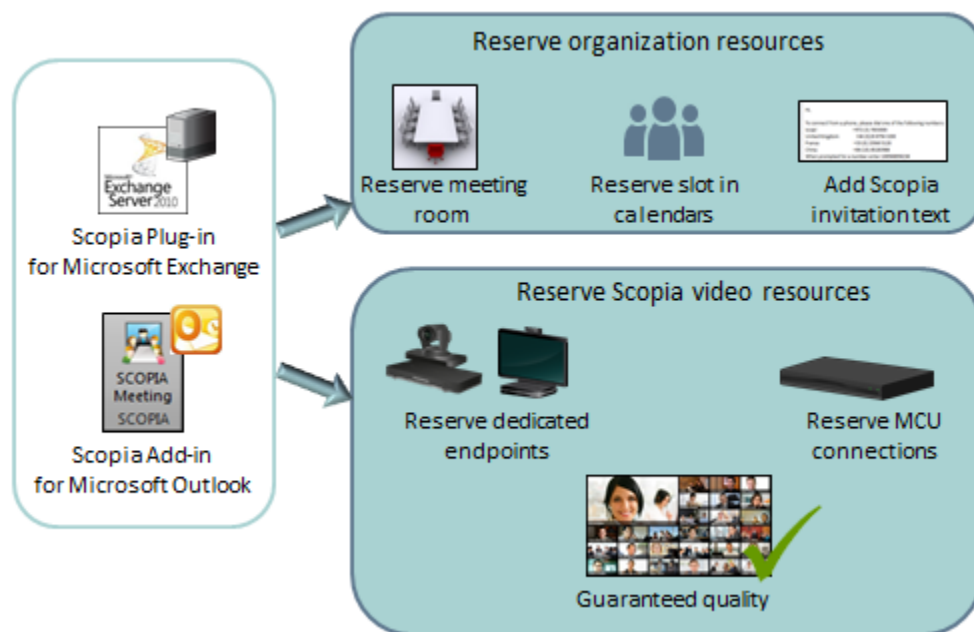


Figure 7: Planning User Access to Scheduling Meetings

The most common way for users to schedule videoconferences is from Microsoft Outlook, since they are already familiar with its interface and are using it to schedule all other (non-video) meetings. This requires deploying one of the Scopia® Management plug-ins for Microsoft Outlook.

Decide which plug-in is right for your organization by using [Table 8: Comparing features of the different Microsoft Outlook Plug-ins](#) on page 28 as a guide. For example, if users in your organization have Mac computers or schedule meetings on-the-go from their mobile devices, deploy Scopia® Plug-in for Microsoft Exchange (see [Installing the Scopia® Plug-in for Microsoft Exchange](#) on page 28). The

Scopia® Add-in for Microsoft Outlook (64-bit), allows more settings to be configured from Outlook, but requires installation on each client (see *User Guide for Scopia® Add-in for Microsoft Outlook*).

Table 8: Comparing features of the different Microsoft Outlook Plug-ins

Features	Scopia® Plug-in for Microsoft Exchange	Scopia® Add-in for Microsoft Outlook
Supported clients	Microsoft Outlook clients on PC Microsoft Outlook clients on Mac Microsoft Outlook Web Application Other calendar applications (such as iOS and Windows-based mobile devices connected to Exchange)	Microsoft Outlook clients on Windows-based PC only (64-bit)
Installation	Installed on Microsoft Exchange server only (not on each client)	Requires installation on each user's computer
User access	All users with a virtual room (even if connecting from a public network)	Only internal users with a virtual room (cannot connect from a public network)
Advanced Meeting Settings (such as reserving extra resources)	Configured from the Scopia® Management user portal	Configured directly from Outlook

There is an additional plug-in available that does not require a user account in Scopia® Management (see *Administrator Guide for Avaya Scopia® Desktop server*). Users cannot reserve video network resources with this plug-in.

Installing the Scopia® Plug-in for Microsoft Exchange

About this task

With the Scopia® Plug-in for Microsoft Exchange, users with a virtual room can easily schedule videoconferences without installing a plugin on their computer or device. Since it works on the Exchange server, users can schedule directly from their Outlook client or other calendar application configured with the Microsoft Exchange server, such as: Microsoft Outlook for Mac, Outlook Web App, and both Windows and iOS-based mobile devices. Install the Scopia® Plug-in for Microsoft Exchange as described below.

As part of the installation, you need to define a keyword that users enter when they schedule meetings, to mark the meeting as a videoconference and reserve video network resources. For example, if you defined *video* as your keyword for the **Location** field, users must enter *video* when scheduling videoconferences in Outlook:

The screenshot shows a scheduling window with the following fields:

- To...**: Three radio buttons are selected, each followed by a room name: "London Conf. Room(8) Room 2", "Beijing Conf. Room(12) Room 8", and "New York Conf. Room(8) Penn".
- Subject**: "Conference Agenda"
- Location**: "London Conf. Room(8) Room 2; video". The word "video" is highlighted with a red box.
- Send**: A button with a paper plane icon.

Figure 8: Scheduling a videoconference

For other scheduling options, see [Planning User Access to Videoconferences](#) on page 26.

To uninstall the Scopia® Plug-in for Microsoft Exchange, run the *uninstall.ps1* file and restart the Microsoft Exchange Transport service.

! Important:

This procedure is for certified Microsoft Exchange integrators who can access the command shell, are familiar with Exchange's account impersonation and how to restart Exchange's transport service.

Before you begin

- The installation of Scopia® Plug-in for Microsoft Exchange typically takes a few minutes and temporarily disconnects the Microsoft Exchange server from the Internet. After the installation, check that both the Microsoft Exchange and the Scopia® Plug-in for Microsoft Exchange is functioning properly by performing tests (for example, send a few test invitations).

Consider sending a maintenance notice to all users, alerting them that the Exchange Server is disconnected and cannot send and receive emails during this time.

- In Microsoft Active Directory, create a user account (such as *scopia_admin*) for Exchange impersonation, to allow Scopia® Management to perform scheduling functionality via Microsoft Outlook on behalf of the user by impersonating that login. This account is configured in this procedure to have access to user information and calendars by impersonating users when scheduling meetings and updating calendar information. You need the account username and password to install Scopia® Plug-in for Microsoft Exchange.

For example, when a user (*Jane@companyname.com*) schedules a videoconference from her mobile device, the message goes through the Scopia® Plug-in for Microsoft Exchange, where the *scopia_admin* account intercepts and processes the message as a videoconference invitation, and then forwards it to Exchange Web Service as if the sender is *Jane@companyname.com*.

- To schedule videoconferences, each person must have a user account in Scopia® Management (see [Defining and Managing Video Users](#) on page 160).
- We recommend creating a Scopia® Management user account specifically for the Scopia® Plug-in for Microsoft Exchange (see [Creating or Modifying a User Profile](#) on page 162). You use the credentials of this account as part of installing Scopia® Plug-in for Microsoft Exchange. Alternatively, you can use any Scopia® Management user account, such as the administrator's.

Procedure

1. Copy all the setup files for Scopia® Plug-in for Microsoft Exchange to a temporary local folder on the Exchange server (such as *c:/temp/scopia_exchange_installation*). These files come with Scopia® Management.
2. Configure the following values in the *settings.properties* file for Scopia® Plug-in for Microsoft Exchange, in the For Administrator area.

Whenever you modify these values, restart the Microsoft Exchange Transport service on the Microsoft Exchange server.

```
//For Administrator
ScopiaManagement.url=http://111.111.111.111:8080
ScopiaManagement.loginID=admin
ScopiaManagement.password=1111
ExchangeServer.email.account=scopia_admin@myexchange.com
ExchangeServer.email.password=admin
ExchangeServer.domain=myexchange.com
ExchangeServer.service.account=administrator@myexchange.com
ScopiaMeeting.symbol.location=@scopia;video
ScopiaMeeting.symbol.subject=@scopia;video
ScopiaMeeting.symbol.recipient=Scopia@scopia.com
```

Table 9: Modifying the settings.properties file

Field	Description
ScopiaManagement.url	Enter the FQDN or management IP address of Scopia® Management.
ScopiaManagement.loginID	Enter the username and password to access the dedicated Scopia® Management account for Scopia® Plug-in for Microsoft Exchange (recommended). Alternatively, you can use any Scopia® Management user account, such as the administrator's.
ScopiaManagement.password	
ExchangeServer.email.account	Enter the email associated with the username of the account you created for impersonation in Exchange, for example <i>scopia_admin</i> 's email might be <i>scopia_admin@myexchange.com</i> .
ExchangeServer.email.password	
ExchangeServer.domain	Enter the domain name of the Microsoft Exchange server.
ExchangeServer.service.account	Enter the Exchange account responsible for sending error notifications to the meeting organizer when scheduling fails (see Microsoft Exchange documentation). For example, if the invitation contains an unknown email address, a system account must send the "undeliverable" email to the sender.
ScopiaMeeting.symbol.location	Enter a keyword in one of these three fields to define the keyword users must enter when scheduling, to mark this as a videoconference and reserve video network device resources. You can enter multiple keywords, separated by a semi-colon (;) and without a space, for example: <i>video;scopia</i> . This is useful, for example, if you want to have keywords in multiple languages. • ScopiaMeeting.symbol.location: Enter a keyword that users must enter in the Location field. The default values are <i>@scopia</i> and <i>video</i>. • ScopiaMeeting.symbol.subject: Enter a keyword that users must enter in either the Subject field. The default values are <i>@scopia</i> and <i>video</i>. • ScopiaMeeting.symbol.recipient: Enter a keyword containing the @ symbol, which users must enter in either the Recipient field. The default value is <i>Scopia@scopia.com</i>. Keywords are not case-sensitive.
ScopiaMeeting.symbol.subject	
ScopiaMeeting.symbol.recipient	

3. Configure the username you created earlier to impersonate or act on behalf of meeting organizers (*scopia_admin*). From the Exchange Management Shell, enter the following command:

```
New-ManagementRoleAssignment -Name:<handle> -Role:ApplicationImpersonation -  
User:scopia_admin
```

Where:

Table 10: Configuring impersonation

Field	Description
Name	Enter a handle for viewing impersonation roles on this server. You can use any name (for example, <i>scopia_role</i>).
User	Enter the username you defined in the <code>ExchangeServer.email.account</code> (in the <i>settings.properties</i> file), which alters invitations on behalf of users by impersonating their account. For example, if the email defined is <i>scopia_admin@myexchange.com</i> , the username is <i>scopia_admin</i> .

For more information, see Microsoft Exchange documentation.

4. From the Exchange Management Shell, install the Scopia® Plug-in for Microsoft Exchange by running the *install.ps1* file (copied to the temporary directory on the server).
5. Restart the Microsoft Exchange Transport service from the list of services running on the server, to refresh it after the installation.
6. Configure the Pickup Directory for Scopia® Plug-in for Microsoft Exchange, which temporarily stores failed meeting invitations to send back to the meeting organizer. From the Exchange Management Shell, enter the following command:

```
Set-TransportService <server_FQDN> -PickupDirectoryPath "<local_path>\pickup"
```

Where:

Table 11: Configuring the Pickup Directory

Field	Description
Set-TransportService For Microsoft Exchange 2010, use <code>Set-TransportServer</code> .	(for Microsoft Exchange 2013): Enter the FQDN or name of the Microsoft Exchange server.
PickupDirectoryPath	Enter " <i>C:\Program Files\Microsoft\Exchange Server\TransportRoles\Agents\Pickup</i> " or another local file path to store the temporary emails.

7. For full functionality of the Scopia® Plug-in for Microsoft Exchange, ensure it has administrator privileges:
 - a. From the task manager, right-click on **EdgeTransport.exe** process and select **Properties > Compatibility tab**.

- b. In the **Privilege Level** area, select **Run this program as an administrator**.
 - c. In Windows Services, double-click the **Microsoft Exchange Transport** service and select **Log on**.
 - d. In the **Log on As** area, select **Local System Account**.
 8. Make sure that the Scopia® Plug-in for Microsoft Exchange is working properly:
 - a. Sending out a test invitation using the keyword you defined, and invite multiple participants and dedicated endpoints.
 - b. Access the Scopia® Management user or administrator portal to check that the meeting appears.
 - c. In Microsoft Outlook, check that the meeting invitation has Scopia® Management's template text, which contains information for how to join meetings from various clients (see [Creating an Invitation Template](#) on page 189).
-

Localized Languages in Scopia® Management

Scopia® Management's administrator portal, user portal, and plug-ins are available in English as well as other languages.

You can view Scopia® Management's administrator portal in the following languages:

- Chinese (simplified)
- English (US)
- French
- Japanese

You can view Scopia® Management's user portal, Scopia® Add-in for Microsoft Outlook, and Scopia® Add-in for IBM Sametime in the following languages:

- Chinese (simplified)
- Chinese (traditional)
- English (US)
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian
- Spanish (international)

By default, Scopia® Management is displayed in English. To view Scopia® Management in another language, change your internet browser's language settings.

Accessing Avaya Scopia® Management

Access Avaya Scopia® Management's administrator portal to perform network-wide management, and the user portal to perform scheduling and meeting management.

The system administrator defines different user profiles with varying permissions to determine the management tasks available for a specific user.

See the following for more information about accessing and using Scopia® Management's portals, and configuring users in Scopia® Management to use the Windows credentials:

Navigation

- [Accessing the Administrator Portal to Manage your Video Network](#) on page 33
- [Accessing the User Portal to Manage your Videoconferences](#) on page 34
- [Enabling Single Sign-on for Scopia® Management](#) on page 35
- [Enabling Single Sign-on for Scopia® Add-in for Microsoft Outlook](#) on page 36

Accessing the Administrator Portal to Manage your Video Network

About this task

You can access Avaya Scopia® Management either from the administrator portal, as described below, or the user portal (see [Accessing the User Portal to Manage your Videoconferences](#) on page 34).

Access the Avaya Scopia® Management administrator portal to do the following:

- Manage all video network devices, including 3rd party endpoints:
 - Remote monitoring, configuration, and upgrade of devices
 - Managing your endpoints, for example by enabling the address book on all endpoints
- Manage bandwidth with:
 - Dynamically routed videoconferences for lowest cost.
 - Distributed MCU deployments.
 - Using distributed MCUs to join a single videoconference, thereby conserving bandwidth
- Manage users in the organization by:
 - Creating user profiles with varying user permissions and capabilities. For example, a profile for read-only users, or users with full Scopia® Desktop Pro and Scopia® Mobile functionality (requires a license).

For information about user profiles and Scopia® Management's built-in profiles, see [Managing User Profiles](#) on page 161.
 - Using Scopia® Management's built-in LDAP directory to manage users, or synchronizing users in your external LDAP directory, such as Microsoft Active Directory.
 - Assigning endpoints and virtual rooms to users

Procedure

1. Navigate to the URL of the Scopia® Management administrator portal, as defined during installation. This should be in the following format: <http://host-URL:port-number/iview>, where the host-URL is the name of the application server on the Scopia® Management server.
2. Log in to the Scopia® Management administrator portal using the credentials specified in the installation process.

The Dashboard appears ([Figure 9: Administrator portal's dashboard](#) on page 34).

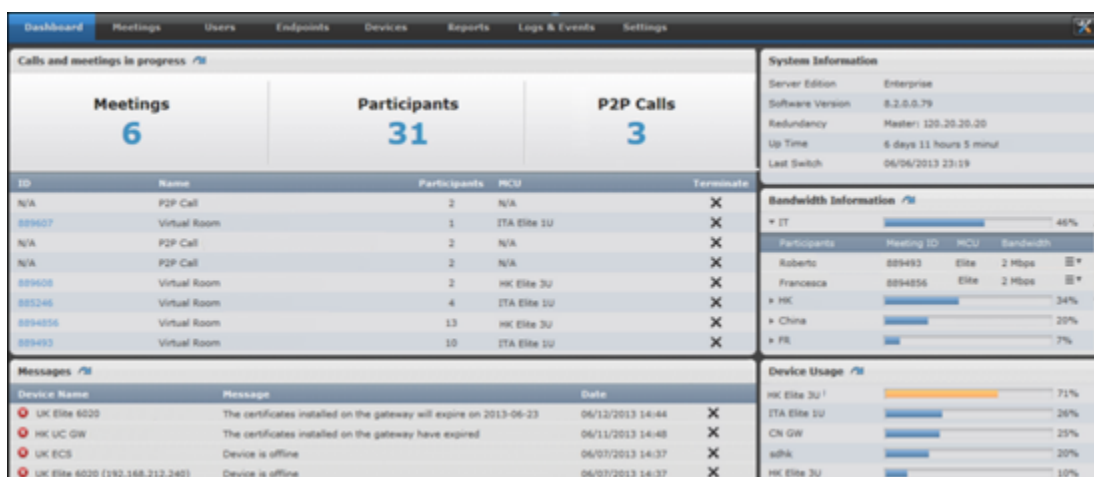


Figure 9: Administrator portal's dashboard

Accessing the User Portal to Manage your Videoconferences

About this task

You can access Avaya Scopia® Management either from the user portal, as described below, or the administrator portal (see [Accessing the Administrator Portal to Manage your Video Network](#) on page 33). Only users who have a Scopia® User assigned to them by the administrator can access the user portal.

All licensed users (such as regular users and meeting operators) access the Avaya Scopia® Management user portal to do the following:

- Schedule, manage and moderate their videoconferences from a single access point.
- View their own videoconferences.
- Manage their own profiles and virtual rooms.

For information about user profiles and Scopia® Management's built-in profiles, see [Managing User Profiles](#) on page 161.

Procedure

1. Navigate to the URL of the Scopia® Management administrator portal, as defined during installation. This should be in the following format: <http://host-URL:port-number>, where the host-URL is the name of the application server on the Scopia® Management server.
2. Log in to the Scopia® Management user portal using the credentials provided by your administrator.

The welcome screen appears ([Figure 10: User portal's welcome screen](#) on page 35).

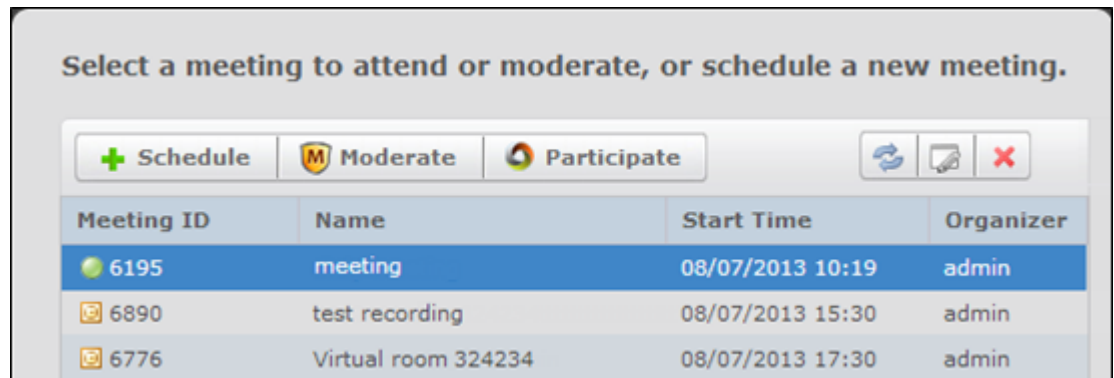


Figure 10: User portal's welcome screen

Enabling Single Sign-on for Scopia® Management

About this task

This procedure enables users to automatically log into Scopia® Management when signing in with their Windows credentials. By default, single sign-on is disabled.

Procedure

1. Open the `vnex.properties` file, located in `<install_dir>\iCM\tomcat\config`.

```
vnex.auth.challenge=never
#
#0:pro version or patch status
#1:No integration with Directory Server
#2:Directory Server
#3:Directory Server with Single Sign On (SSO) Enabled
vnex.user.provision=2
```

Figure 11: Editing the `vnex.properties` file

2. Modify the single sign-on settings as follows:
 - To enable single sign-on, set the `vnex.auth.challenge` parameter to `force`.

- To disable single sign-on, set the `vnex.auth.challenge` parameter to never.

3. Restart the Scopia® Management service.

Enabling Single Sign-on for Scopia® Add-in for Microsoft Outlook

About this task

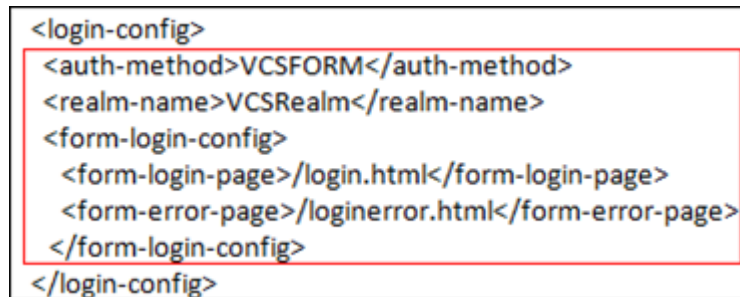
Perform this procedure to allow users to automatically log into Scopia® Add-in for Microsoft Outlook when signing in with their Windows credentials. By default, single sign-on is disabled.

Procedure

1. Open the `web.xml` file, located in `<install_dir>\iCM\tomcat\webapps\xmlservice.war\WEB-INF`.
2. Modify the data within the `<login-config>` tags by replacing it with the following:

```
<auth-method>VCSFORM</auth-method>
<realm-name>VCSRealm</realm-name>
<form-login-config>
  <form-login-page>/login.html</form-login-page>
  <form-error-page>/loginerror.html</form-error-page>
</form-login-config>
```

The modified `web.xml` file reads now as follows:



```
<login-config>
  <auth-method>VCSFORM</auth-method>
  <realm-name>VCSRealm</realm-name>
  <form-login-config>
    <form-login-page>/login.html</form-login-page>
    <form-error-page>/loginerror.html</form-error-page>
  </form-login-config>
</login-config>
```

Figure 12: The modified `web.xml` file

3. Restart the Scopia® Management service.

Initial Configuration Workflow

The tasks you need to perform depend on your role in the deployment.

All tasks are performed by the system administrator, defined during installation, or by additional administrators defined by the system administrator.

Initial Workflow for your Organization

About this task

We recommend that you follow the initial configuration workflow described below, which offers an organized approach to setting up your network in Scopia® Management and preparing the system for daily management. As you configure your network in Scopia® Management, you can view a high-level orientation of your network topology.

Before you begin

- Verify that you have the necessary administrator permissions.

The default system administrator was defined during initial setup of Scopia® Management, and this administrator can create additional administrators. For more information, see [Managing User Profiles](#) on page 161.

- Before you start configuring your Scopia® Management, make sure you have your network planned and all devices are installed and ready to run.

Procedure

1. If you have a distributed deployment (your network devices are situated in multiple locations), define the locations in Scopia® Management, as described in [Defining Locations in your Deployment](#) on page 38.

Important:

If your organization has only one location, it is automatically configured during installation.

2. Add and configure the video network devices, including endpoints, in Scopia® Management according to the workflow described in [Device Configuration Workflow](#) on page 42.

If you are configuring Scopia® Management redundancy, deploy the primary server first, referring to component FQDNs rather than IP addresses (for example, *smgmt.company.com*). This reduces maintenance when servers switch to their backups.

See [Defining your Video Network Devices](#) on page 42 for details about configuring your devices.

3. Define additional administrators, if necessary (see [Creating or Modifying a User Profile](#) on page 162). This is done by the system administrator, who is automatically configured during installation. This step can be done at any time.
4. Define the video users in your enterprise (see [Defining and Managing Video Users](#) on page 160).
5. For high availability, deploy multiple Scopia® Management servers (see [High Availability of Scopia® Management](#) on page 221).

Once redundancy is configured, the database on each Scopia® Management server are synchronized with each other.

Chapter 2 | Defining Locations in your Deployment

This section describes how to create locations within your network. Once you define locations, you can start building your network by adding devices to specific locations.

Locations are where network devices such as gatekeepers, MCUs, endpoints and gateways are placed.

According to the bandwidth threshold defined for each location, Scopia® Management can perform least-cost or best-performance allocation of resources.

Important:

Defining locations is only relevant for administrators of distributed deployments.

Navigation

- [Adding or Modifying a Location](#) on page 38
- [Defining Bandwidth Limits for a Location](#) on page 39

Adding or Modifying a Location

About this task

This procedure is relevant for administrators of distributed deployments.

When configuring your deployment, first divide the network into locations. Then you can start building the infrastructure by adding the network devices, such as gatekeepers, MCUs, gateways, and endpoints to specific locations.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Topology > Locations**.
3. Select a location name or select **Add**.

The **Add Location** or **Location** page appears.

Basic Settings

Location Name: * **Locate on map**

Domain Name:

Max bandwidth allowed for internal calls (Kbps): ☐ Reject calls above limit

Alarm threshold (%): ☐ Generate alarm above threshold

Max bandwidth allowed for cross-location calls (Kbps): ☐ Reject calls above limit

Alarm threshold (%): ☐ Generate alarm above threshold

Figure 13: Adding a location

4. Define the location's basic information, as described in [Table 12: Adding or modifying a location's basic information](#) on page 39.

Table 12: Adding or modifying a location's basic information

Field Name	Description
Location Name	Define the name used to identify this location. Use the same naming conventions to identify zones when adding gatekeepers to the network. See Adding Video Network Devices in Scopia® Management on page 44.
Domain Name	(Optional) If the locations in your deployment have different domain names, enter it for this location. The domain name is useful for identifying the location of SIP endpoints in your network. For example, if an endpoint's SIP URI is name@domain_name.com, and this location's domain name is domain_name, the SIP endpoint is automatically matched to this location.
Locate on map	(Optional) Select to display your location on the map. The location is detected from the Location Name field and a flag icon  appears to mark the location. If more than one location matches the Location Name , select the correct one from the search results.

5. Define the distance and bandwidth thresholds for the location, as described in [Defining Bandwidth Limits for a Location](#) on page 39.

Defining Bandwidth Limits for a Location

About this task

This procedure is relevant for administrators of distributed deployments.

You can define the maximum bandwidth for calls across locations, or the bandwidth dedicated to calls within a location.

When calling across locations, you can define the maximum bandwidth usage and set alerts to be triggered if the maximum designated bandwidth is close to being exceeded.

The bandwidth threshold calculations take into account all types of calls, including Scopia® Desktop calls.

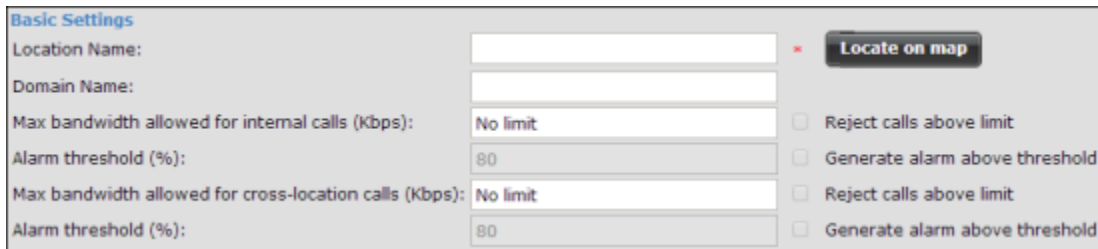
Before you begin

Add the location to your network, as described in [Adding or Modifying a Location](#) on page 38.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Topology > Locations**.
3. Select a location from the **Name** column.

The **Location Profile** window appears ([Figure 14: Defining bandwidth thresholds for a new office or branch](#) on page 40).



The screenshot shows the 'Basic Settings' window for a location profile. It contains the following fields and options:

- Location Name:** A text input field with a 'Locate on map' button to its right.
- Domain Name:** A text input field.
- Max bandwidth allowed for internal calls (Kbps):** A dropdown menu currently set to 'No limit'.
- Alarm threshold (%):** A text input field set to '80'.
- Max bandwidth allowed for cross-location calls (Kbps):** A dropdown menu currently set to 'No limit'.
- Alarm threshold (%):** A text input field set to '80'.
- Checkboxes:** For each bandwidth field, there are two checkboxes: 'Reject calls above limit' and 'Generate alarm above threshold'.

Figure 14: Defining bandwidth thresholds for a new office or branch

4. Enter the information, as described in [Table 13: Defining bandwidth settings for a location](#) on page 40.

Table 13: Defining bandwidth settings for a location

Field Name	Description
Max bandwidth allowed for internal calls (Kbps)	Define the total maximum bandwidth for all calls within this location, in kilobits per second.
Max bandwidth allowed for cross-location calls (Kbps)	Define the total maximum bandwidth for all calls between this location and another, in kilobits per second.

Field Name	Description
Reject calls above limit	Select to automatically disallow calls that exceed the defined maximum bandwidth. To automatically reject calls within the office, select the check box next to in-zone calls. To automatically reject calls between offices, select the check box next to cross-zone calls. If a call is rejected because of bandwidth limits, the system triggers a Call Rejected alert.
Alarm threshold (%)	You can set a system alert when the maximum bandwidth is close to being exceeded. Enter the percentage bandwidth usage that would trigger the BW Utilization alert. The default value is 80%.

5. Determine what is considered an internal call, and what is considered a cross-location call by defining the location.

You can modify a rule by selecting the **Modify** button, or delete it by selecting **Delete**.

- a. Set the location rule by selecting **Add** in the **Advanced Settings** area.

The **Matching Rule** dialog box appears.



The image shows a 'Matching Rule' dialog box with a title bar and a close button. Inside, there are three fields: 'Matching Rule Type' with a dropdown menu showing 'IP range', 'From IP address' with a text input field, and 'To IP address' with a text input field. Both text input fields have a red asterisk to their right. At the bottom, there are two buttons: 'Apply' and 'Cancel'.

Figure 15: Defining the rule for your location

- b. Define a location by setting one of the following rules in the **Matching Rule Type** field:
 - Any device with an IP address within a range, for example between 192.168.1.1 and 192.168.1.110.
 - Any device within an IP subnet, for example to specify 192.168.x.x, enter a base IP of 192.168.1.1 and a subnet of 255.255.0.0.
 - An E.164 dialing prefix, for example any call dialled beginning with the prefix 85.
- c. Select **Apply**.
- d. Select the rule to use from the **Matching Rule Type** column, and select **Apply**.

Chapter 3 | Defining your Video Network Devices

This section provides step-by-step procedures for adding network devices and endpoints, and configuring your videoconferencing network. We recommend that you configure your endpoints and devices according to the workflow described in [Device Configuration Workflow](#) on page 42.

Navigation

- [Device Configuration Workflow](#) on page 42
- [Adding Video Network Devices in Scopia® Management](#) on page 44
- [Planning and Configuring Gatekeepers in Scopia® Management](#) on page 47
- [Adding a Lync Server, an OCS or a SIP Server in Scopia® Management](#) on page 53
- [Planning and Configuring MCUs in Scopia® Management](#) on page 57
- [Planning and Configuring a Scopia® Desktop server in Scopia® Management](#) on page 76
- [Planning and Configuring Gateways in Scopia® Management](#) on page 78
- [Remotely Configuring Avaya Scopia® PathFinder server](#) on page 87
- [Planning and Configuring Endpoints in Scopia® Management](#) on page 89

Device Configuration Workflow

About this task

This procedure describes the recommended workflow for setting up your video network devices. We recommend first adding all devices to Scopia® Management by entering the device's basic information, such as a name to identify the device and its management IP address. This gives you a high-level orientation of your network topology before you configure your devices.

If you are configuring Scopia® Management redundancy, deploy the primary server first, referring to component FQDNs rather than IP addresses (for example, *smgmt.company.com*). This reduces maintenance when servers switch to their backups.

After you add each device, Scopia® Management connects to it and retrieves additional information. You can then perform advanced configurations, such as defining your gatekeeper's dial plan or synchronizing MCU meeting types between multiple MCUs.

Important:

Scopia® Management only retrieves information from MCUs, Avaya gatekeepers, and gateways. Only alarms and traps are retrieved from Avaya Scopia® PathFinder.

Before you begin

If you have multiple locations in your network, make sure you have all the locations defined in Scopia® Management before adding devices to the network. See [Adding or Modifying a Location](#) on page 38.

Verify that your network connections are working and you performed the initial installation procedures for the devices (such as setting up the management IP address), as described in their *Installation Guide*.

Procedure

1. If your deployment includes an external gatekeeper, add it to Scopia® Management as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

Gatekeepers are typically relevant only for distributed deployments. Add the Avaya Scopia® ECS Gatekeeper and third-party gatekeepers to which your H.323 endpoints are registered to.

2. Add and configure the SIP server. This is necessary if your deployment includes SIP endpoints. For details, see [Adding a Lync Server, an OCS or a SIP Server in Scopia® Management](#) on page 53.

For Scopia® Video Gateway deployments, the SIP server is your Microsoft Lync or OCS server.

3. Add the following video network devices relevant for your deployment to Scopia® Management, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44:

- MCUs
- Gateways:
 - A Scopia® Video Gateway is necessary if your video network includes Microsoft Lync.
 - A SIP Gateway is necessary if your deployment includes IBM Sametime.
 - A Scopia® Gateway is necessary if your deployment includes ISDN/PTSN endpoints, or standard telephones or mobile phones.
 - A TIP Gateway is necessary if your deployment includes Cisco Telepresence systems.
- Avaya Scopia® PathFinder servers: are necessary if you require a complete firewall and NAT traversal solution for your H.323 deployment, to enable secure connectivity between enterprise networks and remote sites.

4. Add and configure the Scopia® Desktop servers, as described in [Planning and Configuring a Scopia® Desktop server in Scopia® Management](#) on page 76.

5. Configure each device you added, in the following order:

- Gatekeepers: See [Planning and Configuring Gatekeepers in Scopia® Management](#) on page 47 for details.
- Scopia® Elite MCUs and Scopia® MCUs: See [Planning and Configuring MCUs in Scopia® Management](#) on page 57 for details.
- Gateways: If your deployment includes multiple gateways, you can configure them in any order (see [Planning and Configuring Gateways in Scopia® Management](#) on page 78 for details).
- Avaya Scopia® PathFinders: Are necessary if you require a complete firewall and NAT traversal solution for your H.323 deployment, to enable secure connectivity between

enterprise networks and remote sites. (see [Remotely Configuring Avaya Scopia® PathFinder server](#) on page 87 for details)

Adding Avaya Scopia® PathFinder server to Scopia® Management is optional. Scopia® Management can retrieve alarms and traps from Avaya Scopia® PathFinder server, but cannot manage it.

6. Add and configure the endpoints in your network to Scopia® Management. See [Planning and Configuring Endpoints in Scopia® Management](#) on page 89 for details.

! Important:

If you are importing endpoints from an external LDAP server or H.350 search base, import endpoints after you define the video users in Scopia® Management. See [Defining and Managing Video Users](#) on page 160 for details.

7. If your deployment includes telepresence endpoints, add and configure these endpoints, as described in [Adding Telepresence Systems in Scopia® Management](#) on page 104.

! Important:

If you are adding a Cisco Telepresence system, first configure the TIP Gateway, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

For more information about telepresence systems, see [Planning and Configuring Telepresence in Scopia® Management](#) on page 111.

8. If your deployment includes two Scopia® Management servers, configure your redundant server as described in [High Availability of Scopia® Management](#) on page 221.

Once redundancy is configured, the database on each Scopia® Management server are synchronized with each other.

Adding Video Network Devices in Scopia® Management

About this task

This section describes how to add or modify the following video network devices in Scopia® Management.

If you are configuring Scopia® Management redundancy, deploy the primary server first, referring to component FQDNs rather than IP addresses (for example, *smgmt.company.com*). This reduces maintenance when servers switch to their backups.

- (Optional) External gatekeepers: are typically relevant only for distributed or service provider deployments. Add the Avaya Scopia® ECS Gatekeeper or third-party gatekeepers to which your H.323 endpoints are registered.

! Important:

If your Avaya Scopia® Management uses the internal gatekeeper, you do not need to add it.

- MCUs

- Gateways:
 - A Scopia® Video Gateway is necessary if your video network includes Microsoft Lync.
 - A SIP Gateway is necessary if your deployment includes IBM Sametime.
 - A Scopia® Gateway is necessary if your deployment includes ISDN/PTSN endpoints, or standard telephones or mobile phones.
 - A TIP Gateway is necessary if your deployment includes Cisco Telepresence systems.
- Avaya Scopia® PathFinder servers: are necessary if you require a complete firewall and NAT traversal solution for your H.323 deployment, to enable secure connectivity between enterprise networks and remote sites.

After you add a device, Scopia® Management connects to it and retrieves additional information. You can then configure additional settings for your device, such as managing your bandwidth by using distributed MCUs for a single videoconference.

Important:

Scopia® Management does not retrieve information from the following devices, so you configure all device settings when you add it:

- Third-party gatekeepers (configure as described in the steps below)
- Avaya Scopia® PathFinder server (configure as described in the steps below)
- SIP servers (configure as described in [Adding a Lync Server, an OCS or a SIP Server in Scopia® Management](#) on page 53)
- Scopia® Desktop (configure as described in [Planning and Configuring a Scopia® Desktop server in Scopia® Management](#) on page 76)

Before you begin

Verify that your network connections are working and you performed the initial installation procedures for the devices (such as setting up the management IP address), as described in their *Installation Guide*. Add devices in the order listed in [Device Configuration Workflow](#) on page 42.

If you have multiple locations in your network, make sure you have all the locations defined in Scopia® Management before adding devices to the network. See [Adding or Modifying a Location](#) on page 38.

For Scopia® Video Gateway deployments, ensure your Microsoft Lync Servers are fully configured before adding the gateway to Scopia® Management.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select the type of device you are adding or modifying, such as MCU or gatekeeper from the list in the sidebar.
4. Do one of the following:
 - To add the device, select **Add**.



Figure 16: Adding a new video network device

- To modify the basic attributes of the device, select the link of the device in the **Name** column, and select the **Configure** tab if present.
5. Enter or modify the basic settings for your device, as described in [Table 14: Configuring your device's basic settings](#) on page 46. Scopia® Management then connects to the devices and retrieves additional information, such as the version number.

Figure 17: Adding a new gateway

Table 14: Configuring your device's basic settings

Field Name	Description
Name	Enter the name used to identify the device. This name will be displayed in the list of devices.
IP Address	Enter the device's management IP address, as configured during device installation.
Location	This is only relevant for deployments with multiple locations. Select the device's location.

Field Name	Description
Model	This field is only necessary when adding gatekeepers and gateways: • If adding a gatekeeper profile, select the gatekeeper's vendor and model from the list. • If adding a gateway profile, select the gateway type from the list.
Required GK	(For MCUs and Gateways only) Select the gatekeeper to which the device is registered to from the list. If you select None , the device can be added to Scopia® Management but will not be connected until you register the device with the gatekeeper, and select the gatekeeper here.

6. If you are adding or modifying a third-party gatekeeper, enter the additional fields as described in [Table 15: Configuring a third-party gatekeeper](#) on page 47.

Table 15: Configuring a third-party gatekeeper

Field Name	Description
Login Name Login Password	Enter the username and password required to access the gatekeeper's web interface.
Strip Prefixes	Select for a gatekeeper that is configured to remove zone prefixes.
Zone Prefix	Enter the zone prefix that matches the configuration of the gatekeeper.

7. Configure your devices in the following order, depending on which devices are included in your deployment (after initial configuration, you can modify the devices in any order):
1. Gatekeepers (see [Planning and Configuring Gatekeepers in Scopia® Management](#) on page 47 for details)
 2. MCUs (see [Planning and Configuring MCUs in Scopia® Management](#) on page 57 for details)
 3. Gateways, such as Scopia® Video Gateway, TIP Gateway, or SIP Gateway (see [Planning and Configuring Gateways in Scopia® Management](#) on page 78 for details)
 4. Avaya Scopia® PathFinder (see [Remotely Configuring Avaya Scopia® PathFinder server](#) on page 87 for details)

Planning and Configuring Gatekeepers in Scopia® Management

You can use the following types of gatekeepers in Scopia® Management:

- Avaya Scopia® Gatekeeper: Scopia® Management's built-in gatekeeper, which can be used to manage and route endpoint-initiated calls and point-to-point calls. For more information, see [About](#)

[the Scopia® Management's Internal Gatekeeper](#) on page 48. You do not need to manually add Avaya Scopia® Gatekeeper in Scopia® Management.

- Avaya Scopia® ECS Gatekeeper or Third-Party Gatekeepers: Gatekeepers are typically only used in service provider and other large capacity deployments. You need to define these gatekeepers in Scopia® Management, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

Once defined, you can register your devices and endpoints to the gatekeeper. You can only manage ECS and Avaya Scopia® Gatekeeper via Scopia® Management, for example, by modifying the dial plan.

Navigation

- [About the Scopia® Management's Internal Gatekeeper](#) on page 48
- [Defining the Gatekeeper's Dial Plan in Avaya Scopia® Management](#) on page 49
- [Defining Scopia® Management as the Gatekeeper's Authorization Server](#) on page 51

About the Scopia® Management's Internal Gatekeeper

Scopia® Management is shipped with a built-in gatekeeper, Avaya Scopia® Gatekeeper, which can be used to manage and route endpoint-initiated calls and point-to-point calls.

Gatekeepers are similar to a PBX for an IP video network. After you register the network devices with Scopia® Management's internal gatekeeper, it can perform a number of key functions, including:

- Translate the alias of an address to its actual IP address. There are three types of aliases:
 - E.164 aliases are numeric addresses representing the endpoint, like a phone number.
 - H.323 aliases are alphanumeric addresses that represent endpoints, like 'user_endpoint'.
 - URI aliases are similar to email addresses, like 'user@companyname.com'.

In each case, the gatekeeper translates the alias into its corresponding IP address and routes the call successfully.

- Gatekeepers negotiate the connecting and disconnecting of calls.
- Gatekeepers implement an organization's dial plan. A dial plan is the set of call routing rules based on the pre-defined prefixes of a number. The format can determine the location and/or the services you want.

The most common example of a dial plan comes from the traditional telephony world, where locations are determined by the format of the phone number:

- Numbers which do not begin with a zero are local calls.
- Numbers starting with a single zero denote an inter-city call.
- Numbers starting with a double-zero indicate an international call.

Similarly, a gatekeeper can be configured to determine locations in an organization's dial plan. For example, all numbers beginning with '5' might be located in Europe, '6' routes to the west coast of the US, '7' to the east coast and so on.

In addition to locations, gatekeepers can also invoke services from a number format (dial plan). For example, a number beginning with '88' might be chosen to access a person's video virtual room.

Avaya Scopia® Gatekeeper supplies the correct destination IP and authorizes the appropriate bandwidth for the call. In this way, Scopia® Management can manage endpoint-initiated calls and point-to-point calls.

MCUs, gateways, and endpoints can be registered with the Scopia® Management's internal gatekeeper.

Scopia® Management can also work with the standalone Avaya Scopia® ECS Gatekeeper or third-party gatekeepers when they are configured as neighbors to its internal gatekeeper, including the Cisco IOS H.323 Gatekeeper and the Tandberg (Cisco) Video Communications Server (VCS). Only endpoints can be registered to a third-party gatekeeper.

Defining the Gatekeeper's Dial Plan in Avaya Scopia® Management

About this task

This procedure is relevant only for Avaya Scopia® ECS Gatekeeper and is typically necessary only for service providers and administrators of distributed deployments.

An organization's dial plan must be implemented in Avaya Scopia® Management and also configured in any standalone gatekeepers to ensure the dial plan is managed effectively.

A dial plan is the set of call routing rules based on pre-defined number prefixes. The number prefixes are used to determine the location and/or the services a user needs.

The most common example of a dial plan comes from the traditional telephony world, where locations are determined by the format of the phone number:

- Numbers which do not begin with a zero are local calls.
- Numbers starting with a single zero denote an inter-city call.
- Numbers starting with a double-zero indicate an international call.

Similarly, a gatekeeper can be configured to determine locations in an organization's dial plan. For example, all numbers beginning with '5' might be located in Europe, '6' routes to the west coast of the US, '7' to the east coast and so on.

In addition to locations, gatekeepers can also invoke services from a number format (dial plan). For example, a number beginning with '88' might be chosen to access a person's video virtual room.

Before you begin

You must first add a ECS gatekeeper, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44. Scopia® Management then retrieves information about your gatekeeper, such as the endpoints registered to the gatekeeper.

Procedure

1. Access the Scopia® Management administrator portal.
2. In the **Devices** tab, navigate to **Devices by Type > Gatekeepers**.
3. Select the link of the gatekeeper name you require.
The gatekeeper's information page opens.
4. Select the **Configure** tab and enter the information, as described in [Table 16: Configuring the dialing plan settings](#) on page 50.

Figure 18: Configuring a gatekeeper's basic settings

If these fields are already configured in the ECS web interface, the values are automatically retrieved and displayed here. If you modify these fields via Scopia® Management, they are synchronized with the gatekeeper's web interface.

For more information about these fields, see the *Reference Guide for Avaya Scopia® ECS Gatekeeper*.

Table 16: Configuring the dialing plan settings

Field Name	Description
Name	Enter the name used to identify the gatekeeper. This name will be displayed in the list.
Location	This is only relevant for service providers or deployments with multiple locations. Select the gatekeeper's location.
Gatekeeper ID	Enter the gatekeeper ID, as defined on the gatekeeper.
Registration Mode	Select the registration mode to determine which endpoints can register to the ECS, as follows: • All: Any endpoint can register to the ECS. This option is useful if you have many endpoints to register to the gatekeeper, but is less secure since you do not manage which endpoints connect to the gatekeeper. • None: No endpoints can register to the ECS. Select this option before taking the ECS offline. • Predefined: Only predefined endpoints can register to the ECS. This allows you to effectively manage network resources and gatekeeper services.
Strip Prefixes	Select for a gatekeeper that is configured to remove zone prefixes.

Field Name	Description
Zone Prefix	Enter the zone prefix that matches the configuration of the gatekeeper.
LRQ Hop Count	Enter a number from 1 to 98 to set the maximum number of gatekeepers that an LRQ message can pass. The LRQ hop count prevents deadlocking when an LRQ loop occurs involving Avaya Scopia® ECS Gatekeeper applications and third-party gatekeepers.

5. Select **Apply** to save your changes.

Defining Scopia® Management as the Gatekeeper's Authorization Server

About this task

This procedure is relevant only for Avaya Scopia® ECS Gatekeeper and is typically necessary only for service providers and administrators of distributed deployments.

Define the Avaya Scopia® Management as an authorization server to Avaya Scopia® ECS Gatekeeper to ensure that every call that is routed by the gatekeeper is authorized by Scopia® Management, in terms of bandwidth management and other IT policies.

This procedure is not necessary for the built-in gatekeeper, Avaya Scopia® Gatekeeper, since it gets its authorization from Scopia® Management by default.

Before you begin

You must first add a ECS gatekeeper, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44. Scopia® Management then retrieves information about your gatekeeper, such as the endpoints registered to the gatekeeper.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Navigate to **Gatekeepers** in the sidebar menu, located under **Devices by Type**.
4. Select the link in the **Name** column for the gatekeeper you require.
5. Select the **Access** tab.

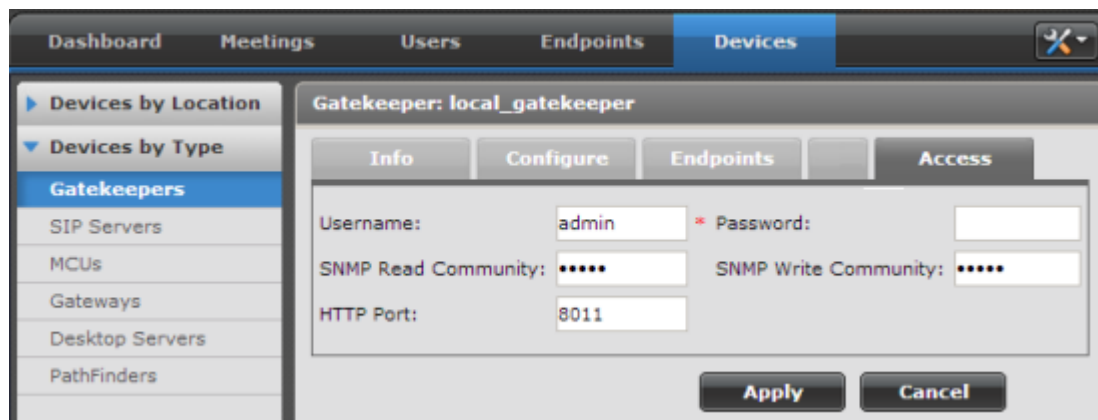


Figure 19: Gatekeeper authorization from Scopia® Management

6. Ensure the access information correspond to the settings on the ECS web interface, as described in [Table 17: Configuring the gatekeeper's access information](#) on page 52.

You can view the **SNMP Get Community** and **SNMP Set Community** fields on the ECS host server under **Control Panel > Administrative Tools > Services > SNMP Service > Security**.

Table 17: Configuring the gatekeeper's access information

Field Name	Description
Username	Enter the login username and password of the ECS web interface login.
Password	
SNMP Read Community SNMP Write Community	Scopia® Management displays the names of the SNMP communities that support the read and write operations of SNMP management in your network. Both the ECS and Scopia® Management support sending and receiving SNMP alerts to track the ECS's behavior and handle any errors which may occur. SNMP community information must match the settings defined in the ECS to enable Scopia® Management to synchronize its information with the ECS. ! Important: The community values are case-sensitive.
HTTP Port	Enter the port used to access the ECS web interface.

7. Select **Apply** to save your changes.
8. Verify your ECS authorization server settings:
 - a. Access the ECS web interface.
 - b. Navigate to **Settings > External API**.
 - c. Select **Allow Authorization servers to connect**.

Adding a Lync Server, an OCS or a SIP Server in Scopia® Management

About this task

To enable Scopia® Management to operate with SIP endpoints, configure Scopia® Management with an external SIP server to which the SIP endpoints are registered. For Scopia® Video Gateway deployments, your Lync/CSR2 server is your SIP server.

Add your Lync Server or OCSR2 to Scopia® Management so that it can use them as a SIP proxy/registrar.

Microsoft's Lync Server and OCSR2 Server are SIP devices. Scopia® Management can communicate with SIP network devices (such as to MCUs) when they are managed by Scopia® Management.

You can view the connection status between Scopia® Management and your SIP server by navigating to **Devices > SIP Servers**.

Scopia® Management is interoperable with these /external SIP servers:

- Microsoft Lync Server 2010
- Microsoft Office Communications Server 2007 R2
- Microsoft Lync Server 2010 Hosting Pack
- Broadsoft IPCentrix
- Cisco Unified Communications Manager (CUCM)

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select **SIP Servers** in the sidebar.
4. Select **Add**.

The **Add SIP Server** page appears.

The screenshot shows the 'Add SIP Server' configuration page. The 'Devices' tab is active. The 'Basic Settings' section contains the following fields:

- Name:** A text input field with a red asterisk indicating it is required.
- FQDN:** A text input field with a red asterisk indicating it is required.
- Port:** A text input field containing the value '5060'.
- Transport Type:** A dropdown menu with 'TCP' selected.
- Model:** A dropdown menu with 'Microsoft LYNC/OCSR2' selected.
- Location:** A dropdown menu with 'Beijing' selected.
- SIP Domain:** A text input field with a red asterisk indicating it is required.
- Use Outbound Proxy:** A checked checkbox.

Figure 20: Adding a SIP server

5. Configure the SIP server settings in the **Basic Settings** section, as described in [Table 18: Configuring SIP server settings](#) on page 54.

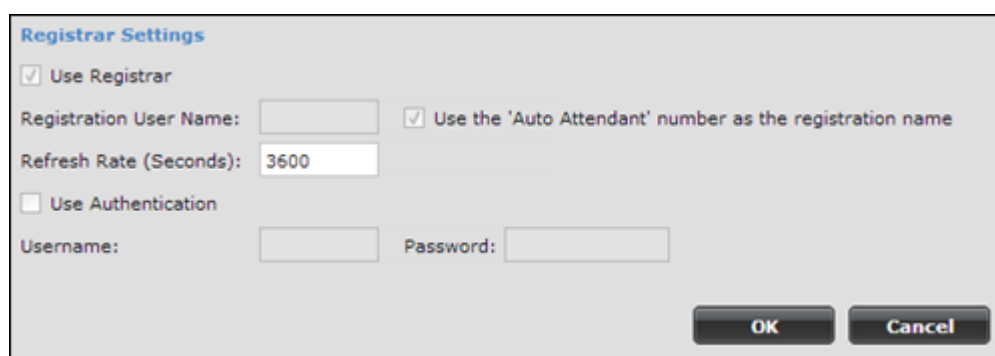
Table 18: Configuring SIP server settings

Field Name	Description
Name	Enter a name to identify your SIP server. This name is displayed in the list of SIP servers.
IP Address/ FQDN	Enter either the network name (FQDN) of the computer that you are using for SIP (specify all domain levels), or the computer's IP address. ! Important: For Scopia® Video Gateway deployments, you must enter the FQDN.
Port	Enter the port used for SIP connections. The default port is 5060 for TCP/UDP, and 5061 for TLS.
Transport Type	Select the transport protocol used for connecting to the SIP server, according to the selected port number. If the default port is 5060, select TCP/UDP; if it is 5061, select TLS.
Model	Select the type of SIP server you are using from the list.
Location	Select the location of the SIP server. This field is only relevant for distributed or service provider deployments.

Field Name	Description
SIP Domain	Enter the domain name of the SIP server's network. For example, if the FQDN is <SIP server name>.companyname, the SIP domain is 'companyname'.
Use Outbound Proxy	Select to forward SIP connections to a proxy SIP server. Otherwise, Scopia® Management handles the SIP connection directly. ! Important: For Scopia® Video Gateway deployments, this is mandatory and therefore selected by default.

6. If required by your SIP server, configure the registrar settings in the **Registrar** section, as described in [Table 19: Configuring Registrar settings](#) on page 55.

A SIP Registrar is used to register IP addresses of SIP endpoints in the network with their SIP URIs.



The image shows a 'Registrar Settings' dialog box. It contains the following fields and controls:

- Use Registrar:** A checked checkbox.
- Registration User Name:** A text input field.
- Use the 'Auto Attendant' number as the registration name:** A checked checkbox.
- Refresh Rate (Seconds):** A text input field containing the value '3600'.
- Use Authentication:** An unchecked checkbox.
- Username:** A text input field.
- Password:** A text input field.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Figure 21: Defining the SIP registrar

Table 19: Configuring Registrar settings

Field Name	Description
Use Registrar	Select to register Scopia® Management to the SIP server. ! Important: For Scopia® Video Gateway deployments, this is mandatory and therefore cannot be modified.
Registration User Name	Enter a name or number to use for registering Scopia® Management to the SIP server, used to forward calls from SIP endpoints to Scopia® Management. ! Important: For Scopia® Video Gateway deployments, this value is the username of the Auto-Attendant, and cannot be modified.

Field Name	Description
Use the "Auto Attendant" number as the registration name	Select if you are using the Auto Attendant. The Auto-Attendant feature provides quick access to meetings hosted on Scopia® Elite 5000 Series MCUs, allowing meeting participants to access a video menu and select menu options using DTMF. To enable the Auto Attendant, see the Enabling Auto-Attendant Support on page 72. The Auto-Attendant number is used for registering Scopia® Management to the SIP server that forwards calls from SIP endpoints to Scopia® Management. ! Important: For Scopia® Video Gateway deployments, this is automatically selected and cannot be modified.
Refresh Rate (Seconds)	Select the frequency with which Scopia® Management sends updated user information to the SIP server, in seconds.
Use Authentication	This is not relevant for Lync or OCS servers. If required by your SIP server, select this option to authorize Scopia® Management to register to the SIP server.
Username Password	To enable Scopia® Management to automatically register to the SIP server, enter the username and password required to access the SIP server.

7. Select **OK** to save your changes.

You can modify these settings at any time by selecting the device name link in the **SIP Servers** list.

8. To identify your organization's domain when calling external SIP endpoints, define the default network domain:

- a. 

Select **Advanced Parameters**.

- b. Find the **vnex.vcms.core.conference.defaultDomain** property and select the **Edit** icon



Advanced Parameters

Caution: null property value will delete the property

Add Property

> Enter property name and value

> Property Name:

> Property Value:

☒ Save to File

Core Properties

vnex.vcms.core.conf.mpInitialTime	10000		
vnex.vcms.core.conf.p2pInitialTime	40000		
vnex.vcms.core.conference.adhoc.allowAdHoc	true		
vnex.vcms.core.conference.autoSyncMcuResou	true		
vnex.vcms.core.conference.callip.special.p	:0		
vnex.vcms.core.conference.cleanUnknownPhyC	true		
vnex.vcms.core.conference.defaultDomain			

c. Enter the network's domain name in the **Property Value** field.

For example, if the FQDN is <SIP server name>.companyname, the domain name is 'companyname'.

d. Select **Apply**.

9. For Scopia® Video Gateway deployments only: Configure your LDAP server in Scopia® Management, as required by your deployment (see [Connecting Scopia® Management with the LDAP Server](#) on page 172 for more details).

Planning and Configuring MCUs in Scopia® Management

The MCU is a hardware unit that hosts videoconferences between multiple endpoints, both H.323 and SIP. MCUs are added to a specific organization or branch, according to pre-defined network topology. For more information about adding the MCU and other devices to Scopia® Management, see [Adding Video Network Devices in Scopia® Management](#) on page 44.

After adding your MCU profile, you can use Scopia® Management to reserve MCU resources, schedule MCU conferences, and control in-session MCU meetings.

This section describes how to modify MCU profiles in Scopia® Management and how to configure and manage MCU services, known as meeting types.

! Important:

This version of Scopia® Management for Aura Collaboration Suite supports only Scopia® Elite 6000 Series MCU.

Navigation

- [Configuring the MCU from Scopia® Management](#) on page 58

- [Modifying an MCU's Location or Organization](#) on page 61
- [Downloading MCU Meeting Types to Scopia® Management](#) on page 62
- [Increasing MCU Capacity by Cascading Multiple MCUs](#) on page 69
- [Enabling Auto-Attendant Support](#) on page 72
- [Integrating the Avaya Aura Conferencing Server](#) on page 75

Configuring the MCU from Scopia® Management

About this task

This procedure describes how to modify and configure your MCU settings, such as the MCU's location and registered gatekeeper.

Before you begin

Add the MCU to Scopia® Management by entering its basic settings, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab and navigate to **MCUs**, located under **Devices by Type**.
3. Select the link of the MCU you want to modify in the **Name** column.

The MCU page appears.

The screenshot displays the 'Configuration' tab of the MCU settings interface. It is divided into three sections: Basic Settings, H.323 Settings, and SIP Settings. In the Basic Settings section, the 'Name' field is set to 'Italy Elite 6105', and there are three unchecked checkboxes for 'In Maintenance', 'Secure XML connection using TLS', and 'Secure connection using HTTPS'. The H.323 Settings section shows 'Required Gatekeeper' and 'Current Gatekeeper' both set to 'Italy ECS (10.110.10.10)', and 'Location' set to 'Italy'. The SIP Settings section shows 'SIP Proxy Server' as '202.20.20.20', 'Transport Type' as 'TCP', and 'Default SIP Domain' as 'mcu.company.com'.

Figure 22: Configuring the MCU

4. Select the **Configuration** tab to configure your MCU settings, as described in [Table 20: Configuring your MCU](#) on page 59.

Table 20: Configuring your MCU

Field Name	Description
Name	You can modify the name used to identify the MCU. This is the name displayed in the list of MCUs.
In Maintenance	Select if the MCU is currently being upgraded or in repair. If this option is selected, you can still configure settings and perform upgrades, but this MCU cannot be used to host videoconferences.
Secure XML connection using TLS	For enhanced security, you can secure XML communication between Scopia® Management and the MCU, using TLS. This field is relevant only for Scopia® Elite 6000 Series MCU version 8.3 and later. You can do this only if you installed certificates for the MCU, either from Scopia® Management or from the MCU interface (see <i>Administrator Guide for the Scopia® Elite 6000 Series MCU</i>).

Field Name	Description
Secure connection using HTTPS	Select to secure access to the MCU web interface using HTTPS. You can do this only if you installed certificates for the MCU, either from Scopia® Management or from the MCU interface (see <i>Administrator Guide for the Scopia® Elite MCU</i>).
Required Gatekeeper	Select the gatekeeper to which the MCU is registered from the list. If the MCU is not registered to a gatekeeper, select None. This might be the case, for example, in a SIP-only environment.
Current Gatekeeper	This (read-only) field displays the management IP address of the gatekeeper this MCU is currently registered to. In most cases, this is the same gatekeeper selected in the Required Gatekeeper field. If the current gatekeeper is not the same as the gatekeeper configured in Required Gatekeeper, an alarm is issued by Scopia® Management. This can happen if, for example, the gatekeeper was modified via the MCU web interface.
Location	This is only relevant for service providers or deployments with multiple locations. You can modify the MCU's location.
SIP Proxy Server	If your deployment includes SIP endpoints, enter the IP address of the local server that you are using to enable SIP functionality.
Transport Type	Select the transport protocol used for connecting to the SIP server, according to the security level you require. For secured communication between the MCU and the SIP server, select TLS. You can do this only if you installed certificates for the MCU, either from Scopia® Management or from the MCU interface (see <i>Administrator Guide for the Scopia® Elite MCU</i>). The port used for SIP connections automatically changes to 5061.
Default SIP Domain	Enter the domain name of the SIP server's network. For example, if the FQDN is <SIP server name>.companyname, the SIP domain is 'companyname'.

5. Select the **Access** tab and enter the MCU's information, as described in [Table 21: Configuring the MCU's access information](#) on page 61.

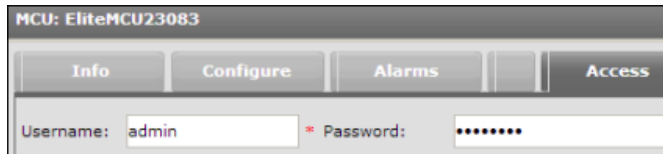


Figure 23: Configuring the MCU's access information

Table 21: Configuring the MCU's access information

Field Name	Description
Username Password	Enter the login username and password of the MCU web interface login.
SNMP Read Community SNMP Write Community	This is relevant for the Scopia® MCU only. Scopia® Elite MCU sends traps and alarms via APIs, and not SNMP alerts. Scopia® Management displays the names of the SNMP communities that support the read and write operations of SNMP management in your network. SNMP community information must match the settings defined in the MCU to enable Scopia® Management to retrieve information from the MCU. ! Important: The community values are case-sensitive.

6. Select **Apply** to save your changes.

Modifying an MCU's Location or Organization

About this task

This procedure is relevant for administrators of a distributed deployment.

Once the MCU is added to Scopia® Management, you can modify its location according to your network requirements and topology.

A location is a physical space (building) or a network (subnet) where video devices can share a single set of addresses. A distributed deployment places these components in different locations, often connected via a VPN.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select **MCUs**, located under **Devices by Type**.

4. Select the link in the **Name** column for the MCU you want to configure.
5. Select the **Configure** tab.
6. Select the MCU's location from the **Location** list.
7. Select **OK** to save your changes.

Downloading MCU Meeting Types to Scopia® Management

You define MCU meeting types in the MCU (see *Administrator Guide for Scopia® Elite MCU*), and then download them to Scopia® Management. When meeting operators, meeting organizers, and users schedule a videoconference, they determine its characteristics by assigning a meeting type. You can create and customize the meeting types depending on the specific needs of your organization.

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. You can invoke a meeting type by dialing its prefix in front of the meeting ID. Meeting types are created and stored in the MCU, with additional properties in Scopia® Management.

You can also define additional properties specific to Scopia® Management functionality. These are used by Scopia® Management only, and do not need to be synchronized with the MCU.

When you have more than one MCU in your deployment, you first define meeting types only on one of them so that it serves as a reference MCU. You then add the meeting types to Scopia® Management and distribute them from the reference MCU to other MCUs, as shown in [Figure 24: Synchronizing meeting types](#) on page 62.

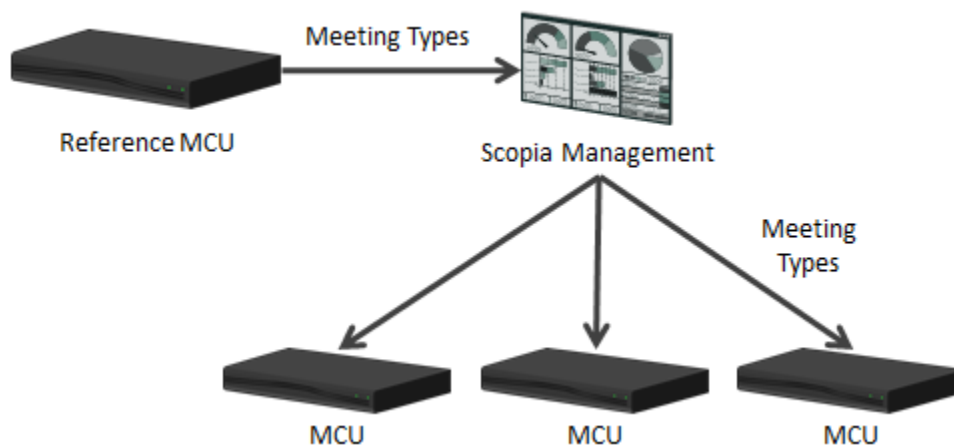


Figure 24: Synchronizing meeting types

In addition to MCU meeting types, Scopia® Management comes with a built-in meeting type for point-to-point meetings, which bypasses MCUs. It is used only when one endpoint dials another endpoint directly. You cannot delete this built-in meeting type, and can modify its default bandwidth only.

This section explains how to manage MCU meeting types in Scopia® Management:

Synchronizing MCU Meeting Types with Scopia® Management

About this task

This procedure describes how to download MCU meeting types to Scopia® Management and then, if relevant for your deployment, synchronize the meeting types among multiple MCUs. Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting.

Once you download the meeting types to Scopia® Management:

- Meeting operators, meeting organizers, and users can assign a meeting type when scheduling a videoconference.
- You can specify which users have access to certain meeting types (see [Creating or Modifying a User Profile](#) on page 162). For example, you can allow a VIP user to schedule meetings with a higher maximum bandwidth for better quality.
- For deployments with multiple MCUs, you can propagate meeting types from the reference MCU to all other MCUs across your organization ([Figure 25: Synchronizing meeting types across MCUs](#) on page 63), as described in the procedure below.

If you later add or remove meeting types on the reference MCU, or you want to change the reference MCU, you need to re-synchronize the meeting types.

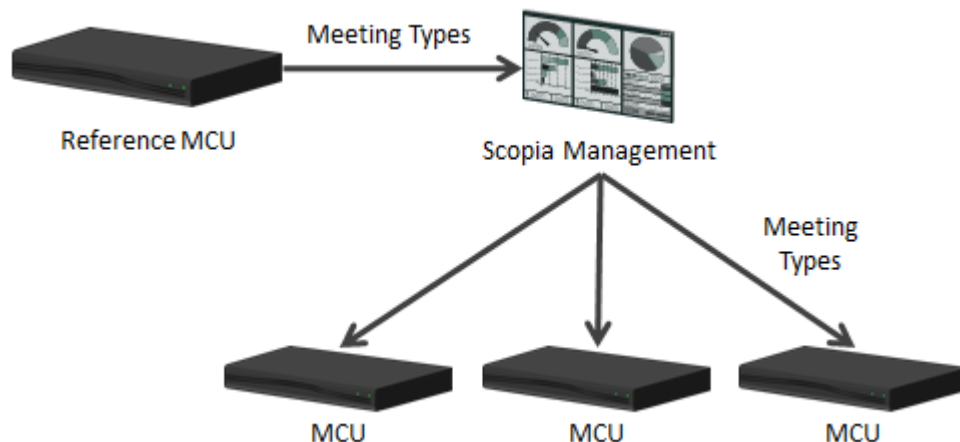


Figure 25: Synchronizing meeting types across MCUs

- If you modify a meeting type setting in the MCU, you need to re-synchronize the meeting types with MCU.

Before you begin

If you have multiple MCUs in your deployment, decide which MCU you would like to use as a reference for other MCUs, and verify that all meeting types are defined on your reference MCU. To create MCU meeting types, see *Administration Guide for Scopia® Elite MCU*.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Settings** tab. The **Meeting Types** page appears.

If this is the first time you are synchronizing, only Scopia® Management's built-in meeting type is displayed.

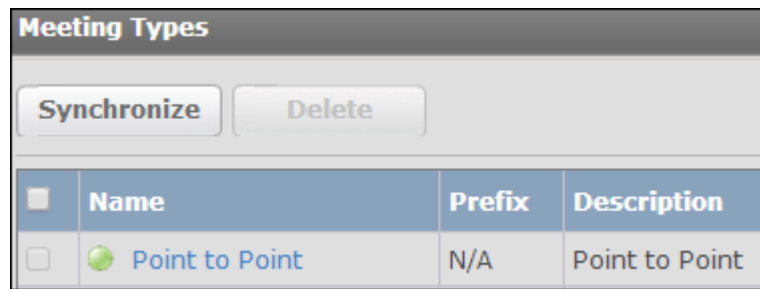


Figure 26: Synchronizing meeting types

3. Select **Synchronize**. The **Meeting Type Synchronization** page appears.
4. For deployments with one MCU, verify that the names of the meeting types are correct and select **Confirm**.



Figure 27: Confirming MCU meeting types

The meeting types are now downloaded to Scopia® Management and appear in the list of meeting types.

5. For deployments with multiple MCUs:
 - a. Select the MCU to use as a reference for other MCUs of that type, from the lists.
 - b. Select **Next**.
 - c. Select the MCUs to be synchronized. By default, all MCUs of that type are selected.

! Important:

Make sure the MCUs support the meeting types being uploaded. For example, you cannot upload a meeting type defined to support High Definition Continuous Presence (HDCP) conferences to an MCU that is not enabled for HDCP.

The following MCUs will be synchronized with the reference MCU.		
Selected MCUs from this list will be synchronized with SCOPIA Elite MCU: EliteMCU23083		
☒	SCOPIA Elite MCUs	Meeting Types
☒	Ava23064	60181, 60182, 60183, 610, 70, 71, 72, 73, 74, 75, 76, 77, 78,
Selected MCUs from this list will be synchronized with SCOPIA MCU: ClassicMCU230109		
☒	SCOPIA MCUs	Meeting Types
☒	162.168.230.102	80, 81, 82, 83, 84, 85, 86

Figure 28: Synchronizing MCUs

- d. Select **Next**.
 - e. Verify that the meeting type names and prefixes in the list are correct.
 - f. Select **Confirm**.
- The MCU's meeting types are now synchronized across the selected MCUs.

Defining a Default and Fallback Meeting Type

About this task

Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting. A default meeting type defines the initial settings of the default meeting type in the **Meeting Scheduling** window when creating a new scheduled meeting both from the Scopia® Management user portal or when initiating a meeting from an endpoint.

Avaya Scopia® Management uses a fallback meeting type when it cannot create an ad-hoc meeting due to lack of resources. For example, if a user wants to start an ad-hoc meeting from the endpoint, Avaya Scopia® Management first tries to create a meeting using the default meeting type, and if resources are unavailable, it uses the fallback meeting type.

Procedure

1. Access the Scopia® Management administrator portal.
 2. Select **Settings > Meetings > Policies**.
- The **Meetings Policies** page appears.

Figure 29: General section of the Meeting Policies page

Meeting Policies	
General	
Default Meeting Type:	79 ▼
Fallback Meeting Type:	79 ▼
Minimum Meeting ID Length:	4
Virtual Meeting ID Prefix:	6
☒ Allow Cascaded Meetings	
Cascading Priority:	Local MCU ▼
Reserved ports for dynamic cascading:	2

3. Select a default meeting type from the **Default Meeting Type** list.
We recommend that you select a default meeting type which is available to all users.
4. Select a meeting type from the **Fallback Meeting Type** list.
5. Select **Apply** to save your changes.

Modifying an MCU Meeting Type in Scopia® Management

About this task

You can modify an existing MCU meeting type in Scopia® Management by defining the properties specific to Scopia® Management functionality. For example, you can modify the default bandwidth (bitrate) that undefined endpoints use when connecting to a videoconference. Bitrate is the speed of data flow. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion.

Other properties that are defined on the MCU, such as the prefix of the meeting type, can only be modified on the MCU (see *Administrator Guide for the Scopia® Elite MCU*).

In addition to MCU meeting types, Scopia® Management comes with a built-in meeting type for point-to-point meetings, which bypasses MCUs. It is used only when one endpoint dials another endpoint directly. You cannot delete this built-in meeting type, and can modify its default bandwidth only.

Before you begin

To enable support for connecting to the Avaya Aura Conferencing (AAC) server, you must first integrate it with Scopia® Solution, as described in [Integrating the Avaya Aura Conferencing Server](#) on page 75.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Meetings > Meeting Types**.
3. Select the link in the **Name** column for the meeting type you require.

The **Meeting Type Details** page opens, displaying all the properties available for this specific meeting type.

Meeting Type Details

Name: HD 4MB BW *

Prefix: 74

Description: HD 4MB BW

Media: Video

Maximum Bandwidth (Kbps): 4096

Default Connection Rate (Kbps): 4096 ▼

☐ Auto-Attendant Support

☒ Enable Gallery Layouts (requires additional 480p resource per meeting)

☐ Enable Avaya Aura Conferencing

MCUs: EliteMCU18550

Figure 30: Modifying the meeting type (example)

Table 22: Meeting type parameters

Parameter	Description
Name	Displays the name of the meeting type, as defined in Scopia® Management. MCUs do not give names to meeting types. You can enter a new name if necessary.
Prefix	Displays the dial prefix for this meeting type. A dial prefix is a number added at the beginning of a dial string to route it to the correct destination, or to determine the type of call. The meeting type prefix is downloaded from the MCU and cannot be changed in Scopia® Management.
Description	Displays the meeting type description, downloaded from the MCU.
Media	Displays the type of media available for this meeting type, downloaded from the MCU: • Audio only: No video (either from participants or a presentation) is displayed, to conserve bandwidth and MCU resources. • Video: High Definition (HD) video, the default value for meeting types. • Video (Switched HD): Displays only one participant at a time to conserve bandwidth. • Video (Desktop): Video at a lower resolution (CIF), doubling the MCU capacity (Scopia® MCU only).
Maximum Bandwidth (Kbps)	Displays the maximum meeting bandwidth (bitrate) between an endpoint and the MCU when using this meeting type, downloaded from the MCU.

Parameter	Description
Default Connection Rate (Kbps)	Specify the default bandwidth (bitrate) for this meeting type, used for any endpoints that are not defined in Scopia® Management, and are invited without specifying the bandwidth. The default bandwidth must be equal to or less than the Maximum Bandwidth. Kilobits per second (kbps) is the standard unit to measure bitrate, measuring the throughput of data communication between two devices. You can also specify the bandwidth for an endpoint when scheduling the meeting, or during the meeting. Endpoints that are defined in Scopia® Management use their specified bandwidth by default (see Planning and Configuring Endpoints in Scopia® Management on page 89).
Auto-Attendant Support	Select to enable Auto-Attendant support for this meeting type. Auto-Attendant, also known as video IVR, offers quick access to meetings hosted on MCUs, via a set of visual menus. Users can view and join meetings from the Auto-Attendant, which displays all ongoing meetings in the organization. Disable this option if, for example, you do not want videoconferences with this meeting type to appear on the Auto-Attendant.
Enable Gallery Layouts (requires additional 480p resource per meeting)	Select to enable gallery layouts when sharing content, which use additional MCU resources (an extra 480p connection per meeting). This is available for Scopia® Elite 6000 Series MCUs only, and for Video meeting types (as displayed in the Media field). The Scopia® Elite 6000 Series MCU supports an additional set of layouts to optimize screen space during content sharing on single-screen endpoints (see <i>User Guide for Scopia® Elite MCU</i>). The MCU processes the presentation and places it in the video layout alongside participant images, allowing endpoints with proprietary content sharing protocols such as Avaya Flare Experience or Microsoft Lync to simultaneously display content and participants.
Enable Avaya Aura Conferencing	Select to automatically connect to Avaya endpoints via the AAC server when the meeting starts. This is only relevant for Scopia® Solution integration with the AAC server.
MCUs	Lists the MCUs in your deployment that support this meeting type. You can select the link to access the MCU's administrator interface.

4. Select **Apply** to save your changes.

Searching for a Meeting Type

About this task

You can search for a specific meeting type by name. Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting.

Procedure

1. Access **Scopia®** Management.
 2. Select **Meeting Types** in the sidebar menu.
 3. Enter the partial or complete name of the meeting type in the **Name** field.
Search results are listed.
 4. To return to the complete list of meeting types, delete text in the **Name** field.
-

Deleting a Meeting Type from Scopia® Management

About this task

You can permanently remove a meeting type from Scopia® Management to remove it from all MCUs in your deployment. Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting.

❗ Important:

When you delete meeting types, they cannot be restored later.

You cannot delete meeting types which are currently in use. If you need to delete a meeting type, wait until a meeting using this meeting type is over, then delete it.

Procedure

1. Access **Scopia®** Management.
 2. Select **Meeting Types** from the sidebar.
 3. Select the meeting type you want to delete.
 4. Select **Delete** and then **OK**.
The meeting type is deleted from Scopia® Management.
-

Increasing MCU Capacity by Cascading Multiple MCUs

About this task

A cascaded videoconference is a meeting distributed over more than one physical Scopia® Elite 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.

You can cascade MCUs to reduce potential drain on network resources, increase the efficiency of MCU usage, and allow large conferences to be held ([Figure 31: A single cascaded videoconference](#) on page 70).

MCU cascading is enabled by default. This procedure describes how to configure the MCU's cascading behavior, which is managed by Scopia® Management.

A videoconference is typically hosted on the MCU closest to the meeting organizer's location, although this can be modified when scheduling a meeting. For example, if most meeting participants are in a different location, the meeting organizer may decide to change the master MCU for this meeting. Depending on the cascading preference set below, this master MCU connects to one or more slave MCUs to form a cascaded meeting.

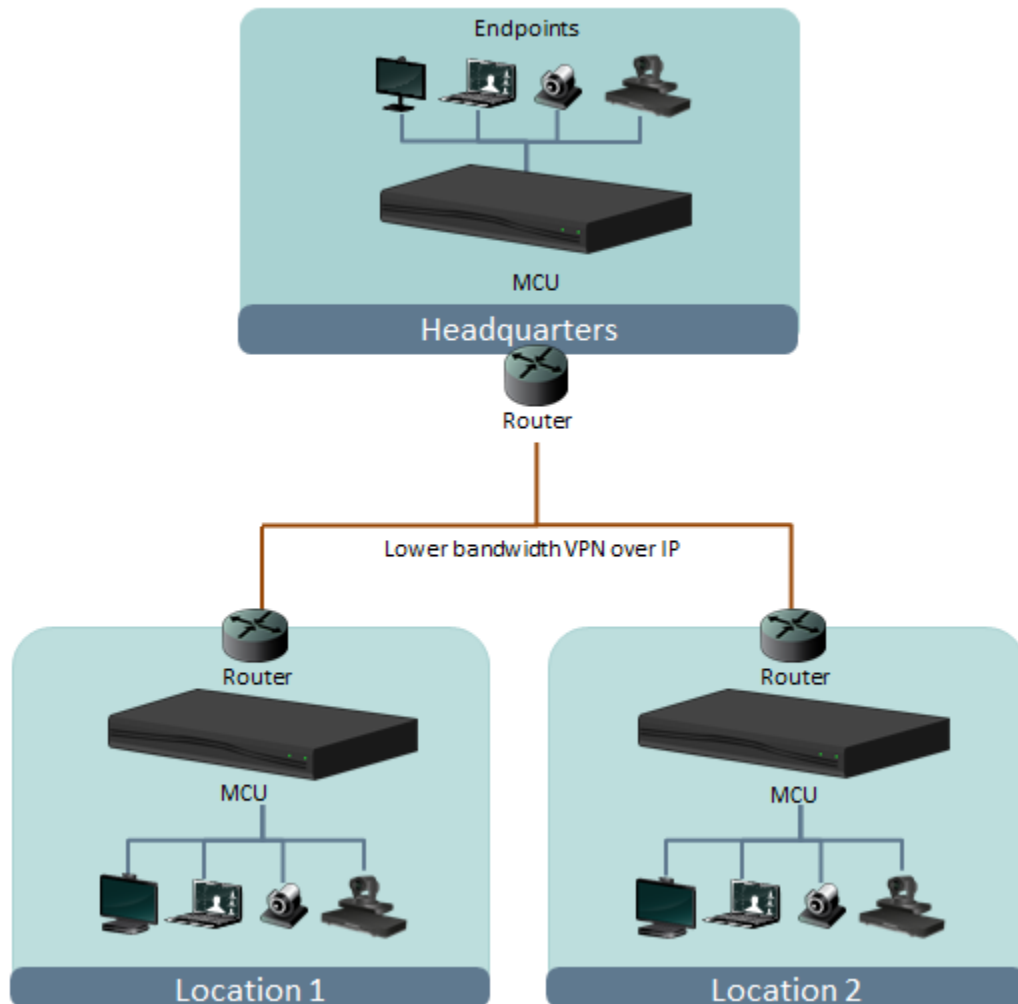


Figure 31: A single cascaded videoconference

The following points about cascading should be noted:

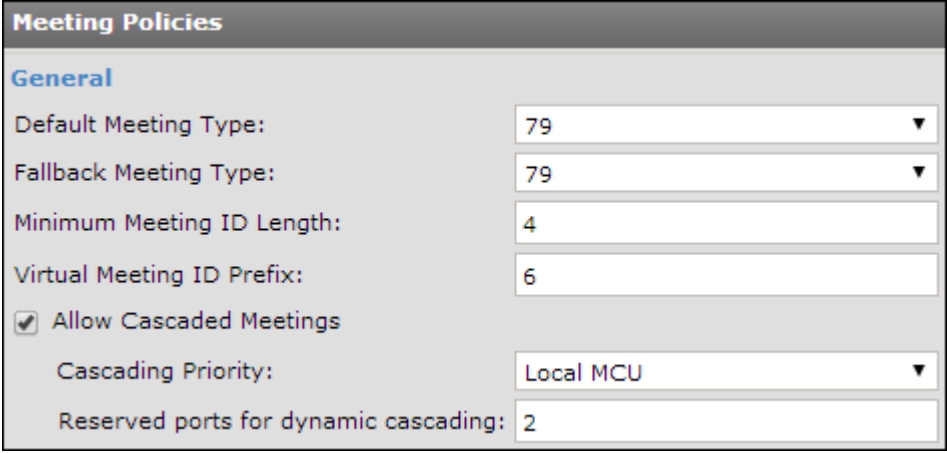
- The Meeting Type (MCU service) representing the required meeting must be available on all participating MCUs. For example, if the meeting uses MCU service 81, then 81 must exist on the master MCU and on the slave MCUs.
- A cascaded connection uses two ports—one on the master MCU, and one port on the slave MCU.
- Only one participant (typically the active speaker) connecting from each slave MCU can send video and be seen by other meeting participants in the video layout.
- Only one level of cascading is supported. All slave MCU conferences must cascade to the same master MCU conference.

- The lecturer and any telepresence endpoints must connect from the master MCU.
- Participants connecting to the slave MCU:
 - View only the default meeting layout
 - Can send and receive video with a resolution up to 720p (for Scopia® Elite 5000 Series MCU)
 - Perform actions (such as joining the meeting) via their endpoint or web interface, and not via DTMF.

For information about planning your MCU's topology, including bandwidth considerations and cascading MCUs, see *Administrator Guide for Scopia® Elite MCU*.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Meetings > Policies**.
3. Verify that **Allow Cascaded Meetings** is selected ([Figure 32: Configuring cascading settings](#) on page 71).



Meeting Policies	
General	
Default Meeting Type:	79 ▼
Fallback Meeting Type:	79 ▼
Minimum Meeting ID Length:	4
Virtual Meeting ID Prefix:	6
☒ Allow Cascaded Meetings	
Cascading Priority:	Local MCU ▼
Reserved ports for dynamic cascading:	2

Figure 32: Configuring cascading settings

4. Select one of the following options from the **Cascading Priority** list:
 - **Delay:** This is the default option. Scopia® Management allocates resources to ensure the best video quality and invites all users directly to a main MCU, whatever their location. Since the **Delay** option can be costly in terms of bandwidth, it is recommended that you take topology into account before selecting.
 - **Local MCU:** Select this option if Scopia® Management has more than one MCU and there are at least two meeting participants. Scopia® Management invites all of the participating endpoints to meetings hosted on their respective local MCUs (according to IP Topology settings), and then cascades these meetings together to form a single conference.
5. Enter the number of ports to reserve for cascaded meetings in the **Reserved Ports From Dynamic Cascading** field. By default, one port is reserved.

If you do not reserve ports, new participants automatically connect to the master MCU and when there are no more ports available on this MCU, new participating endpoints are rejected.

6. Select **Apply** to save the preferred behavior as the default.

Enabling Auto-Attendant Support

About this task

The Auto-Attendant feature provides quick access to meetings hosted on **Scopia® Elite** MCUs, allowing meeting participants to access a video menu and select menu options using DTMF. This procedure describes how to enable the Auto-Attendant feature in **Scopia® Management**. You must designate one meeting type for the Auto-Attendant. For more information about meeting types, including configuring its bandwidth and resolution, see [Downloading MCU Meeting Types to Scopia® Management](#) on page 62.

To enable the Auto-Attendant feature, you first configure a meeting type with Auto-Attendant support, and then configure the Auto-Attendant settings.

Before you begin

1. When integrating **Scopia® Solution** with the **Avaya Aura Conferencing** server, use the same number for both the **Avaya** and **Avaya Auto-Attendant**. You must also enable integration, as described in [Integrating the Avaya Aura Conferencing Server](#) on page 75.

2. Choose a number you want to assign to the Auto-Attendant feature.

The Auto-Attendant number must be different from the following numbers:

- All E.164 numbers of your organization's endpoints.
- MCU meeting type
- **Scopia® Gateway** service
- ECS zone prefix
- Auto-Route number

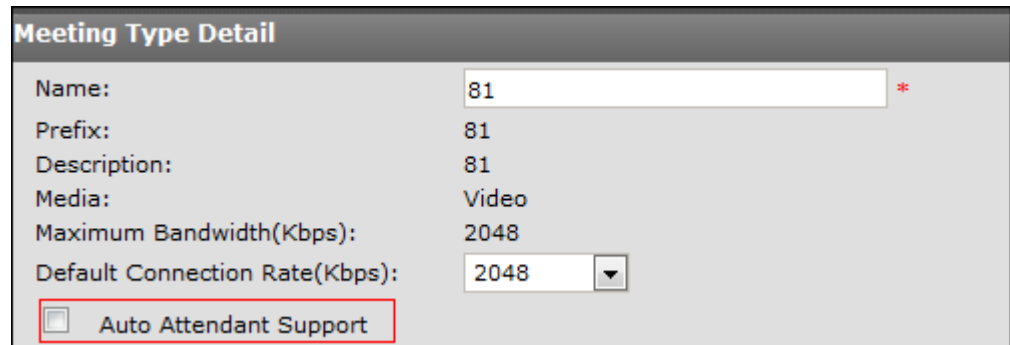
3. Synchronize the **Scopia® Elite** MCU's meeting types with **Scopia® Management**, as described in [Synchronizing MCU Meeting Types with Scopia® Management](#) on page 63.
4. If your deployment uses a third-party gatekeeper, ensure that the gatekeeper has a prefix configured to direct calls to the Auto-Attendant.
5. For **Scopia® Video Gateway** deployments only: Create an Active Directory user dedicated to the Auto-Attendant, to be displayed as a contact on Lync clients. Use the Auto-Attendant's URI when configuring the Auto-Attendant's settings in **Scopia® Management**.

Procedure

1. Access the **Scopia® Management** administrator portal.
2. Select the **Settings** tab.
3. Configure the meeting type for Auto-Attendant support, as follows:
 - a. Select **Settings > Meetings > Meeting Types**.

- b. Select the meeting type for which you want to configure Auto-Attendant support, from the **Name** column.

The **Meeting Type Details** page appears ([Figure 33: Configuring Auto-Attendant support for a meeting type](#) on page 73).



Meeting Type Detail

Name: 81 *

Prefix: 81

Description: 81

Media: Video

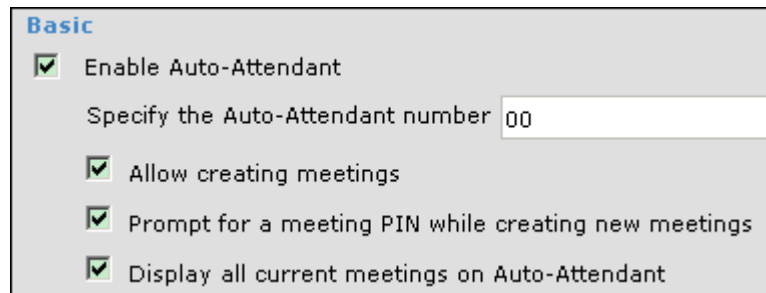
Maximum Bandwidth(Kbps): 2048

Default Connection Rate(Kbps): 2048 ▼

☒ Auto Attendant Support

Figure 33: Configuring Auto-Attendant support for a meeting type

- c. Select **Auto-Attendant Support**.
- d. Select **Apply**.
4. Configure settings for the Auto-Attendant, as follows:
- a. Select **Settings > Meetings > Auto-Attendant**.
- b. Select **Enable Auto Attendant**.



Basic

☒ Enable Auto-Attendant

Specify the Auto-Attendant number 00

☒ Allow creating meetings

☒ Prompt for a meeting PIN while creating new meetings

☒ Display all current meetings on Auto-Attendant

Figure 34: Enabling Auto-Attendant

- c. Configure the Auto-Attendant settings, as described in [Table 23: Configuring Auto-Attendant settings](#) on page 73.

Table 23: Configuring Auto-Attendant settings

Field Name	Description
Specify the Auto-Attendant Number	Assign an Auto-Attendant number to the meeting type you configured with Auto-Attendant support. For details on choosing a number for the Auto-Attendant, see the prerequisites above.
Allow creating meetings	Select to allow guests to create meetings by dialing the Auto-Attendant.

Field Name	Description
Prompt for a meeting PIN while creating new meetings	Select to prompt regular users to enter a meeting PIN when creating new meetings.
Display all current meetings on Auto-Attendant	Select to display all ongoing meetings on the Auto-Attendant.
Automatically route incoming calls according to schedule. Specify the Auto Route number	Select to route all meetings hosted by the MCU to the Auto-Attendant, and assign a unique auto-route number, which is used by the gatekeeper to route calls to the MCU. This number cannot be the same as any of the following: • Auto-Attendant number • MCU meeting type • Virtual room prefix • Scopia® Gateway service • ECS zone prefix

d. Select **Apply**.

5. For Scopia® Video Gateway deployments only, enable the Auto-Attendant contact to be displayed as a contact on your Lync client:

a. Select **Settings > Unified Communications > Microsoft Lync/OCS**.

Figure 35: Adding an Auto-Attendant user to Lync clients

b. Select **Enable Microsoft Lync Integration**.

c. Select **Enable "Auto Attendant" Contact**.

d. Enter the URI of the user you created for the Auto-Attendant in Active Directory, in the **Microsoft Lync Account** field.

The user's URI depends on the attributes configured in your LDAP directory. An example URI could be *Auto-Attendant@companyname.com*.

The Auto-Attendant user is displayed as a contact on Lync clients. When dialing the Auto-Attendant from your Lync, the Auto-Attendant welcome screen appears.

e. Select **Apply**.

Integrating the Avaya Aura Conferencing Server

About this task

You can extend **Scopia®** Solution videoconferences to include video and audio endpoints hosted by the Avaya Aura Conferencing (AAC) server.

This is a cost-effective approach, for example, when the conference includes many Avaya participants joining from an audio device. The AAC hosts Avaya endpoints, providing excellent audio quality to a large number of participants, and the **Scopia®** Elite MCU hosts the video participants.

! Important:

You can allow Avaya endpoints to join a **Scopia®** Solution videoconference directly, without connecting to the AAC server by defining the Avaya Session Manager as a SIP server (see [Adding a Lync Server, an OCS or a SIP Server in Scopia® Management](#) on page 53).

Perform the procedure below to integrate the AAC server into **Scopia®** Management. The MCU then automatically connects to the AAC server when the meeting starts, as long as this is supported by the meeting type (see [Modifying an MCU Meeting Type in Scopia® Management](#) on page 66 for details).

For more information about **Scopia®** Solution integration with Avaya, see the *Scopia® Solution Guide*.

! Important:

This is available for AAC version 7 and later.

Procedure

1. Access the **Scopia®** Management administrator portal.
2. Select **Settings > Unified Communications > Avaya Aura**.
The **Avaya Aura** page appears.

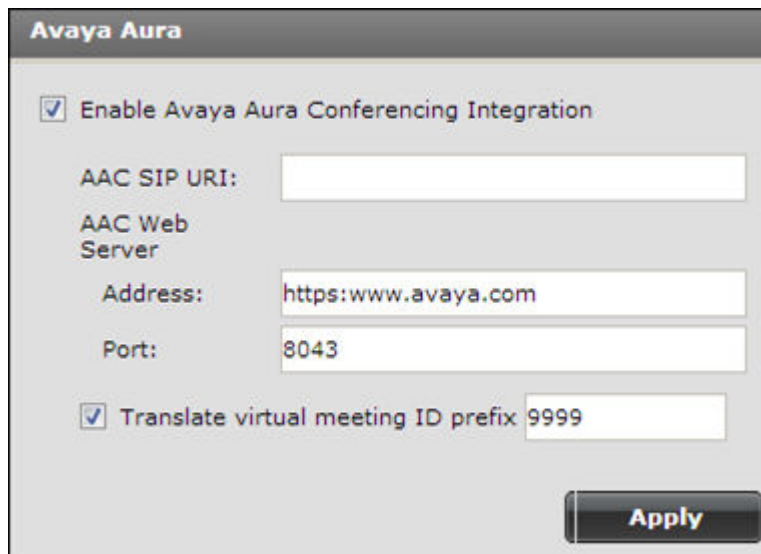


Figure 36: Integrating Avaya Aura Conferencing

3. Select **Enable Avaya Aura Conferencing Integration**.
4. Enter the settings as described in [Table 24: Integrating Avaya Aura Conferencing server](#) on page 76.

Table 24: Integrating Avaya Aura Conferencing server

Field Name	Description
AAC SIP URI	The URI dial string needed to reach the Avaya Aura Conferencing server. For example, <i>server_name@company.com</i> .
AAC Web Server Address	Enter the URL of the web server.
Port	Enter the port used to connect to the web server. By default, port 8043 is used.
Translate virtual meeting ID prefix	Depending on your dial plan, select to remove the prefix of the Scopia® Management virtual meeting ID from the meeting ID when connecting to the AAC server. If required by your dial plan, enter an alternative prefix to use. For example, if the prefix of the virtual meeting ID defined in Scopia® Management is 88, and is already in use in the AAC dial plan, you can define a different prefix such as 9999 here. This new prefix, 9999, will replace the one defined in Scopia® Management, 88, for Avaya endpoints.

5. Select **Apply**.

Planning and Configuring a Scopia® Desktop server in Scopia® Management

Scopia® Desktop is a client/server application that provides video conferencing to remote and desktop users. The Scopia® Desktop server acts as a gateway from Scopia® Desktop clients to the MCU and handles all media connections.

When adding and configuring Scopia® Desktop server in Scopia® Management, a web access URL is defined so users can simply click on a link to connect to a conference.

Adding and Modifying Scopia® Desktop server in Avaya Scopia® Management

About this task

The Scopia® Desktop server uses Scopia® Management to retrieve the list of users from the corporate directory, and also query information about current and scheduled meetings, including the participant names in a meeting. Scopia® Desktop server profiles are manually added to Scopia® Management.

Ensure that Scopia® Desktop server has Scopia® Management's IP address, and conversely Scopia® Management has Scopia® Desktop server's IP address. For more information on how to add Scopia® Management's IP address to the Scopia® Desktop server, see *Installation Guide for Scopia® Desktop server*.

Procedure

1. Access the Scopia® Management administrator portal.
2. In the **Devices** tab, select **Desktop Servers**.
3. Select the link in the **Name** column for the Scopia® Desktop server you require, or select **Add** to create a new Scopia® Desktop server profile. The **Add Scopia® Desktop server** page appears ([Figure 37: Adding a Scopia® Desktop profile](#) on page 77).

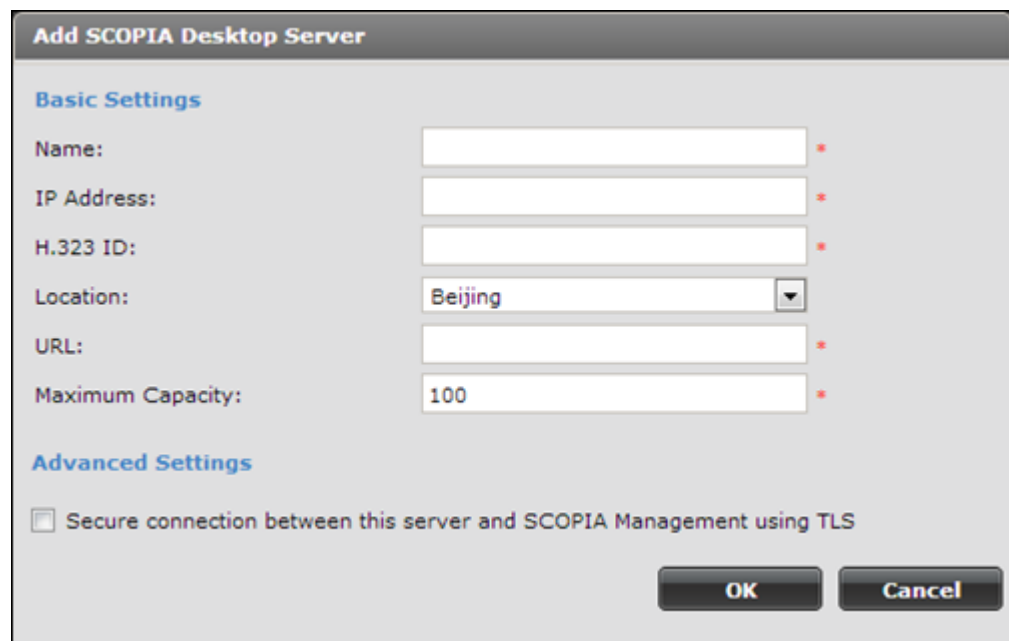


Figure 37: Adding a Scopia® Desktop profile

4. Enter the required information ([Table 25: Configuring Scopia® Desktop server](#) on page 78).

Table 25: Configuring Scopia® Desktop server

Field Name	Description
Name	Enter a name to identify this Scopia® Desktop server. This name is displayed in the list of Scopia® Desktop servers.
IP address	Enter the management IP address of Scopia® Desktop server.
H.323 ID	Enter the H.323 ID used to identify connections from Scopia® Desktop server in MCU conferences. This must match the H.323 ID that is configured in the Scopia® Desktop administrator web interface. Configuring this field allows Scopia® Management to route calls from this Scopia® Desktop server based on the predefined IP topology. The ID can have one of the following formats: • H.323 alias. For example, username. • IP address of an H.323 endpoint. For example, 123.45.678.9. • URI dialing for H.323 or SIP endpoints. For example, <i>user@company.com</i> • E.164 dialing for H.323 or SIP endpoints. For example, 881234.
Location	This is only relevant for deployments with multiple locations. Select the Scopia® Desktop server's location.
URL	Enter the URL used to access the Scopia® Desktop server. The URL must be in the format <i>http://<web URL>:<port number>/scopia</i> .
Maximum Capacity	Enter the maximum number of simultaneous connections you want to allow for your Scopia® Desktop server, based on computing power.
Secure connection between this server and Scopia® Management using TLS	To use the Transport Layer Security (TLS) protocol to secure the transport link between Scopia® Management and Scopia® Desktop, select this checkbox. For more information, see <i>Administrator Guide for Scopia® Management</i> .

5. Select **OK** to save your changes.

Planning and Configuring Gateways in Scopia® Management

Configure gateways in your network to enable non-H.323 endpoints, such as SIP, PSTN, ISDN, and mobile endpoints, to join a meeting. Scopia® Management uses the gateway information to provide proper dialing information for meeting participants, and to dial out to endpoints to invite them to meetings. In addition, Scopia® Management manages gateway resources to allow successful call scheduling using network gateways.

Navigation

- [Configuring the Avaya Scopia® TIP Gateway or Scopia® Video Gateway in Scopia® Management](#) on page 79

- [Configuring a Scopia® Gateway in Scopia® Management](#) on page 82
- [Registering a Gateway with a Gatekeeper](#) on page 86

Configuring the Avaya Scopia® TIP Gateway or Scopia® Video Gateway in Scopia® Management

About this task

This section explains how to configure the Avaya Scopia® SIP Gateway, Avaya Scopia® TIP Gateway or Scopia® Video Gateway settings in Scopia® Management.

Since the Scopia® Gateway does not have its own web interface, its configuration is performed in Scopia® Management.

Scopia® Management and gateways communicate in XML over TCP for control and configuration commands. You can secure the connection by configuring it to the TLS protocol. Make sure to generate the Avaya Scopia® Management and Scopia® Gateway certificates before configuring the connection to TLS (see [Securing Your Video Network Using TLS](#) on page 139).

Important:

If your deployment consists of multiple Scopia® Management servers, configure both Scopia® Management servers before configuring the TLS connection for Scopia® Video Gateway.

Scopia® Video Gateway is configured by default to switch to the presentation channel whenever an H.323 endpoint shares content during a video call by sending the shared content to the Lync client. If this feature does not suit the needs of the video call, you can disable it in Scopia® Management.

Before you begin

1. In Microsoft deployments, perform this procedure after your Microsoft Lync Server or Microsoft Office Communications Server is configured. For more information on adding a Lync Server or OCS profile to Scopia® Management, see [Adding a Lync Server, an OCS or a SIP Server in Scopia® Management](#) on page 53.
2. Add the Scopia® Gateway to Scopia® Management by entering its basic settings, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices > Devices by Type > Gateways**.
3. Select the Scopia® Gateway you are configuring.
4. Select the **Configuration** tab.

The screenshot shows the 'Configuration' tab of the Scopia Gateway interface. It contains several sections: 'Basic Settings' with fields for Name (SIPGW), Secure XML connection using TLS (unchecked), In Maintenance (unchecked), Registration Name (SCOPIA UCGW-...), Meeting Type Prefix (92), Service Encryption (Best effort), and Secure connection using HTTPS (unchecked); 'SIP Settings' with fields for SIP Proxy Server, Transport Type (TCP), Default SIP Domain (mcu.mycompany.com), and STUN/TURN Server; 'H.323 Settings' with fields for Required Gatekeeper (local_gatekeeper), Current Gatekeeper, and Location (Home); 'NTP Settings' with fields for NTP IP Address, NTP Time Zone (GMT-12:00); and 'Network Settings' with fields for MTU Size (1361), DNS Server 1, DNS Server 2 (0.0.0.0), Quality Of Service (Customized), and QoS Priority (Control: 26, Audio: 46, Video: 34). A red box highlights the 'Advanced Parameters' button at the bottom left.

Figure 38: Configuring the gateway

5. Configure the Scopia® Gateway settings as described in [Table 26: Configuring settings for the Scopia® Gateway](#) on page 80.

Table 26: Configuring settings for the Scopia® Gateway

Field Names	Description
Name	You can modify the name that identifies the Scopia® Gateway in Scopia® Management.
Secure XML Connection using TLS	If required, select to use TLS and thus secure the exchange of XML messages and commands between the Scopia® Gateway and Scopia® Management. ! Important: Before selecting TLS, you must generate the Avaya Scopia® Management and Scopia® Gateway certificates. After you select that checkbox, click Test Connection.
Registration Name	The name of this Scopia® Gateway is automatically generated by the system.
Meeting Type Prefix	The prefix to dial to access this gateway.
Secure connection using HTTPS	Select this setting to encrypt the communication between the gateway and the Scopia® Management. Before selecting HTTPS, you must generate the Scopia® Gateway certificates.

Field Names	Description
Required Gatekeeper	The gatekeeper to which you want to register the Scopia® Gateway.
Current Gatekeeper	This (read-only) field displays the management IP address of the gatekeeper this Scopia® Gateway is currently registered to. In most cases, this is the same gatekeeper selected in the Required Gatekeeper field. If the current gatekeeper is not the same as the gatekeeper configured in Required Gatekeeper , an alarm is issued by Scopia® Management.
Location	If there is more than one location in your deployment, assign your gateway to a location by selecting an option from the list.
SIP Proxy Server	The IP of the SIP Server for this gateway. Typically Scopia® Management acts as the SIP server.
STUN/TURN Server	The IP of the STUN/TURN Server for this gateway.
Transport Type	The default setting is TCP. Choose TLS for encrypted communications with the SIP server. TLS requires correctly issued certificates from a CA for the gateway and the SIP server.
Default SIP Domain	The SIP domain of your organization.
NTP IP Address	The IP address of a Network Time Protocol server which sets the time for the gateway's clock. External NTP servers ensure the same clock throughout all devices on the network. If you have no NTP server, enter 0.0.0.0 .
NTP Time Zone	The time zone of the NTP server.
MTU size	The size of the packets received from the gateway. Only change this if a router uses a non-standard MTU size.
DNS Server 1, 2	The IP address(es) of the organization's DNS server(s).
Quality of Service	Typically this setting remains on Default . You can customize the priority given to the different elements of the gateway communication if required.
QoS Priority	Enter a number from 1-100 to represent the relative priority of audio, video, and signaling and control data. During low-bandwidth conditions, Scopia® Management uses these priority settings to adjust the quality of the meeting.

6. Select **Apply**.
7. Allow Scopia® Management to access the Scopia® Gateway:
 - a. Select the **Access** tab.

- b. Enter the login name and password of the Scopia® Gateway. The default username is **admin** and the default password is **password**.
 - c. Select **Apply**.
-

Configuring a Scopia® Gateway in Scopia® Management

About this task

Gateways extend your video capabilities to include protocols outside of your main video network. The Scopia® Gateway, for example, extends your H.323-based network to include ISDN endpoints.

Scopia® Management keeps track of the gateway's available ports to enable the successful scheduling of calls.

When you add a gateway, the settings in Scopia® Management must be consistent with the configuration of the gateway device itself. This includes specifying all the services on that gateway.

A service maps a numeric dial prefix to a type of call. When the gateway receives a call with the designated prefix, it determines the properties of that call:

- Whether it is voice only or video, and
- The bandwidth allocated for this kind of call.

This procedure details how to configure a gateway to the Scopia® Management, including detailing the gateway's services.

Important:

This is relevant only to Scopia® Gateway.

Before you begin

Add the gateway to Scopia® Management by entering its basic settings, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select the gateway you are configuring.
4. Select the **Configure** tab.

Gateway: B40GW

Info | **Configure** | Alarms | Events | Access

Basic Settings

Name: B40GW * IP Address: 168.168.227.110 *

Model: RADVISION GW-B40 (4 BR1) Registered To: local_gatekeeper (127.0.0.1) *

Location: Beijing * Current Gatekeeper: 168.168.230.61

☐ In Maintenance

Operations

Bandwidth (Kbps) : 4096 * Description: B40GW

International Access Code: 00 * Country Code: 86 * ☒ Allow out of area calls

Domestic Long Distance Prefix: 0 Area Code: 10 * ☐ Always dial area code for calls within the same area

Telephone Number: 85283976 *

For local calls, dial: 7

For long distance calls, dial: 7

Service

☐ Gateway is in restricted mode

Meeting Type Prefix	Bandwidth(Kbps)
☐ 40 *	64 voice

☐ DID Working Mode

Advanced Settings

Signaling Port: 1820 ☐ Dial in only

Figure 39: Configuring the gateway

5. Enter the gateway settings in Scopia® Management. The settings must be consistent with the configuration of the gateway device itself.

Field Name	Description
Name	(Optional) Modify the name of the gateway.
Model	(Read-only) Displays the type of gateway.
Registered To	Select the gatekeeper to which the gateway is registered.
Location	If there is more than one location in your deployment, assign your gateway to a location by selecting an option from the list.
IP Address	(Read-only) Displays the IP address of the management stream of the gateway. Scopia® Management communicates with the gateway via its management stream, and does not need the media stream if different. If multiple gateways are pooled together in a local network with the same access phone number, all IP addresses are separated by a semi-colon (;).

Field Name	Description
Bandwidth	The total bandwidth allocated to this gateway. For example, for an E1 line or 30 B-channels, the bandwidth is $64 \times 30 = 1920$ Kbps per network interface. For gateways with two PRI interfaces, the total bandwidth would be $1920 \times 2 = 3840$ Kbps. If multiple gateways are pooled together in a local network with the same access phone number, enter the bandwidth of a single gateway unit in the pool.
IVR	Choose if the gateway routes calls using an Interactive Voice Response (IVR) system. For more information see the gateway documentation.
DID	Choose if call routing is direct to an endpoint without operator intervention using Direct Inward Dialing. For more information see the gateway documentation.
Description	A description of the phone number for the gateway.
International Access Code	The numeric dial prefix required to make an international call.
Country Code	The numeric dial prefix to dial a terminal located in a different country than the country.
Domestic Long Distance Prefix	The numeric dial prefix required to make a long distance call within the same country.
Allow Out of Area Calls	If selected, endpoints can reach Scopia® Management via the gateway even when they have a different area code to that of the gateway.
Area Code	The domestic area code of the gateway number.
Telephone Number	A local telephone number to be assigned to the specific port.
For local calls, dial:	The dial prefix required for the gateway to access an outside line.
For long distance calls, dial:	The dial prefix required for the gateway to make a long distance call.

6. Select **Add** in the **Service** area to create an additional service entry for this gateway. You can add multiple services. The list of services must be identical to the services on the gateway itself.

A service maps a numeric dial prefix to a type of call. When the gateway receives a call with the designated prefix, it determines the properties of that call:

- Whether it is voice only or video, and
- The bandwidth allocated for this kind of call.

7. For each service, enter the field values as required:

Table 27: Adding a service

Field Name	Description
Meeting Type Prefix	The numeric dial prefix used by the gateway to identify this meeting type.
Bandwidth	The properties of this service, both bandwidth and whether it is voice only or video. Choose from a predefined list. If this service's bandwidth is set to Auto on the device itself, in Scopia® Management enter the average bandwidth endpoints use when dialing that service.
Gateway is in restricted mode	Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.

8. Configure the advanced settings.

Table 28: Defining advanced settings

Field Name	Description
Signaling Port	The gateway port used for signaling. Leave this field blank to negotiate the signaling port dynamically.
Dial-in Only	Indicates the gateway is used for incoming calls only. Scopia® Management would not schedule outgoing calls on this gateway.

9. Select **Apply** to save your changes.
10. Select the **Access** tab and enter the Scopia® Gateway's information to enable encrypted SNMP communications between the gateway and Scopia® Management, as described in [Table 21: Configuring the MCU's access information](#) on page 61.

Table 29: Configuring the Scopia® Gateway's access information

Field Name	Description
Username Password	Enter the login username and password of the gateway web interface login.
SNMP Read Community SNMP Write Community	Scopia® Management displays the names of the SNMP communities that support the read and write operations of SNMP management in your network. Both the gateway and Scopia® Management support sending and receiving SNMP alerts to track the gateway's behavior and handle any errors which may occur. SNMP community information must match the settings defined in the gateway to enable Scopia® Management to retrieve information from the gateway.  Important: The community values are case-sensitive.

11. Select **Apply**.

Registering a Gateway with a Gatekeeper

About this task

Gatekeepers, which maintain the register of aliases in a video network, sometimes include endpoints working under a different network protocol, and therefore must be routed through a gateway. Gateways bridge between the H.323 protocol and other video protocols, like ISDN.

Therefore the gatekeeper must register a network's gateways, to ensure safe call routing across different protocols.

Procedure

1. Access the Avaya Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select the gateway you are configuring.
4. Select the **Configure** tab.

Gateway: B40GW

Info **Configure** **Alarms** **Events** **Access**

Basic Settings

Name: B40GW * IP Address: 168.168.227.110 *

Model: RADVISION GW-B40 (4 BR1) Registered To: local_gatekeeper (127.0.0.1) *

Location: Beijing * Current Gatekeeper: 168.168.230.61

☐ In Maintenance

Operations

Bandwidth (Kbps) : 4096 * Description: B40GW

International Access Code: 00 * Country Code: 86 * ☒ Allow out of area calls

Domestic Long Distance Prefix: 0 Area Code: 10 * ☐ Always dial area code for calls within the same area

Telephone Number: 85283976 *

For local calls, dial: 7

For long distance calls, dial: 7

Service

Add **Delete** ☐ Gateway is in restricted mode

Meeting Type Prefix	Bandwidth(Kbps)
☐ 40 *	64 voice

☐ DID Working Mode

Advanced Settings

Signaling Port: 1820 ☐ Dial in only

Apply **Cancel**

Figure 40: Registering a Gateway with a gatekeeper

5. Select the gatekeeper to register your gateway from the **Required Gatekeeper** list.
6. Select **Apply**.

Remotely Configuring Avaya Scopia® PathFinder server

About this task

Avaya Scopia® PathFinder provides a complete firewall and NAT traversal solution enabling secure connectivity between enterprise networks and remote sites.

You can remotely monitor and configure the Avaya Scopia® PathFinder server by accessing its web interface from Scopia® Management.

See the *Deployment Guide for Avaya Scopia® PathFinder* for information on the device's configuration.

Before you begin

Add Avaya Scopia® PathFinder server to Scopia® Management as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select **PathFinders** in the sidebar.
The **Avaya Scopia® PathFinders** page opens.
4. Select the name of the relevant Avaya Scopia® PathFinder server in the list of devices.
The Avaya Scopia® PathFinder window opens.
5. To modify the Avaya Scopia® PathFinder server's **IP Address** , select **Info > IP Address > Change** and then enter the new IP address.
6. Select the **Configure** tab.

The screenshot shows the 'PathFinder: 168.168.225.51' configuration window. The 'Configure' tab is selected, displaying various settings sections:

- Basic Settings**
 - Name: 168.168.225.51
 - Location: BJ
- Collaborator Access**
 - Login Name: huan
 - Login Password: ****
- SSH & SFTP Access**
 - SSH/SFTP Login Name: admin/uadmin
 - Login Password: *****
- HTTP Access**
 - Login Name: admin
 - Login Password: *****
 - Port: 8080

At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 41: Configuring the Avaya Scopia® PathFinder server

7. Configure the Avaya Scopia® PathFinder server's settings, as described in [Table 30: Configuring the Avaya Scopia® PathFinder server's basic information](#) on page 89.

See the *Avaya Scopia® PathFinder Deployment Guide* for more information on the server configuration.

Table 30: Configuring the Avaya Scopia® PathFinder server's basic information

Field Name	Description
Name	If it was changed in the deployment only, modify the name of the Avaya Scopia® PathFinder server. We recommend to use the same name across all the deployment.
Location	If it was changed in the deployment only, modify the location of your Avaya Scopia® PathFinder server in the deployment.
Collaborator Access: Login Name Login Password	Enter the collaborator's username and password, required to send XML API requests to the Avaya Scopia® PathFinder server. The account details must match those defined for the collaborator on Avaya Scopia® PathFinder server. By default, the collaborator's Login Name is Collab , and Login Password is balloC .
SSH & SFTP Access: SSH/SFTP Login Name Login Password	An SSH client is required for accessing the shell administration menu of Avaya Scopia® PathFinder server, and an SFTP client is required for uploading or downloading resources of Avaya Scopia® PathFinder server. Enter the password required to access the SSH and SFTP clients. The default password is admin . The SSH/SFTP Login Name is predefined and cannot be modified.
HTTP Access: Login Name Login Password	Enter the username and password required to access the Avaya Scopia® PathFinder server web interface. By default, the Login Name is admin , and Login Password is admin .
Port	Enter the firewall Port number for HTTP access. The default value is 8080.

8. Select **Apply**.

Planning and Configuring Endpoints in Scopia® Management

Scopia® Management supports both Avaya and third-party endpoints. After importing endpoints to Scopia® Management, you can configure Scopia® Management to manage your endpoints. The main management tasks include the following, depending on the endpoint type:

- Simultaneously upgrading all endpoints (of the same type).
- Controlling your endpoint's bandwidth.
- Configuring your endpoint's resolution settings.
- Configuring your endpoints to display the corporate address book, as described in [Using Scopia® Management's Endpoint Directory as a Corporate Address Book](#) on page 118.
- Monitoring your endpoints via alarms and traps sent by Scopia® Management.

Every dedicated endpoint requires a license to join a videoconference and to be defined and managed by Scopia® Management (see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22).

You can configure Scopia® Management to manage the following endpoint types: Polycom, Tandberg, and LifeSize (see [Managing Endpoints using Scopia® Management](#) on page 113.)

You can import endpoints to Scopia® Management in the following ways (see [Figure 42: Importing endpoints into Scopia® Management](#) on page 91):

- Import from the H.350 search base: Use this method for endpoints that are defined in your LDAP server and your LDAP server is configured with an H.350 search base.
- Import from the LDAP server: Use this method when your H.323 endpoints are defined in your LDAP server and your LDAP server is not configured with an H.350 search base.
- Import from the gatekeeper: Use this method to import H.323 endpoints registered to your gatekeeper.
- Add endpoints manually: Use this method to import SIP, ISDN/PTSN, Dual H.320 and H.323, and H.323 endpoints. Endpoints imported manually are automatically managed by Scopia® Management.

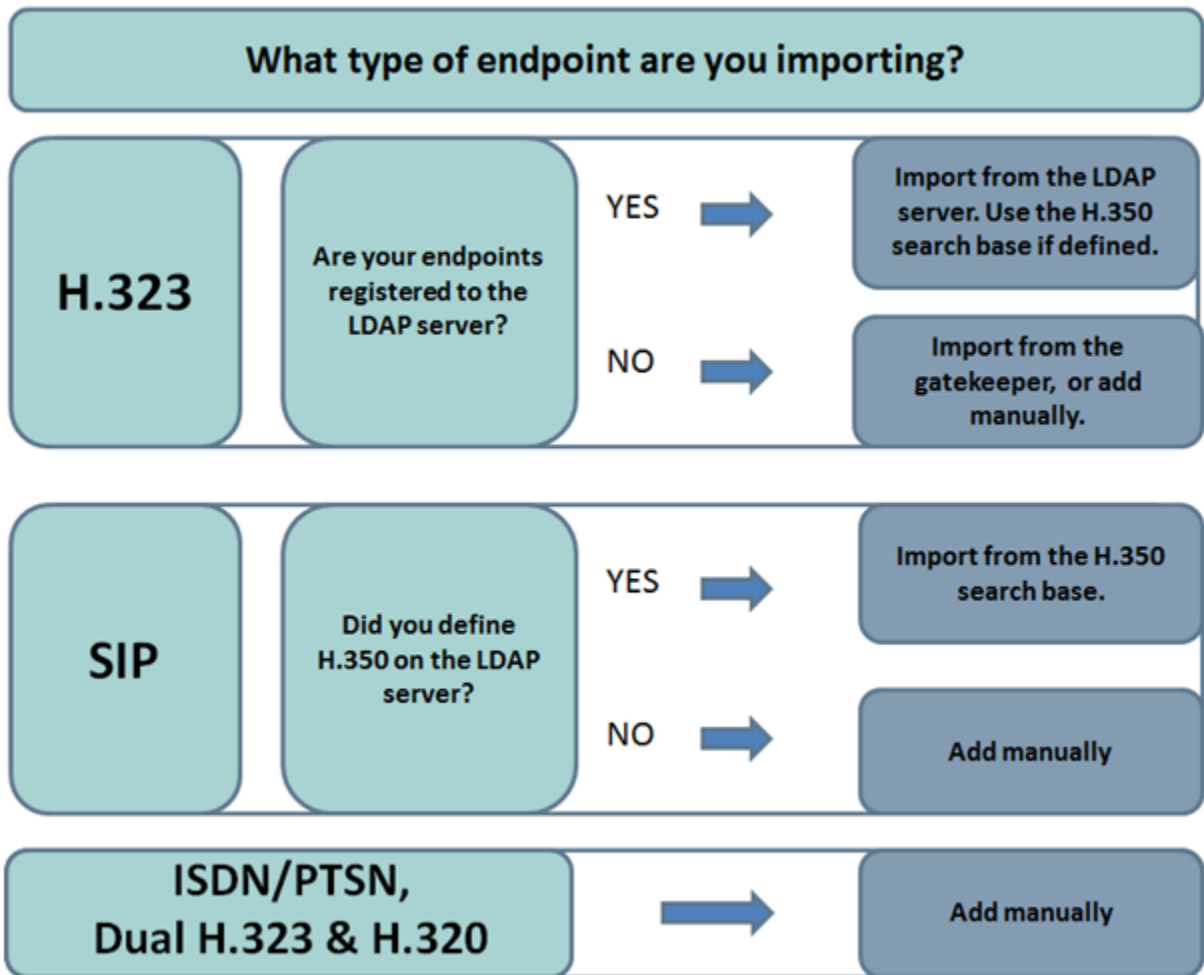


Figure 42: Importing endpoints into Scopia® Management

Navigation

- [Importing H.323 Endpoints from the Gatekeeper](#) on page 91
- [Importing H.323 Endpoints from an External LDAP Server](#) on page 94
- [Importing Endpoints from the H.350 Search Base](#) on page 97
- [Adding Endpoints in Scopia® Management Manually](#) on page 99
- [Planning and Configuring Telepresence in Scopia® Management](#) on page 111
- [Managing Endpoints using Scopia® Management](#) on page 113
- [Replicating Endpoint Settings on Multiple Endpoints](#) on page 115
- [Using Scopia® Management's Endpoint Directory as a Corporate Address Book](#) on page 118
- [Managing your Endpoint's User Directory with LDAP](#) on page 120
- [Configuring Presentation Layouts for Single-Screen Endpoints](#) on page 127
- [Organizing Endpoints into Groups with Labels](#) on page 129

Importing H.323 Endpoints from the Gatekeeper

About this task

This procedure describes how to import endpoints registered to Avaya Scopia® ECS Gatekeeper, Avaya Scopia® Gatekeeper (Scopia® Management's internal gatekeeper), or third-party gatekeepers to Scopia® Management.

Avaya Scopia® XT Series and Scopia® VC240 endpoints imported from the gatekeeper are automatically managed by Scopia® Management as long as there are enough Scopia® Named Endpoint licenses in the system.

Follow this procedure when:

- You want to import multiple or all endpoints registered to the gatekeeper.
- You want all Avaya Scopia® XT Series and Scopia® VC240 endpoints to be automatically managed by Scopia® Management.

Managed endpoints communicate with Scopia® Management to provide events and alarms management, and store endpoint information. Endpoints that are not managed by Scopia® Management only have basic endpoint dialing information needed to call or invite the endpoint to meetings. For more information about managed endpoints, see [Managing Endpoints using Scopia® Management](#) on page 113.

Before you begin

If you are importing endpoints from Avaya Scopia® ECS Gatekeeper or a third-party gatekeeper, you must first define the gatekeeper, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

If you are using Avaya Scopia® Gatekeeper, Scopia® Management's internal gatekeeper, you do not need to define it before importing endpoints.

Verify that you have sufficient Scopia® Named Endpoint licenses in the system, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

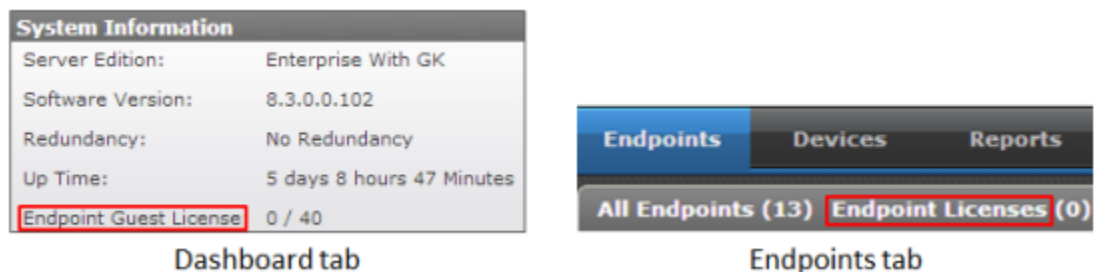


Figure 43: Checking the number of available Scopia® Named Endpoint

Procedure

1. Access the Scopia® Management web interface.
2. Select the **Endpoints** tab.
3. Select **Add > Import from Gatekeeper**. A gatekeeper list is displayed.

Select	Gatekeeper Name	Gatekeeper Location
☐	HKECS	HongKong
☐	local_gatekeeper	Beijing
☐	TBG_VCS_GK	HongKong

OK Cancel

Figure 44: Selecting the gatekeeper

4. Select the gatekeeper whose endpoints you would like to import, and select **OK**. A list of all endpoints registered to the gatekeeper that are not already in Scopia® Management is displayed.

Select	Name	Location	Bandwidth (Kbps)	E.164 Number	Visible in the directory of other endpoints
--------	------	----------	------------------	--------------	---

OK Cancel

Figure 45: Selecting the endpoints

5. Select the endpoints you want to import.
6. Configure settings for each selected endpoint, as described in [Table 31: Configuring endpoint settings](#) on page 94.

! Important:

The endpoint's dialing information (E.164 number) and location (relevant for distributed deployments) are retrieved from the gatekeeper.

XT Series and Scopia® VC240 endpoints are automatically managed by Scopia® Management.

Table 31: Configuring endpoint settings

Field Name	Description
Name	The endpoint's name appears, as it is configured in the gatekeeper. If necessary, you can modify the endpoint's name as it is displayed in Scopia® Management.
Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Scopia® Management uses the bandwidth value to reserve resources for this endpoint.
Visible in the directory of other endpoints	To display this endpoint in the corporate address book, select Display from the list.

7. Select **OK**.

A confirmation page appears, listing the endpoints that were added to Scopia® Management. These endpoints are now listed in the **Endpoints** tab.

 Important:

If any endpoints were not successfully imported, they appear in the list as well, with an explanation of why the import failed.

Importing H.323 Endpoints from an External LDAP Server

About this task

This procedure describes how to import H.323 endpoints from your external LDAP server. Endpoints are predefined in the LDAP server and can be imported to Scopia® Management as room systems and personal endpoints. Follow the procedure described below when:

- Your endpoints are defined in your LDAP server and your LDAP server is not configured with an H.350 search base. If your LDAP server is configured with an H.350 search base, follow the procedure described in [Importing Endpoints from the H.350 Search Base](#) on page 97.
- You are importing endpoints from the LDAP server for the first time. After this initial import, you can add endpoints by just synchronizing Scopia® Management with the LDAP server.
- You want to synchronize only endpoints, and not users, in your LDAP directory with Scopia® Management.

To synchronize both users and endpoints in your LDAP server, see [Synchronizing Users from the LDAP Server](#) on page 177.

- You are modifying the endpoints' import settings, such as the E.164 dialing number.

During this procedure you can define a prefix for endpoints you import (this is optional). The prefix is like an area code which is added to the start of a phone number. In this case, the prefix helps to route a call to a specific endpoint.

The following is relevant for Scopia® Video Gateway deployments:

- The LDAP Server is your Active Directory Server.
- When an endpoint is registered to ECS, Avaya Scopia® Gatekeeper, or Tandberg VCS, the status of the endpoint is visible in Lync clients.
- If imported endpoints are registered to any other gatekeeper, their status is not displayed on Lync clients.

Before you begin

1. Define your LDAP server in Scopia® Management, as described in [Connecting Scopia® Management with the LDAP Server](#) on page 172.
2. Synchronize your LDAP server with Scopia® Management.

Otherwise, personal endpoints belonging to users recently added to the LDAP but not listed in Scopia® Management, are not imported to Scopia® Management.

Verify that you have sufficient Scopia® Named Endpoint licenses in the system, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

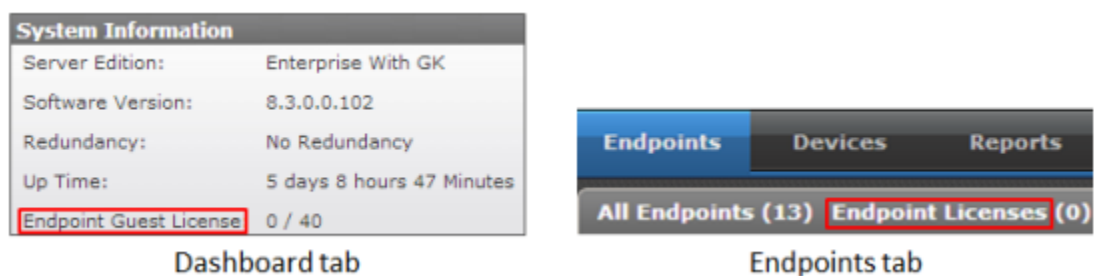


Figure 46: Checking the number of available Scopia® Named Endpoint

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** tab.
3. Select **Add > Import from LDAP**, and select the LDAP server's IP address from the list.
4. Select the type of endpoint you are importing, as follows:
 - **Room system**: Select this option if you are importing room system endpoints.
 - **Personal endpoint**: Select this option if you are importing personal endpoints.

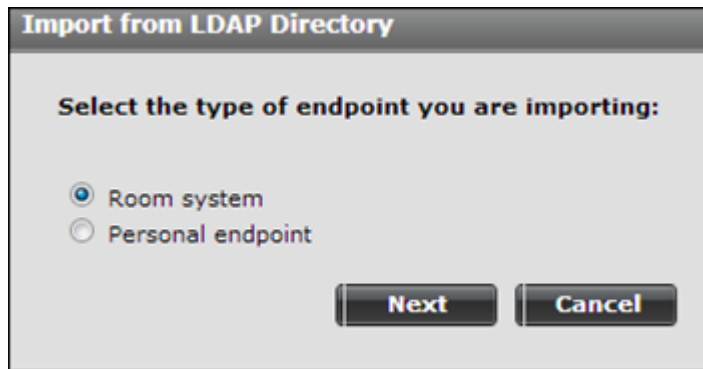


Figure 47: Selecting the endpoint type

5. Select **Next**.
6. Select the user group to which you want to assign personal endpoints or import room systems.
7. Select **Next**.

The **Import from LDAP Directory** window opens.

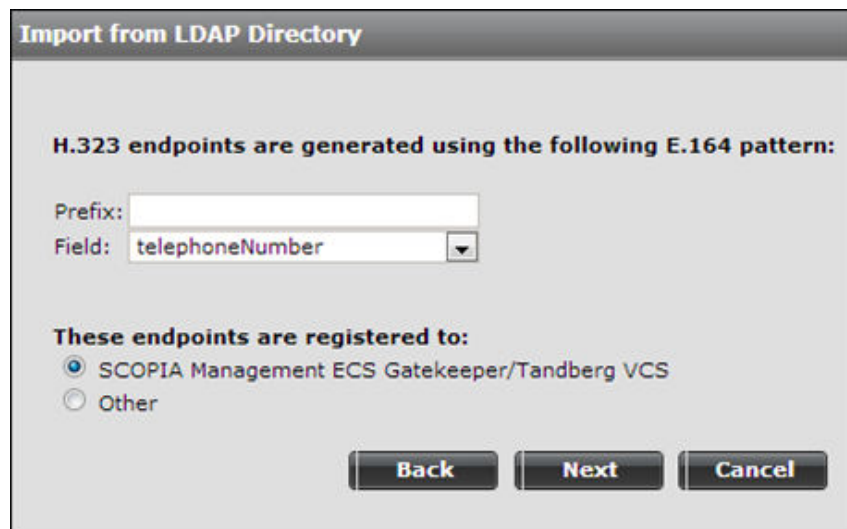


Figure 48: Configuring import settings for these endpoints

8. Configure the endpoints or room systems, as described in [Table 32: Configuring import settings for these endpoints](#) on page 97.

Table 32: Configuring import settings for these endpoints

Field Name	Description
Prefix	If required by your dialing plan, enter a number to use for a prefix for these endpoints, according to the following guidelines: • Must contain less than 11 digits • Cannot already be used as a prefix for the auto-attendant, auto-routing, or for other deployment components. • Personal endpoints cannot have the same prefix as personal virtual rooms, when configuring the same LDAP attribute (such as telephoneNumber).
Field	Select the LDAP attribute you want to use to retrieve the endpoint's information from the LDAP server, depending on your organization's dialing plan. The most commonly used attribute is telephoneNumber .  Important: Do not select non-numerical attributes, such as streetAddress or OU .
Those endpoints are registered to	Select the gatekeeper the endpoints are registered to.

9. Select **Next > Finish**.

The endpoints are added to Scopia® Management.

10. Verify that endpoints were downloaded correctly:
- a. Select **Endpoints > Imported Endpoints > From Active Directory**.
 - b. Verify that all endpoints defined in the LDAP server were downloaded and appear in the **Endpoints** tab.

Importing Endpoints from the H.350 Search Base

About this task

This procedure describes how to import endpoints using your LDAP server's H.350 search base. The H.350 search base allows you to search your LDAP database for users based on videoconferencing-specific attributes. Follow the procedure described below when:

- Your endpoints are defined in your LDAP server and your LDAP server is configured with an H.350 search base.
- You are importing endpoints from the H.350 search base for the first time. After this initial import, you can add endpoints by just synchronizing Scopia® Management with the LDAP server.

Before you begin

1. Define your LDAP server in Scopia® Management, as described in [Connecting Scopia® Management with the LDAP Server](#) on page 172.
2. Define a schema with specific user attributes to be imported from the LDAP server to Scopia® Management on your LDAP server. For example, you can define the type of endpoint to be imported, or you can define a schema to import endpoints with a specific video profile. In addition, you can define new fields in the LDAP server to add more endpoint details.

Verify that you have sufficient Scopia® Named Endpoint licenses in the system, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

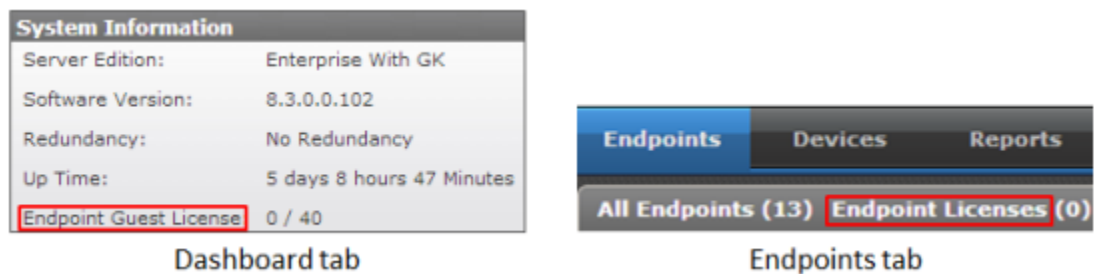


Figure 49: Checking the number of available Scopia® Named Endpoint

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Endpoints**.
3. Select **Add > Import from H.350**.

A tree structure is displayed showing all the organizational units (OU) defined on the LDAP server:

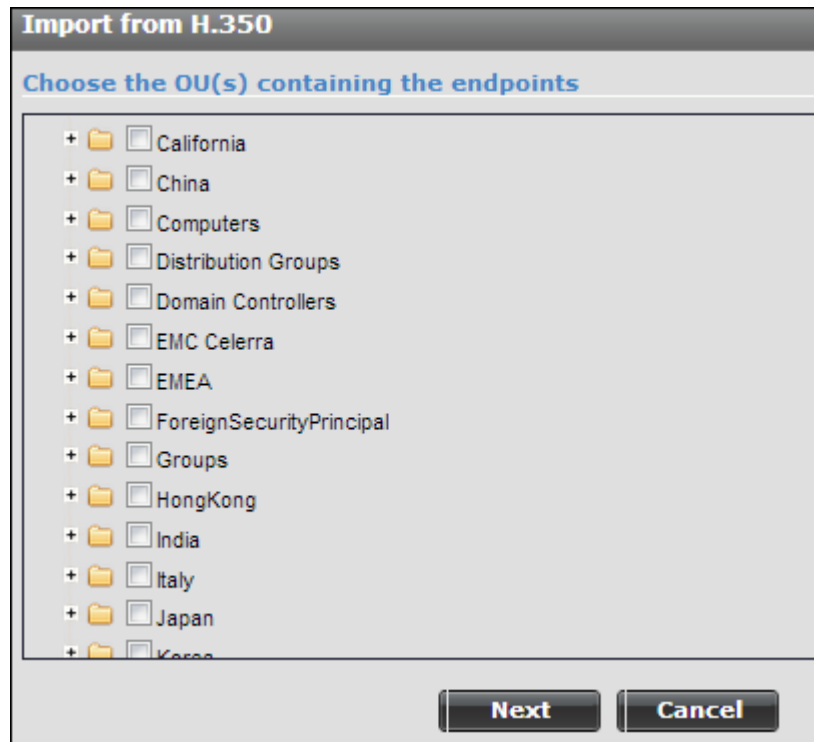


Figure 50: Importing endpoints from the H.350 search base

4. Select the relevant organizational units (OU) where your endpoints are defined.
5. Select **Next**.
6. Select **Finish**.

Adding Endpoints in Scopia® Management Manually

You can manually add H.323, SIP, ISDN/PSTN H.320, Dual H.320/H.323 endpoints to Scopia® Management. Endpoints imported manually are automatically managed by Scopia® Management. Add endpoints manually when:

- You are adding SIP, ISDN/PSTN H.320, or Dual H.320/H.323 endpoints. If your LDAP server is configured with an H.350 search base, you can import the endpoints as described in [Importing Endpoints from the H.350 Search Base](#) on page 97. Otherwise, you can only add these types of endpoints manually.

H.323 endpoints can be added manually or imported from the gatekeeper, your LDAP server, or the H.350 search base.

- You are adding endpoints that you want automatically managed by Scopia® Management.

Managed endpoints communicate with Scopia® Management to provide events and alarms management, and store endpoint information. Endpoints that are not managed by Scopia® Management only have basic endpoint dialing information needed to call or invite the endpoint to meetings. For more information about managed endpoints, see [Managing Endpoints using Scopia® Management](#) on page 113.

Every dedicated endpoint (other than ISDN and mobile) requires a license to join a videoconference and to be managed by Scopia® Management (see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22).

Add endpoints to Scopia® Management manually, as described in the following procedures:

Navigation

- [Adding H.323 IP Endpoints](#) on page 100
- [Adding SIP IP Endpoints](#) on page 102
- [Adding Telepresence Systems in Scopia® Management](#) on page 104
- [Adding ISDN/PSTN H.320 Endpoints](#) on page 109
- [Adding Mobile Endpoints](#) on page 110

Adding H.323 IP Endpoints

About this task

This procedure describes how to manually import H.323 endpoints registered to gatekeepers that are configured in Scopia® Management.

Before you begin

If you are adding endpoints registered to Avaya Scopia® ECS Gatekeeper or a third-party gatekeeper, you must first define the gatekeeper, as described in [Adding Video Network Devices in Scopia® Management](#) on page 44.

If you are using Avaya Scopia® Gatekeeper, Scopia® Management's internal gatekeeper, you do not need to define it before importing endpoints.

Verify that you have sufficient Scopia® Named Endpoint licenses in the system, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

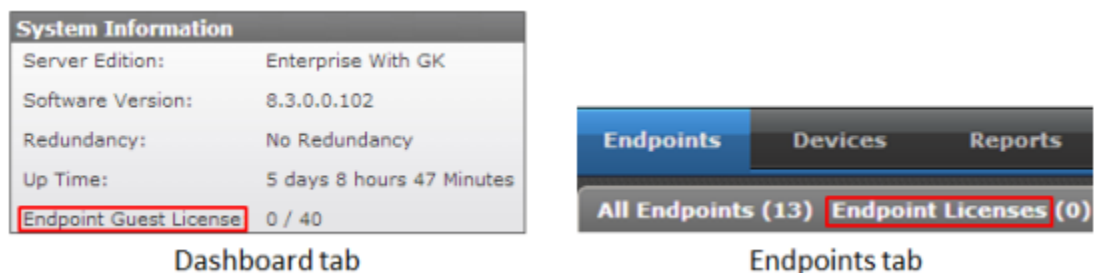


Figure 51: Checking the number of available Scopia® Named Endpoint

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** tab.
3. Select **Add > Add manually**.

The **Add Endpoint** dialog box appears.

Add Endpoint

Name: *

Description:

Type: Single Codec Endpoint

Protocol: IP (H.323)

E.164/IP Address: *

Registered To: local_gatekeeper (127.0.0.1)

Location: Beijing *

Max IP Bandwidth: 2048 * Kbps

☒ Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile)

☐ VIP Endpoint (experience will not be downgraded during call)

☐ Presence

☐ Manage (upgrade and configure) this endpoint

☐ Has Embedded MCU

OK Cancel

Figure 52: Adding H.323 endpoints

4. Configure your endpoint as described in [Table 33: Adding H.323 endpoints](#) on page 101.

Table 33: Adding H.323 endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter any description text that you may have for this endpoint.
Type	Select the model of the endpoint.
Protocol	Select IP(H.323) from the list.
E.164/IP Address	Enter one of the following: • If the endpoint is registered to a gatekeeper, enter the E.164 number of the endpoint. • If the endpoint is not registered to a gatekeeper, enter the IP address of the endpoint.
Manage (upgrade and configure) this endpoint	Select to manage this endpoint using Scopia® Management. If selected, you can configure the endpoint and upgrade its software via Scopia® Management.
Registered To	Select the gatekeeper to which the endpoint is registered to from the list. If you select None , the endpoint can be added to Scopia® Management but will not be connected until you register the endpoint with the gatekeeper, and select the gatekeeper here.

Field Name	Description
Location	Select the location of the endpoint, from the list. The Location field is visible only for distributed deployments.
Max IP Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Scopia® Management uses the bandwidth value to reserve resources for this endpoint.
VIP Endpoint	Select to indicate that this is an important endpoint whose video resolution should not be scaled down to below HD quality even when the available effective bandwidth is less than optimal. A VIP endpoint is marked with this icon  . This option is only available when the effective available bandwidth is above 1800 Kbps.
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.
Presence	If this endpoint was imported from the LDAP server, select to display its availability (for example, in the Lync client for Microsoft environments). Enter the primary endpoint's SIP URI , which consists of the endpoint name or endpoint number, followed by the SIP server domain name and a suffix derived from the domain name of the SIP server. For example, <code><endpoint_name>@<Lync_server_domain_name></code> or <code>user@domain_name.com</code> .
Has embedded MCU	Select if the endpoint has a built-in MCU.

5. Select **Apply** to save your changes.

Adding SIP IP Endpoints

About this task

This procedure describes how to manually import SIP endpoints into Scopia® Management.

Before you begin

Verify that you have sufficient Scopia® Named Endpoint licenses in the system, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

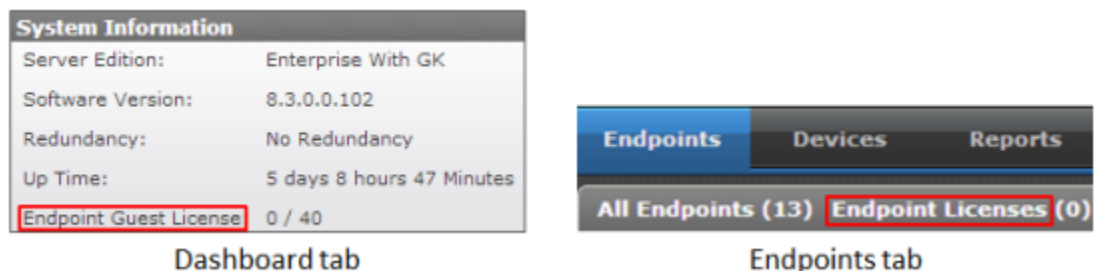


Figure 53: Checking the number of available Scopia® Named Endpoint

Procedure

1. Access the Scopia® Management web browser interface.
2. Select the **Endpoints** tab.
3. Select **Add > Add manually**.

The **Add Endpoint** dialog box appears.

Figure 54: Adding SIP endpoints

4. Configure your endpoint as described in [Table 34: Adding SIP endpoints](#) on page 103.

Table 34: Adding SIP endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter any description text that you may have for this endpoint.
Type	Select the endpoint type.
Protocol	Select IP(SIP) from the list.

Field Name	Description
SIP URI	Define the endpoint name or endpoint number, followed by the SIP server domain name and a suffix derived from the domain name of the SIP server. For example, <terminal name>@<SIP server domain name> or "user@domain_name.com".
Location	Select the location of the endpoint, from the list. The Location field is visible only for distributed deployments.
Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Scopia® Management uses the bandwidth value to reserve resources for this endpoint.
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.
VIP Endpoint	Select to indicate that this is an important endpoint whose video resolution should not be scaled down to below HD quality even when the available effective bandwidth is less than optimal. This option is only available when the effective available bandwidth is above 1800 Kbps.
Manage (upgrade and configure) this endpoint	Select to manage this endpoint using Scopia® Management. If selected, you can configure the endpoint and upgrade its software via Scopia® Management.

5. Select **Apply** to save your changes.

Adding Telepresence Systems in Scopia® Management

About this task

Scopia® XT Telepresence is a videoconferencing system which is used to create video meetings with a telepresence effect.

There are telepresence systems that can be assembled using regular single endpoints; for example, Scopia® XT Telepresence can use three XT5000 endpoints (see [Planning and Configuring Telepresence in Scopia® Management](#) on page 111).

Unlike other endpoints, you must always add telepresence systems to Scopia® Management manually. You need to integrate the Scopia® XT Telepresence with the Scopia® Management to add it as a resource to your video network.

If you use regular endpoints to create a telepresence system, define them in Avaya Scopia® Management as components of the telepresence system, not as single endpoints. You cannot directly change an existing single endpoint in Avaya Scopia® Management into a telepresence endpoint, and vice versa.

If your organization uses an LDAP directory, only the primary endpoint should be defined in the LDAP directory.

Your telepresence system's primary endpoint depends on the system's configuration. Typically the primary endpoint is defined as follows:

- Telepresence systems with three monitors, such as Scopia® XT Telepresence: the central monitor
- Telepresence systems with two monitors: the left monitor
- Telepresence systems with four endpoints: the left-central monitor

Before you begin

- Ensure the gatekeeper to which you registered your telepresence system is defined and configured in Scopia® Management.
- If the endpoints you want to define as part of your telepresence system already exist in Scopia® Management as separate single endpoints, you must delete them. You will redefine these endpoints as part of your telepresence system as described in the procedure below.
- If your organization uses the LDAP directory and the endpoints forming the telepresence system are defined in the LDAP directory, we strongly recommend that you define only the primary endpoint in your LDAP directory and remove non-primary endpoints from it.
- Verify that you have sufficient Scopia® Named Endpoint licenses in the system, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

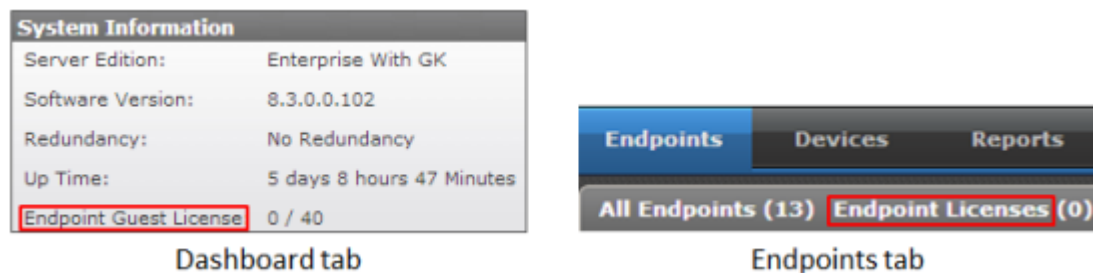


Figure 55: Checking the number of available Scopia® Named Endpoint

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** tab.
3. Select **Add > Add manually**.

The **Add Endpoint** window appears. See [Figure 56: Example of the Add Endpoint window as it appears for a Scopia® XT Telepresence endpoint](#) on page 106 and [Figure 57: Example of the Add Endpoint window as it appears for a Cisco CTS](#) on page 106.

Add Endpoint

Name:

Description:

Type: ☒ Manage (upgrade and configure) this endpoint

IP Address:

Registered To:

Location:

Max Bandwidth Per Segment: (Kbps)

☒ Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile)

OK **Cancel**

Figure 56: Example of the Add Endpoint window as it appears for a Scopia® XT Telepresence endpoint

Add Endpoint

Name:

Description:

Type: ☐ Triple

URI:

Location:

☒ Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile)

OK **Cancel**

Figure 57: Example of the Add Endpoint window as it appears for a Cisco CTS

4. Configure your telepresence endpoint as described in [Table 35: Configuring telepresence endpoints](#) on page 107.

! Important:

The settings you need to configure vary, depending on the model of the telepresence system you are adding.

Table 35: Configuring telepresence endpoints

Field Name	Description
Name	Enter a name used to identify the telepresence system as a whole. This is the name displayed in the list of endpoints.
Description	Enter any description text that you may have for this endpoint.
Type	Select the telepresence system. If your telepresence endpoint is not listed and has three monitors, select Generic Telepresence .
Cameras are cross-connected	Select this check box for systems where the left camera is connected to the right codec and visa versa.
Triple	If you are adding a Cisco 3-monitor CTS-3000 Series endpoint to the deployment, select this check box.
Required Gatekeeper	Select the gatekeeper to which the telepresence system is registered. If you select None, you can add the endpoint to Scopia® Management but it will not be connected until you register the endpoint with the gatekeeper, and select the gatekeeper here.
Location	A location is a physical space (building) or a network (subnet) where video devices can share a single set of addresses. A distributed deployment places these components in different locations, often connected via a VPN. This is only relevant for deployments with multiple locations. Select the location of the telepresence system from the list of locations you defined earlier in Scopia® Management.
Max Bandwidth per Segment	Scopia® Management uses the bandwidth value to reserve resources for this endpoint. Enter the default maximum bandwidth for a single codec in the telepresence system. For example, for the telepresence system to use 6144 Kbps, define 2048 Kbps for one codec. When there is enough bandwidth available, video is displayed in the highest possible resolution. This value is also subject to the bandwidth settings of the meeting type (MCU service) used in a meeting.

Field Name	Description
Visible in the directory of other endpoints	Select to display the telepresence system in the corporate address book. The telepresence endpoint is represented in the address book as a single endpoint. The number which the system displays is the number assigned to the primary monitor. The following solution components can access the telepresence system via this single entry: • Scopia® Management • Scopia® Desktop • XT Series • Scopia® Add-in for IBM Lotus Notes • Scopia® Add-in for Microsoft Outlook • Room systems via H.350 • Cisco telepresence devices
IP Address	Enter the IP address for all component in these cases: • If this telepresence system is not registered to a gatekeeper Or • If you want Scopia® Management to manage this telepresence system
Prefix	If you are adding a Cisco CTMS telepresence endpoint, enter the prefix. A dial prefix is a number added at the beginning of a dial string to route it to the correct destination, or to determine the type of call.
URI	If you are adding a Cisco CTS telepresence endpoint, enter the URI. URI is an address format used to locate a device on a network, where the address consists of the endpoint's name or number, followed by the domain name of the server to which the endpoint is registered. For example, <i><endpoint name>@<server_domain_name></i>.

5. Select **OK**.

The telepresence system appears on the **Endpoints** tab. The telepresence icon  indicates that the type of the endpoint is telepresence. The **Dialing Info** field shows the E.164, the URI or the IP address of the primary component of the telepresence system.

A telepresence endpoint

☐	Name	Dialing Info	Model	IP Address	Version	Registered To	Location
☐	XT TP EP	168.168.1.2	SCOPIA XT Series	168.168.1.2		168.168.227.211	HongKong
☐	225.44	22544	SCOPIA XT5000	168.168.225.44	3.2.0.34	168.168.227.211	Canada
☐	168.168.225.81	22581	SCOPIA XT4000	168.168.225.81	3.2.0.34	168.168.227.211	Beijing
☐	168.168.225.187	992408	SCOPIA VC240	168.168.225.187	2.7.1.4	TBG_VCS_GK	Canada
☐	168.168.225.104	235650	SCOPIA VC240	168.168.225.104	2.7.1.4	TBG_VCS_GK	Beijing

Figure 58: Example of a telepresence endpoint on the Endpoints tab

- To show the presence information for the telepresence system on Microsoft Lync clients, re-import its primary endpoint from the LDAP directory as described in [Importing H.323 Endpoints from an External LDAP Server](#) on page 94.

When the primary endpoint is re-imported, Scopia® Management lists the telepresence system and also reflects its presence information in Lync clients (if applicable).

Adding ISDN/PSTN H.320 Endpoints

About this task

This procedure describes how to manually import H.320 endpoints that you want Scopia® Management to automatically invite to a meeting and manage their availability.

Procedure

- Access the Scopia® Management web browser interface.
- Select the **Endpoints** tab.
- Select **Add > Add manually**.

The **Add Endpoint** dialog box appears.

Add Endpoint

Name:

Description:

Type:

Single Codec Endpoint

Protocol:

ISDN/PSTN (H.320)

Phone Number:

Country Code:

Area Code:

Number:

Max ISDN Bandwidth:

384

Kbps

Restricted Mode

☒ Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile)

OK

Cancel

Figure 59: Adding ISDN/PSTN H.320 endpoints

4. Configure your endpoint as described in [Table 36: Adding ISDN/PSTN H.320 endpoints](#) on page 110.

Table 36: Adding ISDN/PSTN H.320 endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter any description text that you may have for this endpoint.
Type	Select the endpoint type.
Protocol	Select ISDN/PSTN(H.320) from the list.
Phone Number	Enter the complete phone number of the endpoint in the Country Code , Area Code and Number fields. If you do not specify this information, Scopia® Management cannot find the optimal gateway for the endpoint when scheduling a conference.
Max ISDN Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Scopia® Management uses the bandwidth value to reserve resources for this endpoint.
Restricted Mode	Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.

5. Select **Apply** to save your changes.

Adding Mobile Endpoints

About this task

This procedure describes how to manually import mobile endpoints that you want Scopia® Management to automatically invite to a meeting and manage their availability.

Procedure

1. Access the Scopia® Management web browser interface.
2. Select the **Endpoints** tab.
3. Select **Add > Add manually**.

The **Add Endpoint** dialog box appears.

Figure 60: Adding mobile endpoints

4. Configure your endpoint as described in [Table 37: Adding mobile endpoints](#) on page 111.

Table 37: Adding mobile endpoints

Field Name	Description
Name	Enter a name used to identify the endpoint. This the name displayed in the list of endpoints.
Description	Enter any description text that you may have for this endpoint.
Type	Select the endpoint type.
Protocol	Select Mobile from the list.
Phone Number	Enter the complete phone number of the endpoint in the Country Code , Area Code and Number fields. Select 3G for 3G endpoints. If you do not specify this information, Scopia® Management cannot find the optimal gateway for the endpoint when scheduling a conference.
Bandwidth	Define the default maximum bandwidth for the endpoint by selecting bandwidth settings in the list (in Kbps). Scopia® Management uses the bandwidth value to reserve resources for this endpoint.
Visible in the directory of other endpoints	Select to display this endpoint in the corporate address book.

5. Select **Apply** to save your changes.

Planning and Configuring Telepresence in Scopia® Management

Scopia® XT Telepresence is a videoconferencing system which is used to create video meetings with a telepresence effect. A telepresence system consists of two or more endpoints which work together to create a wider image, creating a simulated experience of participants being present in the same room.

With the new telepresence interoperability support, Scopia® Management can establish connections with third-party telepresence systems from Cisco, Logitech/LifeSize, Polycom and Tandberg, allowing

telepresence users to view all meeting participants in a videoconference, including those on traditional videoconferencing systems or telepresence systems from other vendors.

Note the following restrictions and guidelines:

- Telepresence is supported only for IP (H.323) endpoints.
- When there is enough bandwidth available, video is displayed in the highest possible resolution.
- Telepresence endpoints cannot be associated with a specific user.
- Telepresence endpoints cannot be set as VIP (an important endpoint whose video resolution is not scaled down to below HD quality even when the available effective bandwidth is less than optimal).
- In cascaded meetings, telepresence endpoints always connect to the Master MCU. For more information about cascaded meetings, see [Increasing MCU Capacity by Cascading Multiple MCUs](#) on page 69.
- As with all dedicated endpoints, telepresence systems require a license to be defined and managed in Scopia® Management (see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22).

To add telepresence systems to Scopia® Management, see [Adding Telepresence Systems in Scopia® Management](#) on page 104. For detailed information about telepresence systems, see:

Navigation

- [Understanding Telepresence Systems](#) on page 112
- [Hosting Telepresence Meetings](#) on page 113
- [Calculating Resources for Telepresence](#) on page 113
- [Scheduling Telepresence Systems](#) on page 113

Understanding Telepresence Systems

Scopia® XT Telepresence is a videoconferencing system which is used to create video meetings with a telepresence effect. A telepresence system consists of two or more endpoints which work together to create a wider image, creating a simulated experience of participants being present in the same room.

The Scopia® MCU and Scopia® Management support the following telepresence (TP) systems:

- Scopia® XT Telepresence
- Polycom ATX 300
- Polycom RPX 200
- Polycom RPX 400
- Polycom TPX HD 306
- Tandberg T3
- LifeSize Conference
- Cisco CTS
- Cisco CTMS
- Generic (other telepresence endpoints that have 3 screens)

Other than the Scopia® Named Endpoint license required for each dedicated endpoint defined in Scopia® Management (see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22), Scopia® Management does not require any specific license for supporting telepresence but is aware of the Scopia® MCU telepresence license in order to deliver warning messages to administrators and for display purposes.

Hosting Telepresence Meetings

Telepresence meetings are managed by Scopia® Management and hosted by the MCUs in the network. Scopia® Management assigns MCUs to telepresence meetings according to the network deployment:

- In mixed deployments with both telepresence enabled MCUs and telepresence disabled MCUs, Scopia® Management chooses the MCU host according to the endpoint specifications.
- In centralized deployments with telepresence meetings, Scopia® Management chooses a telepresence enabled MCU. For centralized deployments with Non-telepresence Meetings, Scopia® Management gives preference to a MCU with no telepresence support. If there are no resources on the non- telepresence MCU, it will use a telepresence enabled MCU.
- In distributed deployments with telepresence meetings, Scopia® Management chooses a telepresence enabled MCU according to the best location. For distributed deployments in non-telepresence meetings, Scopia® Management chooses the best MCU according to location even if the MCU is telepresence enabled; location has higher priority than telepresence preference.

Calculating Resources for Telepresence

Resources are calculated according to the number of supported screens.

For example: For scheduled telepresence endpoints which have two screens, Scopia® Management calculates 2 HD ports. For scheduled telepresence end points which have four screens, Scopia® Management calculates 4 HD ports.

If a telepresence system is dialing into the system (which can be done from each one of the pre-configured numbers), Scopia® Management attempts to allocate the total number of ports on the master conference, and if managed to do so, it will authorize to connect the call.

Scheduling Telepresence Systems

When scheduling a telepresence system, the following restrictions apply:

- Enabled telepresence MCU must be selected.
- Telepresence must be scheduled to the master conference.
- Pre-positioning the telepresence endpoint in a specific sub frame will not be supported for the telepresence endpoint.

Managing Endpoints using Scopia® Management

About this task

This procedure describes how to manually set endpoints to be managed by Scopia® Management. Follow the procedure below to manage endpoints that were imported from the LDAP server or H.350 search base, or manually added endpoints that were not configured to be managed by Scopia® Management at the time they were added.

Scopia® Management can manage the following endpoint types: Avaya Scopia® XT Series, Scopia® VC240, and endpoints from Polycom, Tandberg, and LifeSize.

By default, all Scopia® Solution endpoints are automatically managed by Scopia® Management, provided they are registered to a gatekeeper defined in Scopia® Management.

The main management tasks include the following:

- Simultaneously upgrading all endpoints of the same type (not supported for LifeSize endpoints).
To quickly select all endpoints for simultaneous upgrades, you can assign labels to all endpoints of the same type. See [Organizing Endpoints into Groups with Labels](#) on page 129 for details.
- Controlling your endpoint's bandwidth (not supported for Polycom and Tandberg endpoints).
- Configuring your endpoint's resolution settings.
- Configuring your endpoints to display the corporate address book, as described in [Configuring Endpoints to be Displayed in the Corporate Address Book](#) on page 120 (not supported for Polycom and Tandberg endpoints).
- Monitoring your endpoints via alarms and traps sent by Scopia® Management.

Before you begin

Verify that the endpoints have a Scopia® Named Endpoint license, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

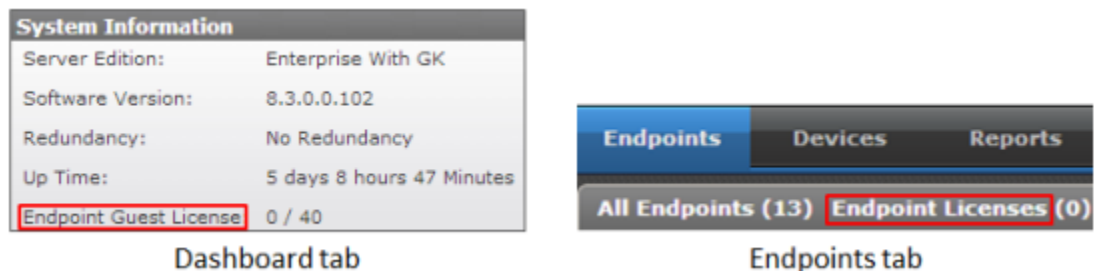


Figure 61: Checking the number of available Scopia® Named Endpoint

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** tab.
3. Select the endpoint you want to manage.
4. Select the **Basic Configure** tab.

Info	Basic Configuration	Advanced Configuration	Alarms
Name:	2222222 *		
Description:			
Type:	Single Codec Endpoint ▼		
Protocol:	IP (H.323) ▼		
Required Gatekeeper:	local_gatekeeper ▼		
Current Gatekeeper:	192.168.1.100		
Location:	Beijing ▼ *		
Max Bandwidth:	2048 ▼ * (Kbps)		
☒ Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile)			
☐ VIP Endpoint (experience will not be downgraded during call)			
☐ Enable Gallery Layouts			
☐ Presence			
☒ Manage (upgrade and configure) this endpoint			
Management IP Address:	192.168.1.100 *		
Model:	Scopia XT Series ▼		
☐ Has Embedded MCU			

Figure 62: Managing the endpoint

5. Select **Manage (upgrade and configure) this endpoint**.
6. Select **Apply**.
7. Select the **Access** tab.

Endpoint: 192.168.1.100					
Info	Basic Configure	Advanced Configure	Alarms	Events	Access
Username:	Admin *		Password:	****	
					Apply Cancel

Figure 63: Configuring the endpoint's access information

8. Enter the username and password for the endpoint's web interface login.
9. Select **Apply**.

Replicating Endpoint Settings on Multiple Endpoints

About this task

You can replicate an endpoint's settings on other endpoints of the same model and vendor. This is useful, for example, to save time by configuring the settings only once.

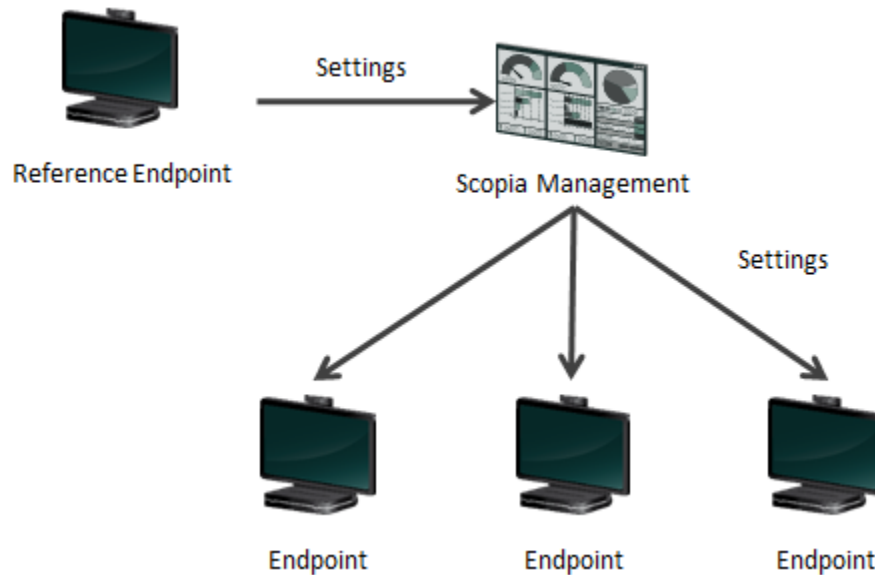


Figure 65: Replicating Endpoint Settings on Multiple Endpoints

You can replicate settings for these endpoints: Avaya Scopia® XT Series, Scopia® VC240, Polycom, and Tandberg.

This is done by accessing an endpoint's configuration file and applying it to other endpoints. The following information can be replicated:

- Basic settings (**Current Gatekeeper**, **Auto-Answer**, and **Default Call Bandwidth** fields)
- SIP settings (**SIP Proxy Server**, **SIP Registrar**, and **Transport Type** fields)
- Monitoring settings (**Trap Server Address** field)
- Video settings (**Video Mode** and **Enable Gallery Layouts** fields)
- Passwords (XT Series only)

You cannot replicate information that is specific to the endpoint, such as its name and whether it has a built-in MCU.

Before you begin

Decide which endpoint you would like to use as a reference for other endpoints, and verify that all settings are defined on your reference endpoint. The reference endpoint must be the same model and vendor as endpoints you are replicating the settings to, as listed in the endpoint's info page:

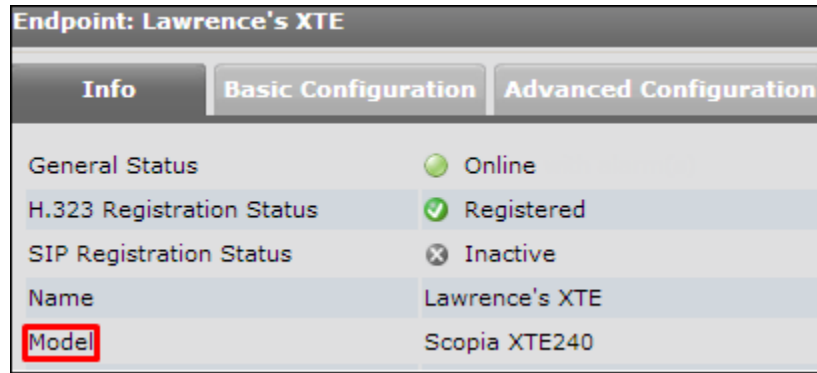


Figure 64: Checking the endpoint's model information

For example, you can replicate Scopia® XT Executive settings only to other Scopia® XT Executives, and not to other XT Series endpoints.

Verify that the endpoints are managed by Scopia® Management: Navigate to the **Basic** tab in the endpoint's page and verify that **Manage (upgrade and configure) this endpoint** is selected (see [Managing Endpoints using Scopia® Management](#) on page 113).

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** tab.
3. From the list, select the endpoint you are using as a reference and select **Manage > Retrieve Configuration File**.

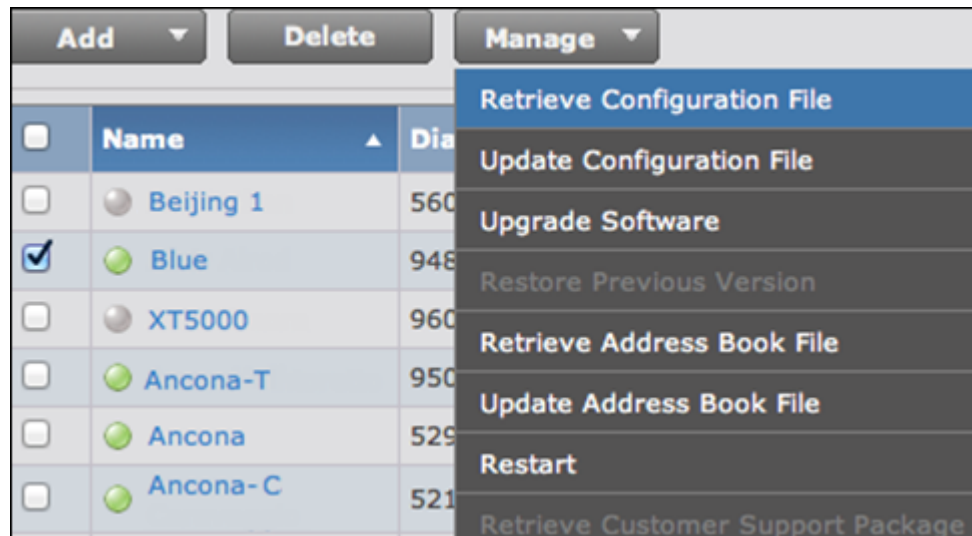
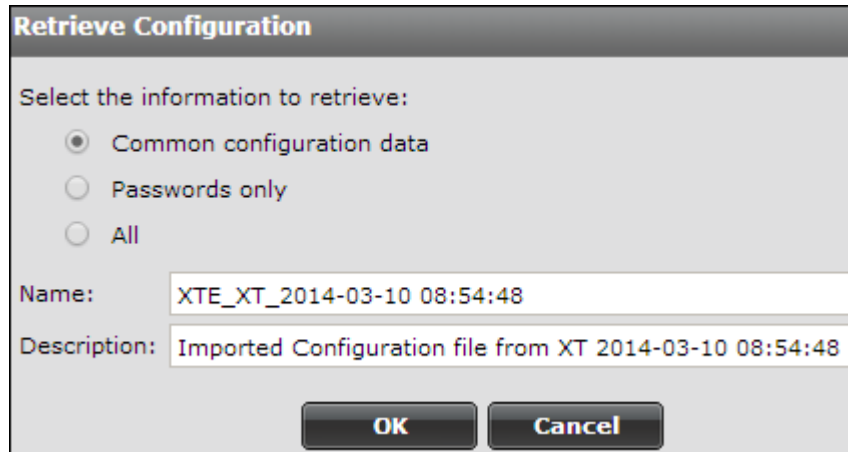


Figure 66: Retrieving the endpoint's configuration file

4. For XT Series endpoints only, you can choose which information to replicate:
 - a. Select the information to replicate:



Retrieve Configuration

Select the information to retrieve:

- ☒ Common configuration data
- ☐ Passwords only
- ☐ All

Name:

Description:

Figure 67: Selecting the information to replicate

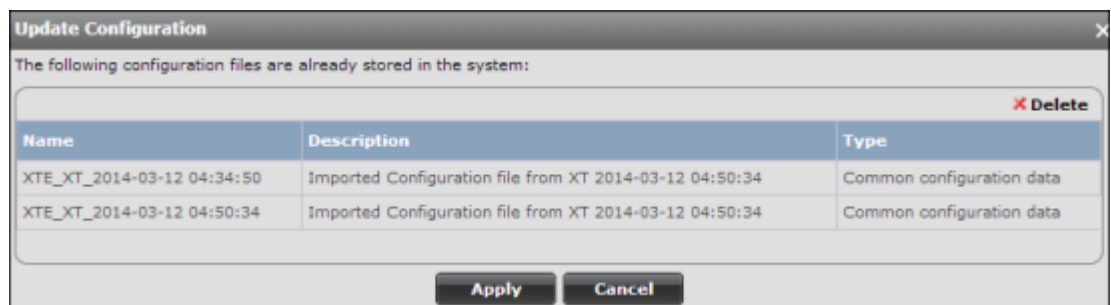
- **Common configuration data** (includes the fields listed in the introduction)
- **Passwords only** (includes all endpoint passwords, such as the administrator PIN, user PIN, and web interface password)
- **All** (both the passwords and the configuration data)

b. Select **OK**.

5. Select the endpoints to which you want to apply this configuration file.

6. Select **Manage > Update Configuration File**.

The system displays the list of imported configuration files.



Update Configuration

The following configuration files are already stored in the system:

Name	Description	Type	X Delete
XTE_XT_2014-03-12 04:34:50	Imported Configuration file from XT 2014-03-12 04:50:34	Common configuration data	
XTE_XT_2014-03-12 04:50:34	Imported Configuration file from XT 2014-03-12 04:50:34	Common configuration data	

Figure 68: Updating an endpoint's configuration file

7. Select the configuration file you want to use.

8. Select **Apply**.

The **Update Log** displays the status of the configuration file update.

Using Scopia® Management's Endpoint Directory as a Corporate Address Book

The corporate address book feature turns Scopia® Management's list of endpoints into a directory, allowing dedicated endpoints (H.350-enabled) to search through and find contact information for other

endpoints. When you add an endpoint to Scopia® Management, you define if it is displayed in the address book.

The following endpoints support this feature:

- Life-Size: Passport, Express, Team, Room, Conference
- Polycom: HDX Series, VSX Series
- Avaya Scopia® XT Series
- All Tandberg endpoints via TMS

This section includes the following topics for configuring corporate address books:

Navigation

- [Configuring Corporate Address Books](#) on page 119
- [Configuring Endpoints to be Displayed in the Corporate Address Book](#) on page 120

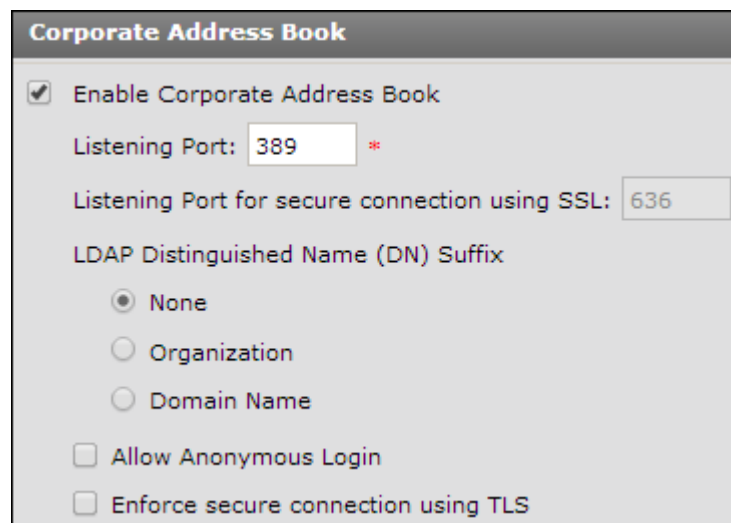
Configuring Corporate Address Books

About this task

This procedure describes how to enable the corporate address book feature, which allows dedicated endpoints (H.350-enabled) to search through Scopia® Management's directory of endpoints. This feature is disabled by default.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Address Book > Corporate Address Book**.



The screenshot shows the 'Corporate Address Book' configuration window. It has a title bar with the text 'Corporate Address Book'. Inside the window, there is a checked checkbox labeled 'Enable Corporate Address Book'. Below this, there are two text input fields: 'Listening Port:' with the value '389' and a red asterisk, and 'Listening Port for secure connection using SSL:' with the value '636'. Underneath these is a section for 'LDAP Distinguished Name (DN) Suffix' with three radio button options: 'None' (selected), 'Organization', and 'Domain Name'. At the bottom, there are two unchecked checkboxes: 'Allow Anonymous Login' and 'Enforce secure connection using TLS'.

Figure 69: Using Scopia® Management's Directory as the Corporate Address Book

3. Select **Enable Corporate Address Book**.
4. Enter the port to receive the LDAP request in the **Listening Port** field.

--Or--

If your organization requires a secure connection, select **Enforce secure connection using TLS** and enter the port in the **Listening Port for secure connection using SSL** field.

5. (Optional) Define the search base for endpoints by selecting one of the following options for **LDAP Distinguished Name (DN) Suffix** (the root DN):
 - Select **None** to set the search base to "ou=name".
 - Select **Organization Name** to limit the search base to a specific organization and enter its name: "o=<organization>".
 - Select **Domain Name** to limit the search base to a specific domain and enter the domain name: "ou=name, dc=<domain>,dc=com".
 6. (Optional) To allow endpoints to search data in the LDAP service without logging in, select **Allow Anonymous Login**.
 7. Select **Apply** to save your changes.
-

Configuring Endpoints to be Displayed in the Corporate Address Book

About this task

You can define if an endpoint is displayed in the corporate address book, or if it is a private number and other endpoints should not have access to this information.

Important:

This is not supported for Polycom and Tandberg endpoints.

Procedure

1. Access the Scopia® Management administrator portal.
 2. Select **Endpoints** tab.
 3. Navigate to the endpoint using the categories on the sidebar.
 4. Select the endpoint you want to configure.
 5. (Optional) Select **Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile)**.
 6. Select **Apply** to save your changes.
-

Managing your Endpoint's User Directory with LDAP

You can manage the contact list of your endpoints using one of the following LDAP servers:

- Scopia® Management's built-in LDAP server

Configure your endpoints to use Scopia® Management as your LDAP server via Scopia® Management or the endpoint's web interface.

- A third-party LDAP server (such as or Microsoft Active Directory or IBM Lotus Domino)

Configure your endpoints to use a third-party LDAP server via Scopia® Management or the endpoint's web interface.

For XT Series endpoints, this is done via the XT Series endpoint's web interface only. For more information, see the *Administrator Guide for XT Series*.

- An endpoint's built-in LDAP server

Configure your endpoints to use one of the endpoint's built-in LDAP servers via Scopia® Management or the endpoint's web interface.

For XT Series endpoints, this is done via the XT Series endpoint's web interface only. For more information, see the *Administrator Guide for XT Series*.

Avaya Scopia® Management's LDAP functionality includes the H.350 extension, which allows you to set up your user directory with specific attributes that are useful in a videoconferencing environment. For example, you can add a meeting room as a user, or define multiple endpoints for one user, and have a directory of endpoints.

Use the following procedures to use Avaya Scopia® Management's built-in LDAP directory to keep track of users and their endpoints:

Navigation

- [Configuring Endpoints to use an LDAP Directory](#) on page 121
- [Configuring Third-Party Endpoints to use Scopia® Management as LDAP Directory](#) on page 124

Configuring Endpoints to use an LDAP Directory

About this task

This procedure describes how to manage the contact list of your endpoints using an LDAP server, such as Scopia® Management's built-in LDAP server. This can be done for XT Series, Scopia® VC240, and endpoints from LifeSize, Polycom, and Tandberg. Depending on the endpoint model, you configure the LDAP server either from Scopia® Management or from the endpoint's web interface (see details in the list below).

A centralized solution like Scopia® Management enables synchronizing the same list of contacts across all the endpoints in your organization, and has other benefits like remote centralized upgrading and backing up of all endpoints in your video network.

LDAP servers are accessed using the H.350 protocol, which enhances the LDAP standard to include video endpoint information.

You can define three types of LDAP servers:

- Scopia® Management's built-in LDAP server

The contacts of this server are read-only from the endpoint. You can define more than one such server, specifying each IP address, port, and its LDAP username and password. The resulting list shows all the organization's endpoints known to Scopia® Management.

From Scopia® Management's administrator portal, you can define it as the LDAP server for XT Series, Scopia® VC240 and LifeSize endpoints. For Polycom and Tandberg endpoints, you must

do this from the endpoint's web interface only (see [Configuring Third-Party Endpoints to use Scopia® Management as LDAP Directory](#) on page 124).

- The endpoint's built-in LDAP server

From Scopia® Management's administrator portal, you can define the endpoint's own LDAP server for Scopia® VC240 and LifeSize endpoints. For XT Series endpoints, this is done via the XT Series endpoint's web interface only (see the *Administrator Guide for Avaya Scopia® XT Series*). For Polycom and Tandberg endpoints, see [Configuring Third-Party Endpoints to use Scopia® Management as LDAP Directory](#) on page 124.

Important:

You cannot remove the endpoint's local LDAP server.

- A third-party LDAP server, such as Microsoft Active Directory

The contacts of a third party LDAP are read-only from the endpoint.

The LDAP tree must have the following specific structure and naming conventions. For more information, see the documentation for your endpoint.

From Scopia® Management's administrator portal, you can define a third-party LDAP server for Scopia® VC240 and LifeSize endpoints. For XT Series endpoints, this is done via the XT Series endpoint's web interface only (see the *Administrator Guide for Avaya Scopia® XT Series*). For Polycom and Tandberg endpoints, see [Configuring Third-Party Endpoints to use Scopia® Management as LDAP Directory](#) on page 124.

Before you begin

- Make sure that your endpoint is configured to be managed in Scopia® Management, as described in [Managing Endpoints using Scopia® Management](#) on page 113.
- If you are using Scopia® Management as the LDAP directory, configure its LDAP settings as described in [Configuring Corporate Address Books](#) on page 119.
- If you are using Scopia® Management as the LDAP directory, associate LDAP usernames to video endpoints; otherwise the endpoints displayed on the XT Series are listed without the correct username.
- When connecting to a third-party LDAP server, the network administrator must verify that the video endpoint information is stored in the h323Identity and SIPIdentity object classes, according to the H.350 protocol.

Important:

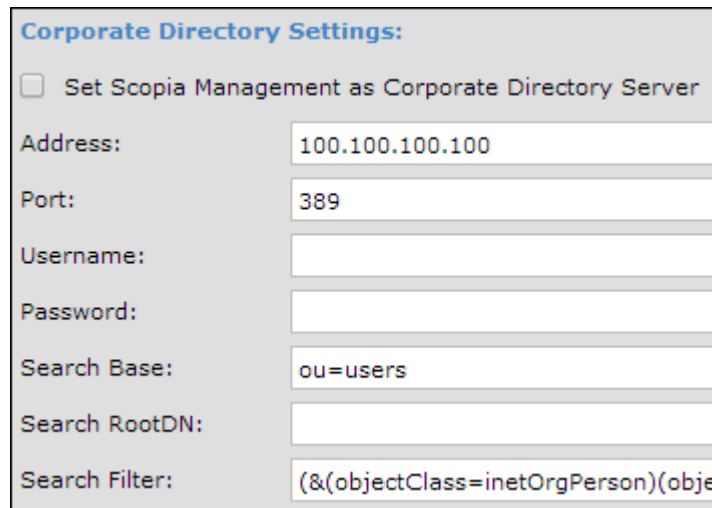
For XT Series, Scopia® VC240, and LifeSize endpoints that are managed by Scopia® Management, it sets parameters like the Gatekeeper address and the name of the LDAP server.

- If you are configuring an XT Series endpoint to use any LDAP server other than Scopia® Management, this is done via the XT Series endpoint's web interface only (see the *Administrator Guide for Avaya Scopia® XT Series*).

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** tab.
3. Select the required endpoint.

4. Select the **Advanced Configuration** tab.
5. Configure the LDAP server settings as described below.
The fields displayed depend on the type of endpoint.



Corporate Directory Settings:

☐ Set Scotia Management as Corporate Directory Server

Address: 100.100.100.100

Port: 389

Username:

Password:

Search Base: ou=users

Search RootDN:

Search Filter: (&(objectClass=inetOrgPerson)(obje

Figure 70: Configuring LDAP server settings from Scotia® Management

Table 38: Configuring LDAP server settings

Field Name	Description
Set Scotia® Management as Corporate Directory Server	(For XT Series only) Select to use Scotia® Management as your LDAP directory.
Address	Enter the LDAP server address. When using Scotia® Management as the LDAP server, displays its IP address.
Port	Enter the port used to connect to the LDAP server. The default port is 389.
Username Password	Enter the username and password required to access the LDAP server. The format of the username is in the form of a Distinguished Name (DN). Some standard components of DN are: domain controller (dc), organizational unit (ou), common name (cn), country (c), state or province (st), locality (l), organization (o). When using Scotia® Management as the LDAP server: - If you enabled anonymous login, these fields cannot be modified. You can verify this in Scotia® Management in Settings > Address Book > Corporate Address Book. - If you did not enable anonymous login, enter the administrator's Scotia® Management credentials. To enable anonymous login, see Configuring Corporate Address Books on page 119. The login to the third-party LDAP servers is via a Simple Bind LDAP v3 operation. When using the endpoint's built-in LDAP server, you can modify its LDAP password here.

Field Name	Description
Search Base	For third-party LDAP servers, enter the root node of the LDAP tree under which all the contacts (inetOrgPerson entities) are defined. For example <i>ou=people</i> . This value is predefined when the LDAP server is Scopia® Management or an XT Series, and cannot be modified.
Search Root DN	This is relevant only for XT Series using Scopia® Management as the LDAP server. If you are using Scopia® Management and you defined its Root DN (see the LDAP Distinguished Name (DN) field in Settings > Address Book > Corporate Address Book), the value is displayed here.
Search Filter	The filter applied to the LDAP tree, so you view only the relevant contacts. This value is predefined when the LDAP server is Scopia® Management or an XT Series, and cannot be modified. The phrase is required to navigate the remote LDAP tree, which depends on the way the tree was structured. For example, if the LDAP tree is built from objects known as inetOrgPerson, the filter would be <code>objectclass=inetOrgPerson</code> .
Authentication Mode	(For Scopia® VC240 only) Specify if the endpoint can search the data in the LDAP directory without the needs of an account. When using Scopia® Management as the LDAP server, this value is retrieved from Settings > Address Book > Corporate Address Book > Allow Anonymous Login and cannot be modified (see Configuring Corporate Address Books on page 119).
Secure Connection Using TLS	(For Scopia® VC240 only) Specify whether to only allow secure TLS connections between endpoints and the LDAP directory. When using Scopia® Management as the LDAP server, this value is retrieved from Settings > Address Book > Corporate Address Book > Enforce secure connection using TLS and cannot be modified (see Configuring Corporate Address Books on page 119).

6. Select **Apply**.

Configuring Third-Party Endpoints to use Scopia® Management as LDAP Directory

About this task

To configure third-party endpoints to use Scopia® Management as their LDAP server from the endpoint's web interface, use the settings detailed in this section. This process synchronizes each endpoint's contacts list with the corporate address book.

To configure third-party endpoints with any LDAP server via Scopia® Management's administrator portal, see [Configuring Endpoints to use an LDAP Directory](#) on page 121.

For LifeSize endpoints apply these settings ([Figure 71: LifeSize Endpoint Settings](#) on page 125):

- **LDAP Enable:** This must be enabled.
- **LDAP Host name:** The Scopia® Management address.
- **LDAP Username:** Set this field to the Scopia® Management's user, or set this to anonymous.
- **LDAP Password:** Set to the user's password.

- **LDAP Base:** The data input in one of the fields is the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. LifeSize searches the terminals by **ou=endpoints**.

For example:

- If Scopia® Management configured the LDAP Distinguished Name (DN) Suffix as **None**, in LifeSize the Base DN should be **ou=endpoints**.
- If Scopia® Management configures the LDAP Distinguished Name (DN) Suffix as **mycompany** for the Organization Name, in LifeSize the Base DN would be: **ou=endpoints,o=mycompany**.
- If Scopia® Management configured the LDAP Distinguished Name (DN) Suffix as: **mycompany.com**, in LifeSize the Base DN would be: **ou=endpoints,dc=radvision,dc=com**.

- **LDAP Filter:** Set its value to **(objectClass=*)**.

The screenshot shows the 'Directory > LDAP' configuration page in the LifeSize Express 220 web interface. The left sidebar has 'LDAP' selected under 'Preferences'. The main area contains the following fields:

- LDAP: Enabled (dropdown)
- LDAP Hostname: (text box)
- LDAP Username: (text box)
- LDAP Password: (password box)
- LDAP Base: ou=terminals,dc=radvision,dc=com (text box)
- LDAP Filter: (objectClass=*) (text box)
- LDAP Refresh: 1 Minute (dropdown)

At the bottom right are buttons: Save Changes, Cancel Changes, Refresh, and Copy. At the bottom left, a note states: 'LDAP Filter: Enter the search filter used to query your LDAP server.'

Figure 71: LifeSize Endpoint Settings

! Important:

You can perform this configuration via Scopia® Management by entering the LDAP settings in **Setting > Endpoint Management > Lifesize > Corporate Directory**.

For Polycom endpoints, apply these settings ([Figure 72: Polycom endpoint settings](#) on page 126):

- **Server Address:** set to the Scopia® Management server address.
- **Server Port:** It must be the same as the settings of Scopia® Management. For example: 389.
- **Group Name:** Define a group name.
- **Base DN (Distinguished Name):** The data input in one of the fields is the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. Polycom must use the **ou=users** because Polycom endpoints access via the users to reach the endpoints.

For example:

- If Scopia® Management configured the **LDAP Distinguished Name (DN) Suffix** as **None**, in Polycom the **Base DN** should be: **ou=users**.
 - If Scopia® Management configured the **LDAP Distinguished Name (DN) Suffix** as **mycompany** for the Organization Name, in Polycom the Base DN should be **ou=users,o=mycompany**.
 - If Scopia® Management configured the **LDAP Distinguished Name (DN) Suffix** as **mycompany.com** for the Domain Name, in Polycom the Base DN should be: **ou=users,dc=mycompany,dc=com**.
- **Authentication Type**: Define it as **Basic**.
 - **Bind DN (Distinguished Name)**: Set it to Scopia® Management's username.
 - **Change Password**: set to your user's password.

The screenshot shows the 'Admin Settings' tab in the Polycom endpoint configuration interface. The left sidebar contains a tree view with categories like 'General Settings', 'Network', 'Global Services', and 'Tools'. Under 'Global Services', 'Directory Servers' is selected. The main area is titled 'Directory Servers' and contains configuration fields for 'Polycom GDS' (disabled) and 'LDAP' (enabled). The LDAP section includes fields for 'Server Address', 'Server Port' (389), 'Group Name' (SCOPIA Directory), and 'Base DN (Distinguished Name)' (ou=users). An example 'dc=company,dc=com' is shown. The 'Authentication Type' is set to 'BASIC'. There are checkboxes for 'Use SSL (Secure Socket Layer)' (disabled) and 'Change Password' (enabled). Password fields for 'New Password' and 'Confirm Password' are shown with masked characters. An 'Update' button is in the top right.

Figure 72: Polycom endpoint settings

For Tandberg endpoints, apply these settings ([Figure 73: Tandberg Endpoint Settings](#) on page 127):

! Important:

You can configure Tandberg endpoints to use Scopia® Management as the LDAP directory only if they are configured to work with Tandberg Management Suite (TMS).

- **IP address/DNS**: Set this field to the Scopia® Management's address.
- **Username**: Set this field to the Scopia® Management's user.
- **Password**: Set to the user's password.
- **LDAP Port Number**: This must be the same as the settings for Scopia® Management. For example, **389**.

- **LDAP Base:** The data input in one of the field will be the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. Tandberg's TMS searches terminals by **ou=terminals**.

For example:

- If Scopia® Management configured the LDAP Distinguished Name (DN) Suffix as **None**, in TMS the Base DN would be **ou=terminals**.
- If Scopia® Management configured the LDAP Distinguished Name (DN) Suffix as mycompany for the Organization Name, on the TMS side the Base DN would be **ou=terminals,o=mycompany**.
- If Scopia® Management configured the LDAP Distinguished Name (DN) Suffix as: mycompany.com, in the TMS the Base DN would be:
ou=terminals,dc=mycompany,dc=com.

- **Custom LDAP Filter:** Enter the value **(commUniqueid=*)**.
- **Field to use for Display Name in TMS:** Enter the value **cn**.

Figure 73: Tandberg Endpoint Settings

Before you begin

Verify that the endpoints have a Scopia® Named Endpoint license, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

Configuring Presentation Layouts for Single-Screen Endpoints

About this task

To improve user experience on a dedicated single-screen endpoint, enable an additional set of video layouts called gallery layouts. Specifically designed for viewing shared content, these video layouts optimize screen space by displaying the presentation as the main part of the screen, with participants as a strip either alongside or underneath. By contrast, a standard video layout might display participants as an image overlay (as an example).

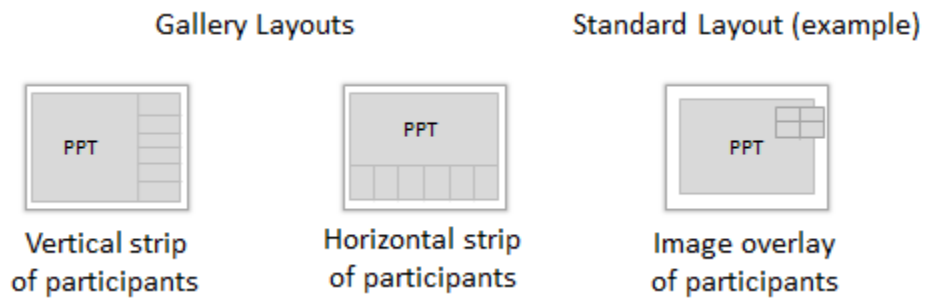


Figure 74: Comparing gallery and standard layouts

These layouts also support a higher resolution by using bandwidth more efficiently: All bandwidth is used for one video stream that includes both the presentation and the participant video, instead of being split between two separate streams. For example, if the XT Series connects using 2048 Kbps, the resulting resolution for a gallery layout is up to 1080p (for a list of video resolutions for a given bandwidth, see *Deployment Guide for Avaya Scopia® XT Series*). For other video layouts, the same bandwidth is split so that each stream uses 1024 Kbps, lowering the maximum resolution to 720p.

By default, gallery layouts are enabled for XT Series endpoints (XT5000 Series/XT4000 Series/Scopia® XT Executive), and disabled for dedicated third-party endpoints.

Gallery layouts are only available on meetings hosted by Scopia® Elite 6000 Series MCUs, and must be supported by the meeting type.

These video layouts require extra MCU resources (an additional 480p connection per meeting). If your MCU capacity is limited, you can disable gallery layouts for specific meeting types as described in [Modifying an MCU Meeting Type in Scopia® Management](#) on page 66.

Before you begin

- For XT Series endpoints only, verify that it is managed by Scopia® Management: Navigate to the **Basic** tab in the endpoint's page and verify that **Manage (upgrade and configure) this endpoint** is selected (see [Managing Endpoints using Scopia® Management](#) on page 113).

You can configure third-party endpoints to use gallery layouts even if they are not managed by Scopia® Management.

- Configure the meeting types to also support gallery layouts (see [Modifying an MCU Meeting Type in Scopia® Management](#) on page 66). Otherwise, gallery layouts are not available (even if enabled on the endpoint).

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the endpoint from the list in the **Endpoints** tab.
3. For XT Series endpoints, navigate to **Advanced Configuration > Video Settings** and select **Enable Gallery Layouts**.

--Or--

For third-party endpoints, select **Basic Configuration > Enable Gallery Layouts**.

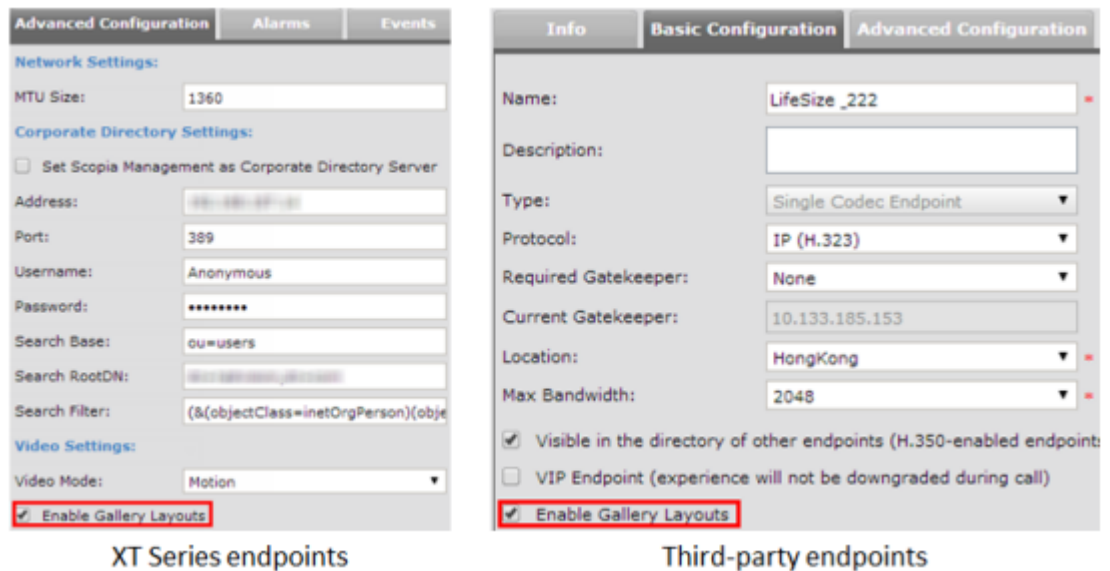


Figure 75: Enabling gallery layouts on your dedicated endpoint

4. Select **Apply**.

Organizing Endpoints into Groups with Labels

About this task

Labels allow you to easily search for and manage endpoints belonging to the same group like department in your organization or vendor. This is useful, for example, when performing management tasks for many endpoints at once. Scopia® Management comes with preconfigured labels for vendor names such as Avaya video endpoints, Cisco endpoints, or Lifesize endpoints. When you import or add an endpoint to Scopia® Management, the relevant vendor label is assigned to it automatically. You can also create labels that serve your needs. You can assign your own labels to endpoints after created them in Scopia® Management.

Assigning labels to endpoints is a very powerful and flexible way to manage your endpoints. You can for example with a few clicks filters all the Scopia® XT Executive endpoints of the Vice Presidents of your company and upgrade them.

An endpoint can have multiple labels. Labels are displayed in the sidebar for you to navigate easily to all endpoints with this label, as shown in [Figure 76: Viewing endpoints by preconfigured labels](#) on page 130.

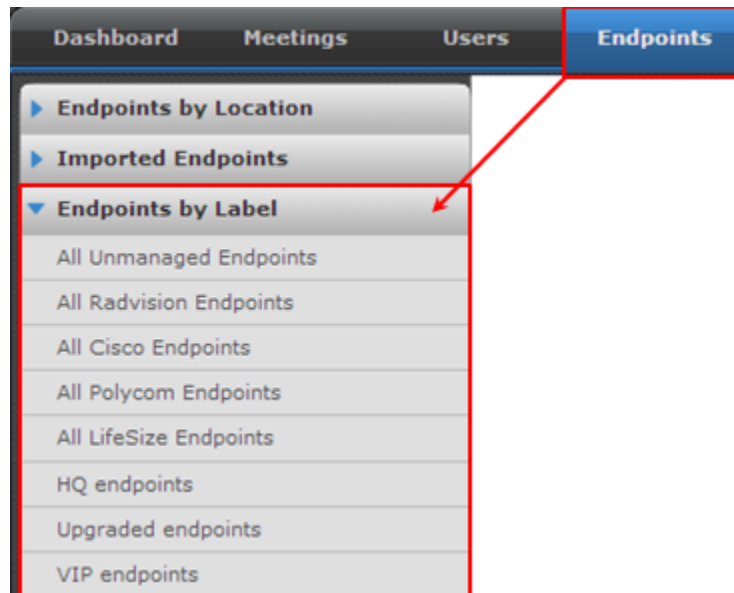


Figure 76: Viewing endpoints by preconfigured labels

After you organized endpoints using labels, you can easily filter the endpoint list to navigate to specific endpoints. For example, instead of navigating to Scopia® XT Executive endpoints of vice presidents in your organization one by one, you can select the relevant label and see all these endpoints in one list.

This procedure describes how to organize your endpoints with labels. You can create and modify labels, assign labels to endpoints or remove labels from endpoints, and delete labels from the system.

Before you begin

Verify that the endpoints have a Scopia® Named Endpoint license, indicated in both the **Dashboard** and **Endpoints** tabs. Only endpoints with a license can be managed in Scopia® Management. To install additional licenses, see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** tab.
3. To create a new label:
 - a. Select **Assign Labels > Create new**.

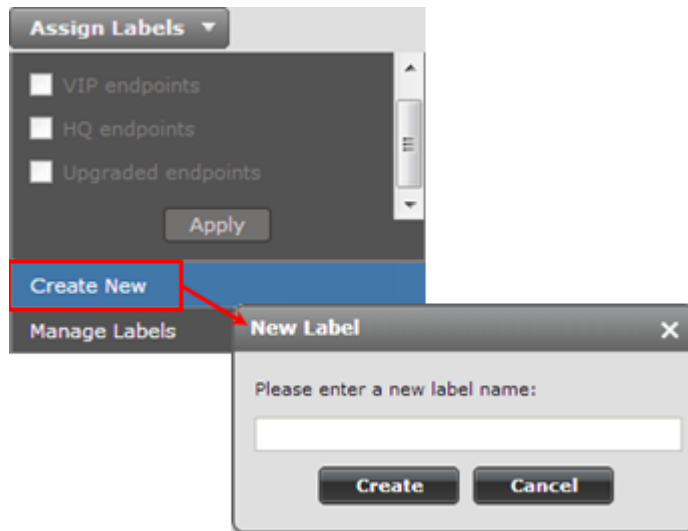


Figure 77: Creating a new label

- b. Enter a name for this label.
 - c. Select **Create**.
4. To assign a label to an endpoint or multiple endpoints:
 - a. Select the endpoints to which you are assigning the label.
 - b. Select **Assign Labels**.

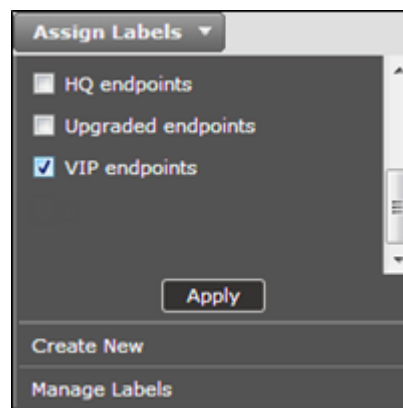


Figure 78: Assigning a label to an endpoint

- c. Select the label and click **Apply**.
5. To remove a label from an endpoint, navigate to the label under **Endpoints by Label**:
 - a. Select the endpoint from which you want to remove the label.
 - b. Select **Unassign Label**.

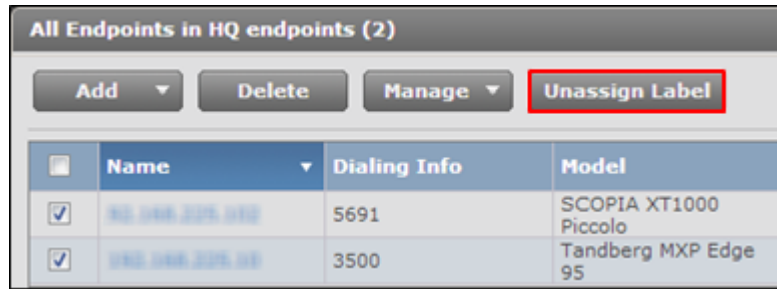


Figure 79: Unassigning labels from endpoints

c. Select **Yes** to confirm.

6. To modify or delete a label from the system, select **Assign Labels > Manage labels**:

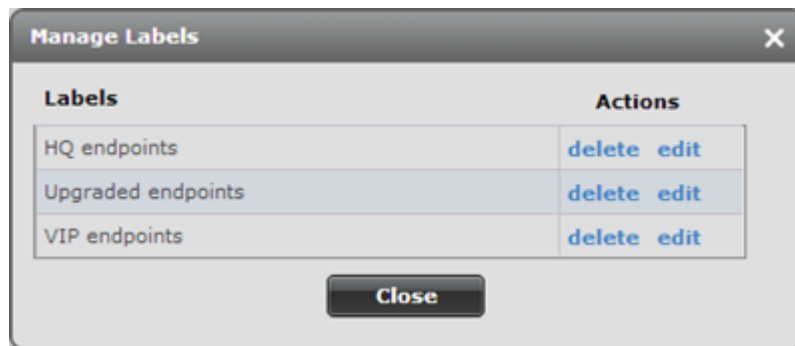


Figure 80: Managing endpoint labels

- Select **delete** to remove the label from Scopia® Management and select **OK**.
- Select **edit** to modify the label name and select **OK**.

Chapter 4 | Securing your Video Network

This chapter describes how to secure the communication between Scopia® Management and other components (such as other Scopia® Solution products, Avaya Session Manager, and your LDAP server), and how to secure your browser access to Scopia® Management using the HTTPS.

Navigation

- [Securing Web Access to Scopia® Management Using HTTPS](#) on page 133
- [Connecting Scopia® Management to WebLM Securely with HTTPS](#) on page 137
- [Securing the Connection between Scopia® Management and an LDAP Server](#) on page 139
- [Securing Your Video Network Using TLS](#) on page 139

Securing Web Access to Scopia® Management Using HTTPS

HTTPS is the secured version of the standard web browser protocol HTTP. It secures communication between a web browser and a web server through authentication of the web site and encrypting communication between them. For example, you can use HTTPS to secure web browser access to the web interface of many Scopia® Solution products.

You can use HTTPS to encrypt communications between Scopia® Management and anyone logging in to manage it using a web browser.

Important:

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

The Scopia® Management is shipped with a pre-created and pre-installed certificate, but it contains non-unique encryption keys. For full encryption, you must first install certificates with unique keys on the application server, and then configure the application server to use HTTPS. After performing these configurations, access Scopia® Management using HTTPS.

Once Scopia® Management's computer (application server) installs the full (private key) certificate, its communications will be encrypted, and only browsers with a corresponding matching (public key) certificates will be able to understand the communication. A private key certificate and its public key certificate are created as a matching pair.

Typically you request a trusted third party certification authority (CA) to issue a certificate which contains the encryption keys to be used for secure communications. A trusted CA signs all the certificates they issue. A trusted signature ensures that Scopia® Management is who it claims to be, and not an imposter. Popular web browsers are preconfigured to trust certificates that are signed by well-known CAs.

But in your deployment it may be good enough for you to issue your own certificates as an administrator if you are solely responsible for both the server's installation (Scopia® Management) and the client side (the browser). Certificates that you issue are self-signed. Most web browsers will issue an alert when

communicating with servers whose certificate is not signed by a well-known CA, questioning the trustworthiness of the server.

There are two stages to this configuration:

Navigation

- [Installing Certificates with Unique Keys on the Tomcat Web Server](#) on page 134
- [Configuring the Tomcat Web Server to Use HTTPS](#) on page 136

Installing Certificates with Unique Keys on the Tomcat Web Server

About this task

The Scopia® Management is shipped with a pre-created and pre-installed certificate which is stored in the `iview.keystore` file in `<install_dir>\iCM\tomcat\conf`. The certificate and your non-unique encryption keys are held in the keystore file, which is protected with a password.

To create a certificate with unique keys for true authentication, you must generate and install a new unique certificate, and then replace the pre-installed certificate held in the keystore file.

The certificate workflow uses a command line Java utility called `keytool`. It accesses the keystore file.

❗ Important:

The Scopia® Management server has Java 1.6 (Java 6) and Tomcat 7 web server pre-installed.

The `keytool` utility contains many more commands and parameters than are mentioned in this procedure. For more information, see the Java Development Kit (JDK) documentation: <http://java.sun.com/j2se/1.4.2/search.html>.

❗ 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. Stop the **Avaya Scopia® Management** service.
2. Open a command line window.
3. Add the directory of the `keytool` utility to the command line path environment:
`set path=%PATH%;<install_dir>\iCM\jre_rt\bin`
4. Create a temporary folder and subfolder to hold the original and new certificates, for example, `c:\cert1` holds the new certificates while `C:\cert1\original` holds the originals.
5. Copy the existing `iview.keystore` file located in `<install_dir>\iCM\tomcat\conf` to `c:\cert1` and `c:\cert1\original`.

The keystore file holds the certificates on each server. Currently they hold the default non-unique certificates.
6. Change your directory to `c:\cert1` to create the new certificate there.

7. Create a key pair to be stored in the keystore file using the `genkey` parameter, as follows:

```
keytool -genkey -keyalg RSA -dname "cn= <SM_FQDN>" -alias scheduler
-keystore c:\cert1\iview.keystore -storepass radvision -validity 360
-keysize 2048
```

Where:

- `-keyalg` determines the algorithm used to sign the certificate. The default is DSA, which is not supported by all versions of browsers. We recommend using RSA.
 - `<SM_FQDN>` is the computer name of Scopia® Management. The `-dname` parameter can also include information about the organizational unit (OU), organization (O), location (L), state (S), country (C). For example:
"cn=hostname.domain.com,ou=videodivision,o=radvision,S=NJ,C=USA"
 - The alias of the pre-installed key pair is `scheduler`.
 - The `iview.keystore` is the file to store the generated certificate.
 - The password on the keystore file is `radvision`.
 - The validity of the certificate is 360 days.
 - The key size is 2048 bits.
8. Press **Enter** at the `Enter key password for <scheduler>` prompt to create the key pair without a password.
9. If you do not want the generated certificate to be signed by a trusted CA, go to [Configuring the Tomcat Web Server to Use HTTPS](#) on page 136, otherwise continue as explained in the following steps.
10. Create a certificate signing request (CSR) file to be sent to the CA using the `certreq` parameter, as follows:

```
keytool -certreq -v -alias scheduler -file filename.csr
-keystore c:\cert1\iview.keystore -storepass radvision
```

The certification signing request (CSR) is stored in the file `c:\cert1\<filename.csr>`.

11. Send the `<filename.csr>` file to your selected CA for signing.
- The CA sends back the newly issued certificate (the CA signed certificate) and the CA trusted root certificate.
12. When you receive the two certificates back from the CA, back them up to `c:\cert1` and copy them to `<install_dir>\iCM\tomcat\conf`. In the following examples, **caroot.crt** refers to the CA trusted root certificate, and **SM.crt** refers to the CA signed certificate.
13. Import the **CA trusted root certificate** into the keystore using the `-import` parameter, as follows:

```
keytool -import -trustcacerts -alias caroot
-file c:\cert1\caroot.crt -keystore c:\cert1\iview.keystore
-storepass radvision
```

Where:

`caroot` is the alias of the CA trusted root certificate file that you received from the CA.

The system confirms the certificate was added to the keystore.

14. Import the **CA signed certificate** into the keystore file using the same alias name that was first given to the certificate key pair, as follows:

```
keytool -import -trustcacerts -alias scheduler
-file c:\cert1\SM.crt -keystore c:\cert1\iview.keystore
-storepass radvision
```

The system confirms the certificate was added to the keystore. You have now created a keystore file that stores a valid certificate for use.

15. Copy the *iview.keystore* file from *c:\cert1* to *<install_dir>\iCM\tomcat\conf*.
16. Restart the **Avaya Scopia® Management** service.
17. Configure the Tomcat web server to use HTTPS (SSL), as described in [Configuring the Tomcat Web Server to Use HTTPS](#) on page 136.

Configuring the Tomcat Web Server to Use HTTPS

About this task

This procedure details how to configure the Tomcat web server to use HTTPS (SSL).

Important:

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

Before you begin

Generate and install a certificate with unique keys, as described in [Installing Certificates with Unique Keys on the Tomcat Web Server](#) on page 134.

Procedure

1. Open the *server.xml* file, located in *tomcat\conf*:

```
<Connector connectionTimeout="20000" port="8080"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  redirectPort="9443"/>

<Connector port="9443"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true"
  keystoreFile="conf/iview.keystore" keystorePass="radvision"
  clientAuth="false" sslProtocol="TLS" />
```

2. Comment out the following line by adding a comment indicator at the beginning and the end:

```
<!--Connector connectionTimeout="20000" port="8080"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  redirectPort="9443"/-->
```

3. If Scopia® Management is installed on a different server than Scopia® Desktop server, we recommend changing Scopia® Management's connector port (TCP) to 443, a known HTTPS port. This allows users to access Scopia® Management without typing the port.

If Scopia® Management and Scopia® Desktop server are installed on the same server, we recommend using the default port value for Scopia Management (9443). This avoids a conflict with the default port value for Scopia® Desktop server (443).

The modified *server.xml* file reads now as follows:

```
<!--Connector connectionTimeout="20000" port="8080"
      protocol="org.apache.coyote.http11.Http11NioProtocol"
      redirectPort="9443"/-->

<Connector port="443"
      protocol="org.apache.coyote.http11.Http11NioProtocol"
      SSLEnabled="true"
      maxThreads="150" scheme="https" secure="true"
      keystoreFile="conf/iview.keystore" keystorePass="radvision"
      clientAuth="false" sslProtocol="TLS" />
```

4. Restart the Scopia® Management service. You can now access Scopia® Management from your web browser using HTTPS.

Connecting Scopia® Management to WebLM Securely with HTTPS

About this task

You can use HTTPS to secure communications between Avaya Scopia® Management and Avaya Web Licensing Manager (WebLM), to securely send license information for users and video network devices. HTTPS is the secured version of the standard web browser protocol HTTP. It secures communication between a web browser and a web server through authentication of the web site and encrypting communication between them.

To secure communications between your Scopia® Management and WebLM, configure the WebLM, which by default uses HTTP, to use HTTPS and to install the WebLM certificate on Scopia® Management to allow WebLM's authentication.

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. Open the *server.xml* file, located in *<install_dir>\tomcat\conf* (Windows) or */opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/deploy/jbossweb.sar/* (Linux) on the WebLM server.
2. Locate the connector section for *port="52233"*, as shown below:

```
<Connector port="52233"
      protocol="HTTP/1.1" SSLEnabled="true"
```

```
maxThreads="150" scheme="https" secure="true"  
clientAuth="false sslProtocol=TLS />
```

Alternatively, if you configured the WebLM to connect on a different port, like port 443, look for that port number in the file.

3. Add the following three attributes to enable https:

- keystoreFile
- keystorePass
- keystoreType

The keystoreFile pathname is either `/opt/cert-store/webLMserver.p12` (Linux), or `${catalina.base}/webapps/webLM/WEB-INF/webLMserver.p12` (Windows).

```
<Connector port="52233"  
  protocol="HTTP/1.1" SSLEnabled="true"  
  keystoreFile="/opt/cert-store/webLMserver.p12"  
  keystorePass="password"  
  keystoreType="PKCS12"  
  maxThreads="150" scheme="https" secure="true"  
  clientAuth="false sslProtocol=TLS"/>
```

4. Restart the WebLM server.
5. On the WebLM, locate the file `trusted_webLM_certs.jks` in `tomcat-6.0.36\webapps\webLM\admin` (Windows) or `/opt/Avaya/Mgmt/6.3.8/wlm/artifact/certs` (Linux).
Copy it to `<install_dir>\tomcat\shared\lib` on the Scopia® Management server.
6. On the WebLM, locate the file `trustedcert.properties` in `tomcat-6.0.36\webapps\webLM\admin` (Windows) or `/opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/conf/webLM` (Linux).
Copy it to `<install_dir>\tomcat\shared\lib` on the Scopia® Management server.
7. Edit the newly copied `trustedcert.properties` file on the Scopia® Management server in a plain text editor.
8. Modify these attributes as follows:

```
WebLM.trustStore=trusted_webLM_cert.jks  
WebLM.trustStoreType=JKS  
WebLM.trustStorePassword=password
```

9. Restart the Scopia® Management service.
10. Configure the Scopia® Management connection with the WebLM server:
 - a. In the Scopia® Management administrator portal, select **Settings > Unified Communications > Avaya Aura**.
 - b. Enter the URL of the Avaya WebLM server in the **Aura Licensing Server Settings (WebLM)** field, making sure to use the `https://` prefix and the port number 52233 you edited in the configuration files earlier in this procedure.
For example, `https://<Aura_System_Manager_FQDN>:52233/WebLM/LicenseServer`, carefully preserving the upper and lower case characters on Linux WebLM deployments.

Avaya Aura

☒ Enable Avaya Aura Conferencing (AAC) Integration

AAC SIP URI:

AAC Web Server Settings

Address:

Port:

☒ Translate virtual meeting ID prefix

Aura Licensing Server Settings (WebLM):

URL (example: http(s)://auraserveraddress:port/weblm/LicenseServer)

Apply

Figure 81: Configuring connection with Avaya WebLM server

c. Select **Apply**.

Scopia® Management automatically connects to the WebLM (indicated by the green icon).

Securing the Connection between Scopia® Management and an LDAP Server

About this task

There are two ways to secure Scopia® Management's connection to your LDAP server:

- Securing the connection with SSL/TLS. This is available for both Microsoft Active Directory and IBM Domino.

For this option, you need to enable SSL/TLS on your LDAP server and then to configure Scopia® Management to use the *ldaps://* prefix for the LDAP as described in [Connecting Scopia® Management with the LDAP Server](#) on page 172.

- Securing the login credentials with MD5 (see [Downloading Users from the LDAP Server](#) on page 175). This is only available for Microsoft Active Directory.

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.

Securing Your Video Network Using TLS

You can configure your video network devices, both Scopia® Solution and third-party, to support Transport Layer Security (TLS) for the SIP protocol. TLS enables network devices to communicate securely using certificates, to provide authentication of the devices and encryption of the communication between them.

Important:

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

TLS is used to secure the connection between Scopia® Management and the following solution components:

- Avaya Scopia® Desktop
- Scopia® Elite MCU
- Avaya Scopia® TIP Gateway
- Scopia® Video Gateway
- Avaya Scopia® XT Series
- Avaya Session Manager
- Microsoft Office Communications Server or Lync Server
- IBM Sametime media manager

Every network component must have its own TLS certificate to authenticate itself. Some of the components have a pre-installed TLS certificate, for example, Scopia® Desktop server or Microsoft Lync Server. You must create a TLS certificate for components that do not have a pre-installed TLS certificate. Scopia® Management must have two separate TLS certificates: one for Scopia® Desktop server and another one for other components ([Figure 82: Using two separate TLS certificates to secure Scopia® Management communications](#) on page 141). Other components need only one TLS certificate.

Communication between Scopia® Management and the LDAP server can also be secured using TLS, but it does not require a TLS certificate for Scopia® Management.

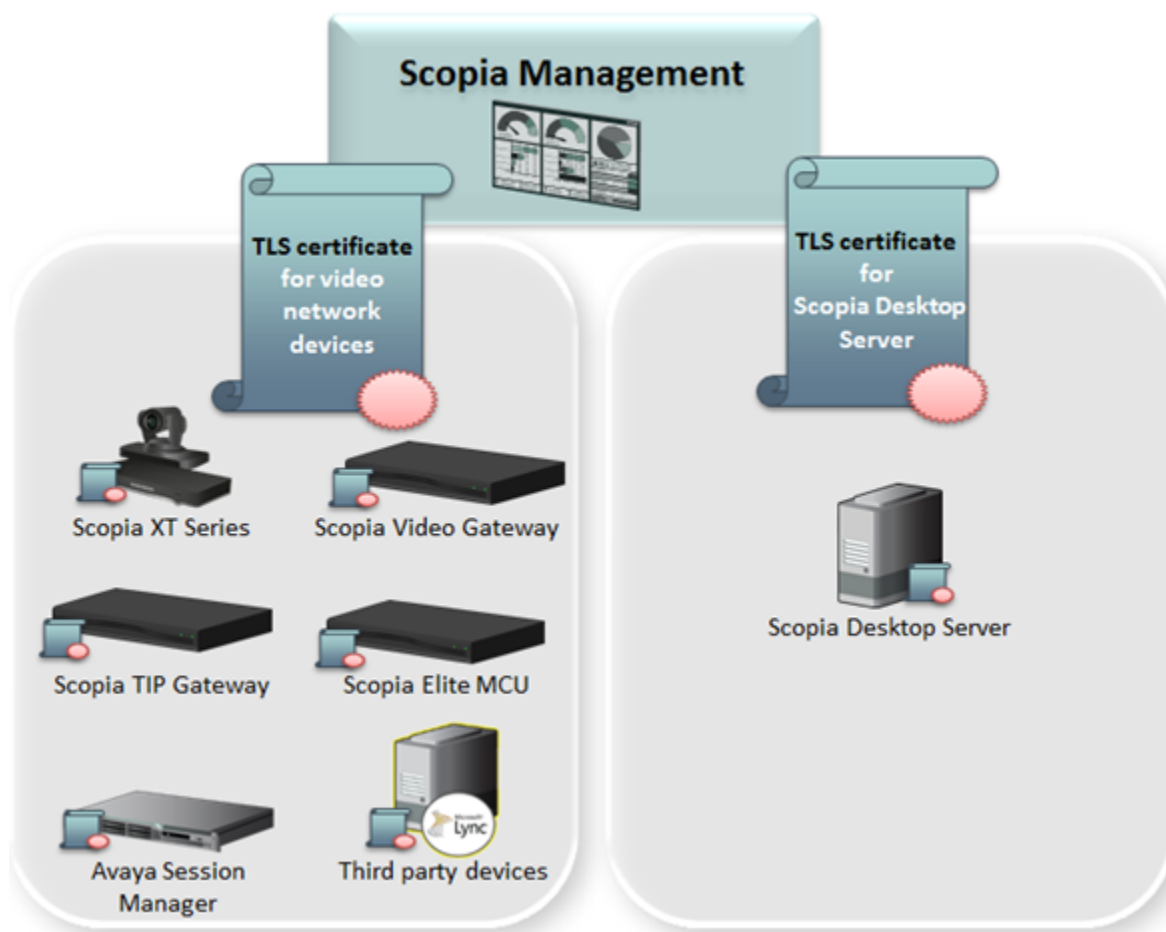


Figure 82: Using two separate TLS certificates to secure Scopia® Management communications

Pre-installed certificates of some of the components are not unique and cannot guarantee strong authentication. For more reliable security, create a new, unique certificate for these components.

To create a TLS certificate, you need to generate a certificate signing request (CSR) and send it to the certification authority (CA) for signing. A CA has its own certificate, known as the CA root certificate. When the CA signed certificate is ready, you upload it into the component for which it was created, together with the CA root certificate. Once this is done, the component can authenticate itself and is ready for TLS connection.

In some cases, when different CAs are used for signing certificates in your deployment, you must obtain an additional certificate vouching for the trustworthiness of these CAs. These certificates are known as intermediary certificates, and must be signed by a trusted CA. For more information, see [Planning the Required Certificates for TLS](#) on page 142.

Each time a video network device starts the TLS communication session, it sends its own signed certificate together with the CA root certificate and requests the same certificates from the other devices to which it wants to connect. After both devices verify each other's identity, a secure TLS connection can be established. Exchanging certificates between devices is part of the TLS protocol; it happens in the background and is transparent to a user.

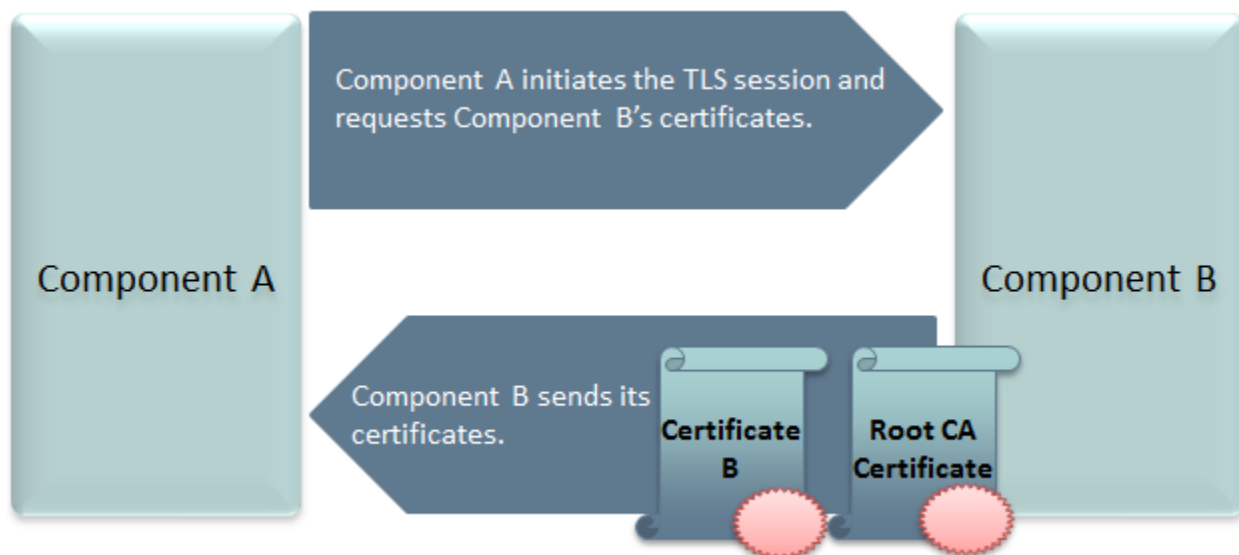


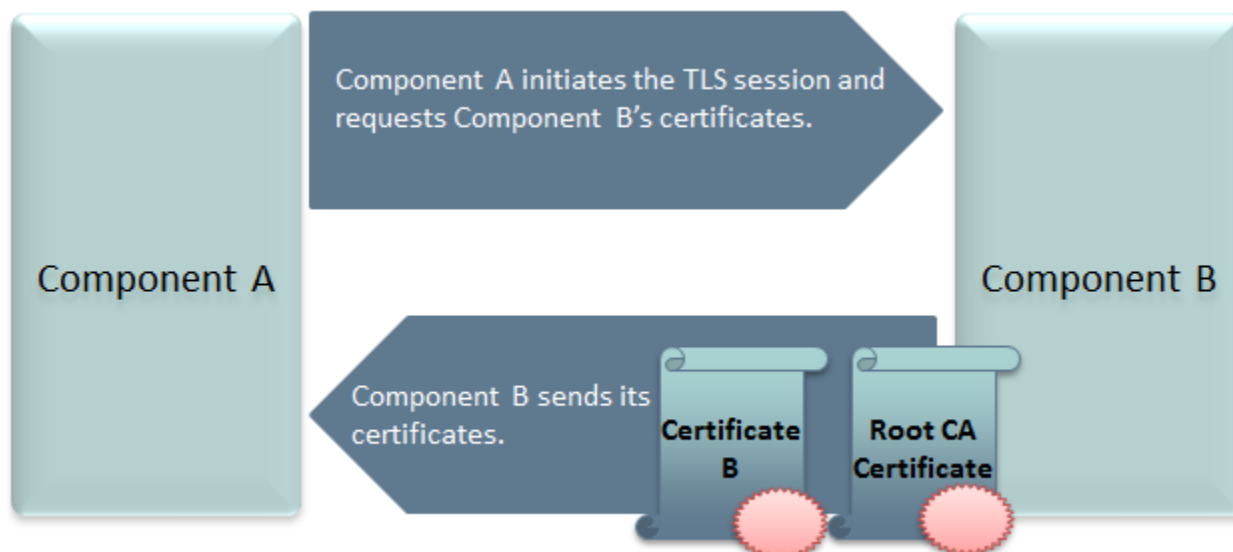
Figure 83: Establishing TLS connection

The following set of procedures secure the connection between Scopia® Management and other devices. Perform these tasks in the order listed below:

1. Decide your deployment's TLS requirements, as described in [Planning the Required Certificates for TLS](#) on page 142.
2. Prepare the first TLS certificate for Scopia® Management as described in [Creating and Uploading Scopia® Management's Certificate for Videoconferencing Components](#) on page 148.
3. Prepare the second TLS certificate for Scopia® Management as described in [Creating and Uploading the Scopia® Management's Certificate for Scopia® Desktop server](#) on page 153.
4. Create TLS certificates for components listed below and upload certificates onto the components for which they are created. Enable TLS encryption on these components.
 - MCU (see the *Administrator Guide for Scopia® Elite MCU*)
 - Scopia® Desktop server (see the *Administrator Guide for Scopia® Desktop server*)
 - XT Series (see the *Deployment Guide for XT Series*)
 - Avaya Scopia® TIP Gateway (see the *Deployment Guide for Avaya Scopia® TIP Gateway*)
 - Scopia® Video Gateway (see the *Lync Deployment Guide for Scopia® Video Gateway* or the *OCS Deployment Guide for Scopia® Video Gateway for Scopia® Video Gateway*)
 - Avaya Session Manager as detailed in the product's documentation
 - Other videoconferencing components (except on the Microsoft Lync and OCS) as detailed in the product's documentation.
5. If the CA used to identify some devices is different from the CA which identifies Scopia® Management, perform [Uploading Root and Intermediate Certificates for Scopia® Video Gateway, Avaya Scopia® TIP Gateway or Other Devices](#) on page 155.
6. Perform [Enabling the TLS Connection in Scopia® Management](#) on page 158.

Planning the Required Certificates for TLS

When a device establishes a secure TLS connection with another component, it requests a signed certificate verifying the other component's identity. The signature on the certificate must be from a known (trusted) certification authority (CA).



! 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.

There are several types of TLS connections:

- Standard TLS, where all certificates are signed by the same CA.
- Unique CAs, where each certificate is signed by a different CA.
- Unknown gateway CA, where the gateway's certificate is signed by an unknown (untrusted) CA.
- Unknown Scopia® Management CA, where Scopia® Management's certificate is signed by an unknown (untrusted) CA.
- Mutually unknown CAs, where both components carry certificates signed by CAs that are unknown to each other.

Each situation requires a different set of certificates to be uploaded to each of the components. Typically, the certificates are all signed by the same CA. Some unique deployments may use multiple CAs.

A CA's signature is always verified by its root certificate, which identifies the CA and is self-signed by that CA. When a device receives a certificate as part of TLS negotiations, it must verify that the CA signing the certificate is trusted, so it must have the CA's root certificate uploaded.

• **Standard TLS**

These connections use the same CA for signing all certificates on both sides. In this case, you need to upload two certificates to Scopia® Management and two for the gateway ([Figure 84: Standard TLS: Component Certificates and a CA Root Certificate](#) on page 144).

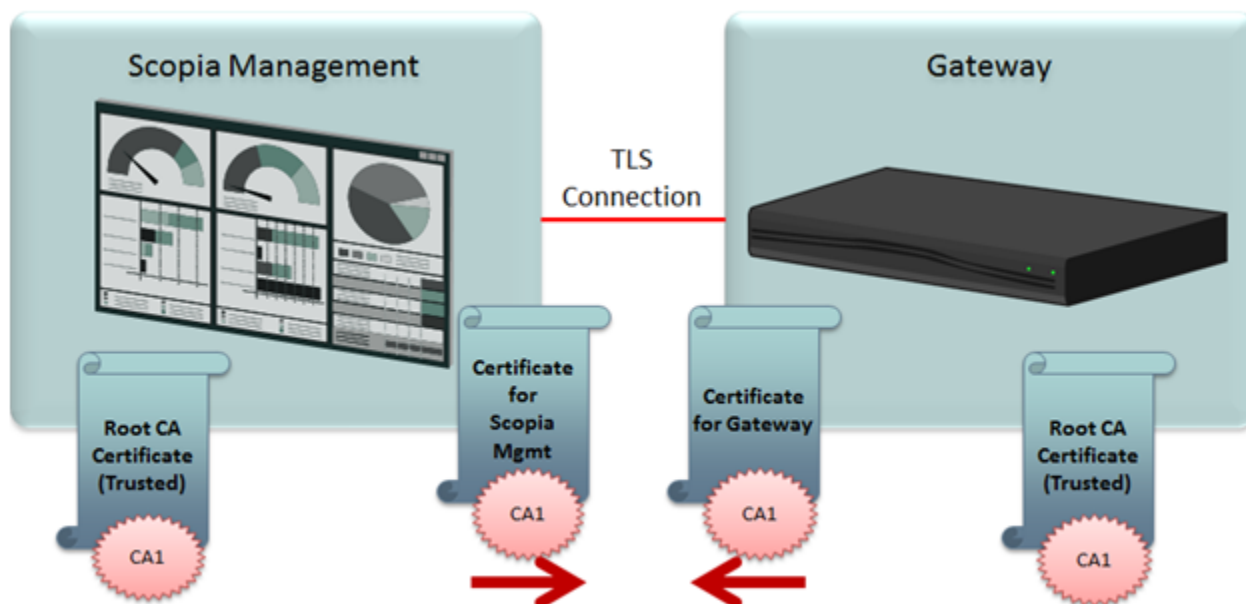


Figure 84: Standard TLS: Component Certificates and a CA Root Certificate

Upload the following certificates to the Scopia® Management:

- A certificate identifying Scopia® Management, signed by the CA. This is sent to the gateway as part of the TLS negotiation.
- A root certificate verifying the CA's identity, self-signed by that CA. This is used by Scopia® Management to verify the certificate sent by the gateway.

On the gateway side, upload the following certificates ([Figure 84: Standard TLS: Component Certificates and a CA Root Certificate](#) on page 144):

- A certificate identifying the gateway, signed by the same CA. This is sent to Scopia® Management as part of the TLS negotiation.
- A copy of the root certificate verifying the CA's identity, self-signed by the CA. This is used by the gateway to verify the certificate sent by Scopia® Management.

• Unique CAs

When certificates are signed by different CAs, each CA requires its own root certificate to be uploaded for authentication.

For example, in [Figure 85: TLS connection using certificates signed by different CAs](#) on page 145, the certificate identifying Scopia® Management is signed by CA1, while the the gateway's certificate is signed by CA2. This requires three certificates to be uploaded to Scopia® Management and two for the gateway ([Figure 85: TLS connection using certificates signed by different CAs](#) on page 145).

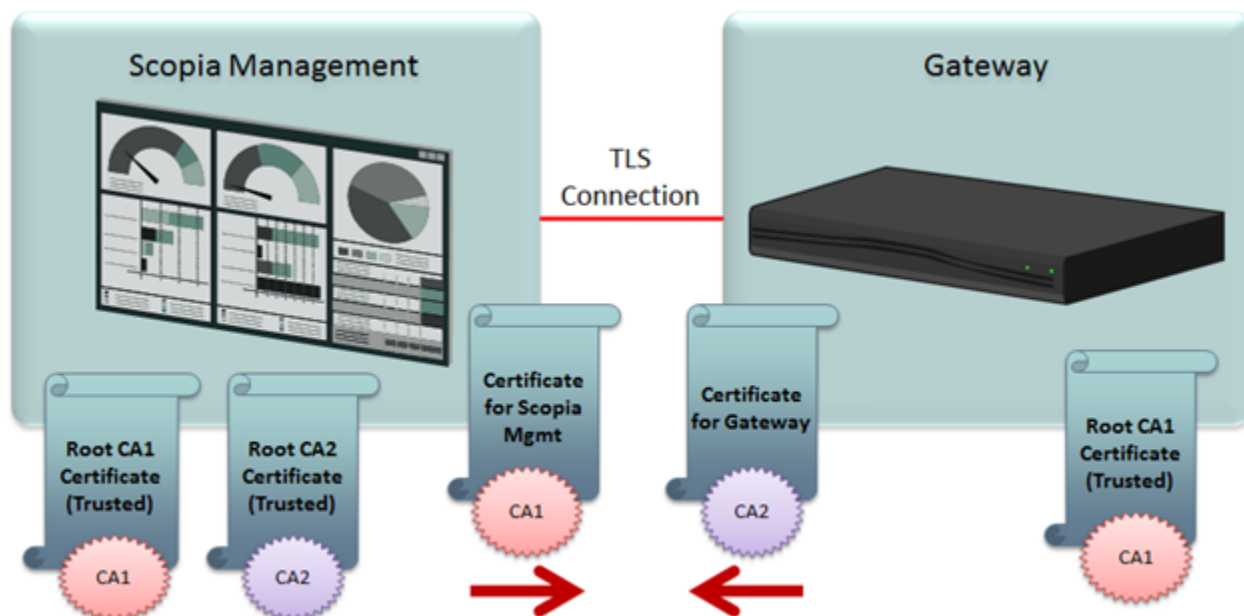


Figure 85: TLS connection using certificates signed by different CAs

When each certificate is signed by a different CA ([Figure 85: TLS connection using certificates signed by different CAs](#) on page 145), upload the following certificates to the Scopia® Management:

- A certificate identifying Scopia® Management, signed by trusted CA1. This is sent to the gateway as part of the TLS negotiation.
- A root certificate from the trusted CA1 verifying CA1's identity, self-signed by CA1. This is used by Scopia® Management to authenticate its certificate.
- A root certificate from the trusted CA2 verifying CA2's identity, self-signed by CA2. This is used by Scopia® Management to authenticate the certificate sent by the gateway, which is signed by CA2.

On the gateway side, upload the following certificates ([Figure 85: TLS connection using certificates signed by different CAs](#) on page 145):

- A certificate identifying the gateway, signed by trusted CA2. This is sent to Scopia® Management as part of the TLS negotiation.
- A root certificate verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the certificate sent by Scopia® Management, which is signed by CA1.

• Unknown gateway CA

If the CA of the gateway's certificate is unknown, it cannot be trusted unless it comes with an intermediate certificate, which vouches for the trustworthiness of the unknown CA. Intermediate certificates must be signed by a trusted CA.

For example, in [Figure 86: Signature of Gateway Certificate from Unknown CA](#) on page 146, the certificate identifying the gateway is signed by CA3, which may be known and trusted by those who installed the gateway, but in this scenario CA3 is not trusted by Scopia® Management. Meanwhile Scopia® Management's certificate is signed by CA1, a trusted CA. This scenario requires four certificates to be uploaded to Scopia® Management and two for the gateway ([Figure 86: Signature of Gateway Certificate from Unknown CA](#) on page 146).

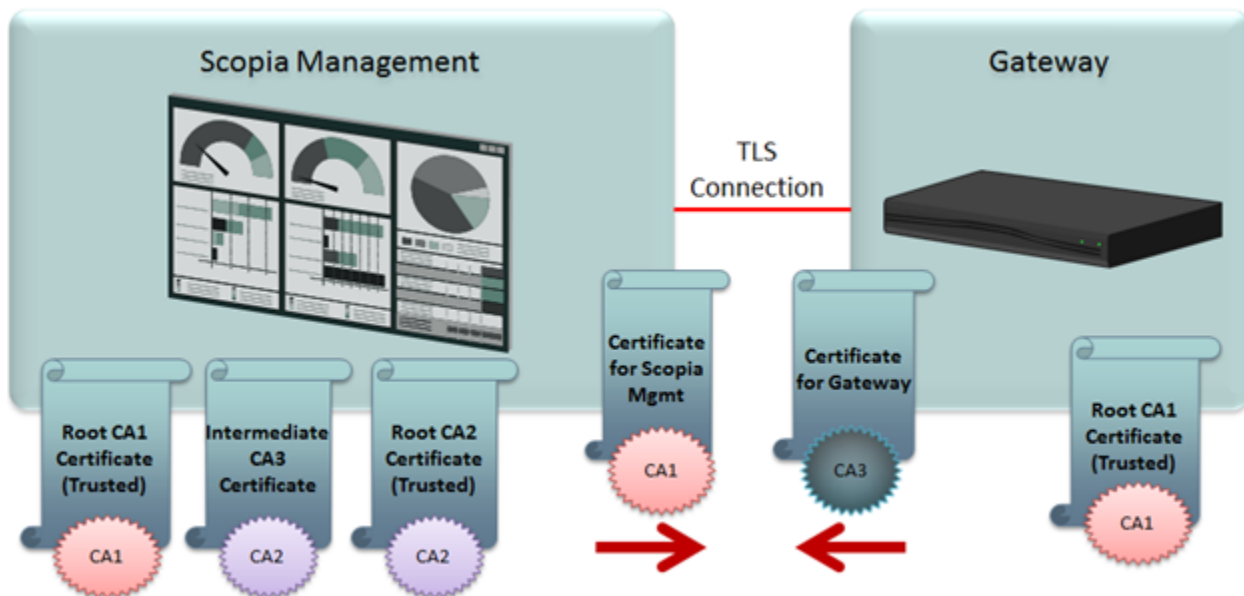


Figure 86: Signature of Gateway Certificate from Unknown CA

When CA3 is untrusted ([Figure 86: Signature of Gateway Certificate from Unknown CA](#) on page 146), the certificates to upload to the Scopia® Management are:

- A certificate identifying Scopia® Management, signed by trusted CA1. This is sent to the gateway as part of the TLS negotiation.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by Scopia® Management to authenticate its certificate.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA2. This is used to trust the certificate sent by the gateway, which is signed by CA3.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by Scopia® Management to authenticate the intermediate certificate, which is signed by CA2.

On the gateway side, the certificates to be uploaded are ([Figure 86: Signature of Gateway Certificate from Unknown CA](#) on page 146):

- A certificate identifying the gateway, signed by CA3, an unknown CA. This certificate is sent to Scopia® Management as part of the TLS negotiation.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the certificate sent by Scopia® Management, which is signed by CA1.

• Unknown Scopia® Management CA

When Scopia® Management's certificate is signed by a CA unknown to the gateway, you must upload an intermediate certificate for the untrusted CA signed by a trusted CA to vouch for its authenticity.

In the example of [Figure 87: Signature of Scopia® Management Certificate from Unknown CA](#) on page 147, Scopia® Management's certificate is signed by CA3, an unknown CA, while the gateway's certificate is signed by CA2, a trusted CA. This requires four certificates to be uploaded to Scopia® Management and three for the gateway ([Figure 87: Signature of Scopia® Management Certificate from Unknown CA](#) on page 147).

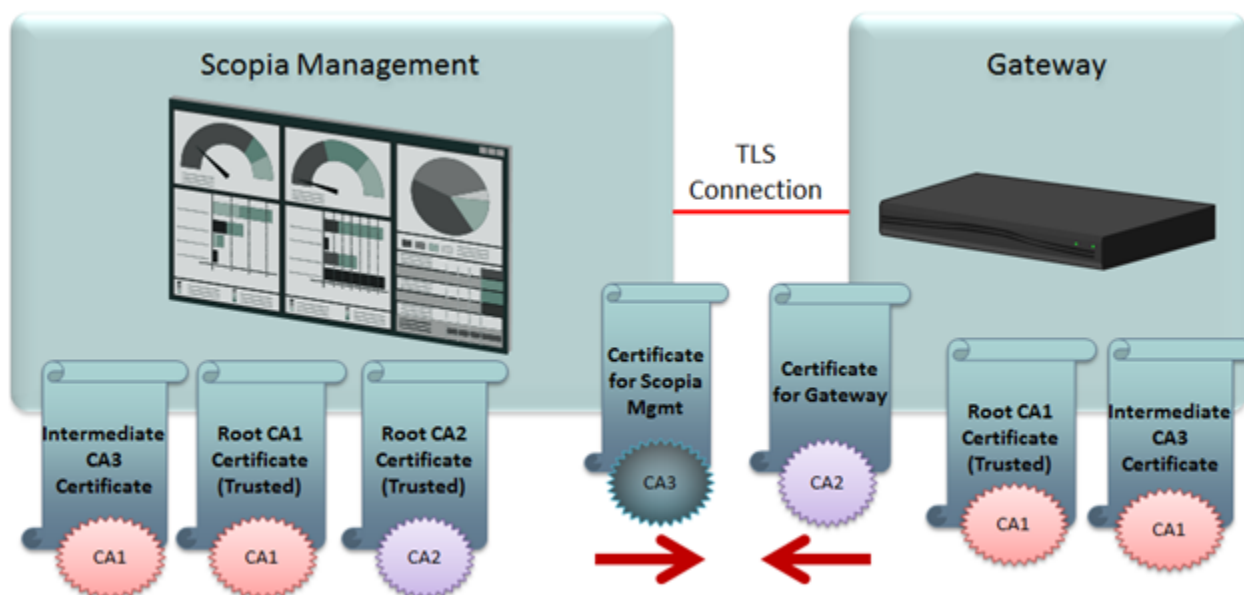


Figure 87: Signature of Scopia® Management Certificate from Unknown CA

When CA3 is untrusted by the gateway ([Figure 87: Signature of Scopia® Management Certificate from Unknown CA](#) on page 147), the certificates to upload to the Scopia® Management are:

- A certificate identifying Scopia® Management, signed by CA3, a CA unknown to the gateway. This is sent to the gateway as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Scopia® Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by Scopia® Management to authenticate the intermediate certificate, which was signed by CA1.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by Scopia® Management to authenticate the gateway's certificate, which is signed by CA2.

On the gateway side, the certificates to be uploaded are ([Figure 87: Signature of Scopia® Management Certificate from Unknown CA](#) on page 147):

- A certificate identifying the gateway, signed by trusted CA2. This certificate is sent to Scopia® Management as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Scopia® Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the intermediate certificate, which is signed by CA1.

• Mutually unknown CAs

In the final scenario, both components use certificates signed by CA's which are not recognized by each other. In this case, there needs to be two intermediate certificates, one for each of the untrusted CAs, to vouch for their authenticity.

For example, in [Figure 88: Signature of Both Certificates are from Untrusted CAs](#) on page 148, the certificate identifying the gateway is signed by CA4, an unknown CA, while Scopia® Management's certificate is signed by CA3, also untrusted. This would require five certificates to be uploaded to Scopia® Management and three for the gateway ([Figure 88: Signature of Both Certificates are from Untrusted CAs](#) on page 148).

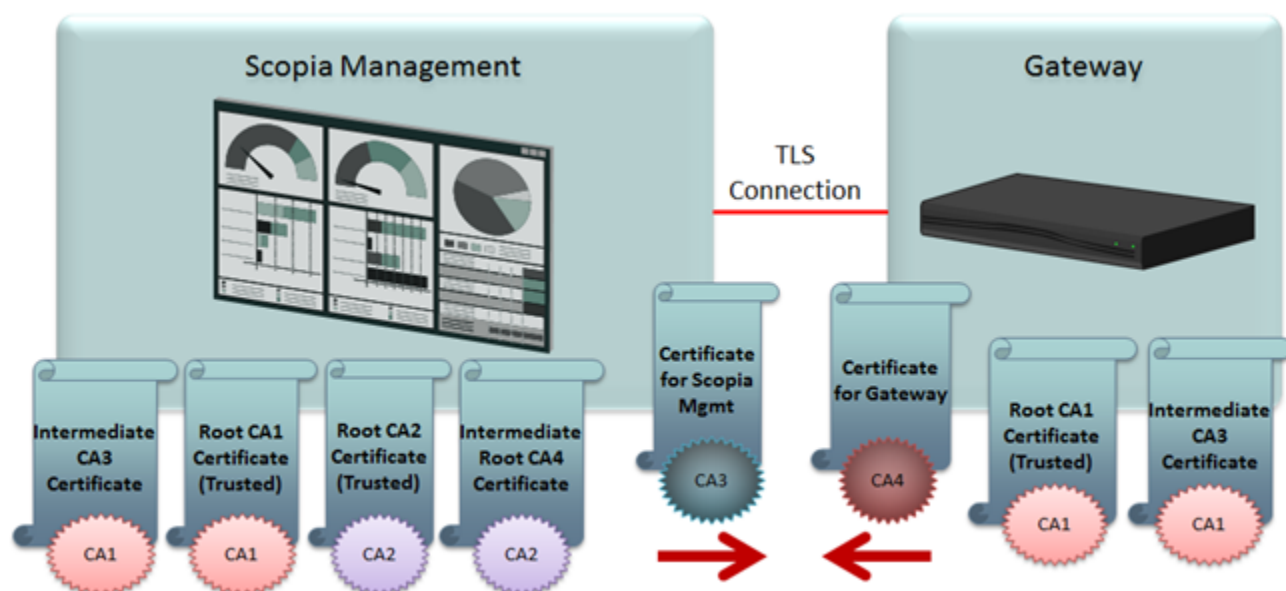


Figure 88: Signature of Both Certificates are from Untrusted CAs

When CA3 is untrusted by the gateway and CA4 is untrusted by Scopia® Management ([Figure 87: Signature of Scopia® Management Certificate from Unknown CA](#) on page 147), the certificates to upload to the Scopia® Management are:

- A certificate identifying Scopia® Management, signed by CA3, a CA unknown to the gateway. This is sent to the gateway as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Scopia® Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by Scopia® Management to authenticate CA3's intermediate certificate, which was signed by CA1.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by Scopia® Management to authenticate CA4's intermediate certificate, which is signed by CA2.
- An intermediate certificate vouching for the trustworthiness of CA4, signed by trusted CA2. This is used to trust the gateway's identity certificate, which is signed by CA4.

On the gateway side, the certificates to be uploaded are ([Figure 87: Signature of Scopia® Management Certificate from Unknown CA](#) on page 147):

- A certificate identifying the gateway, signed by CA4, a CA unknown to Scopia® Management. This is sent to Scopia® Management as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust Scopia® Management's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the intermediate certificate, which is signed by CA1.

For more information on uploading certificates to the gateway and to Scopia® Management, see *Administrator Guide for Scopia Management*.

If you have the Scopia® Management redundant solution, it is important to configure redundancy before proceeding with TLS configuration. See [Creating a Redundant Secondary Server for Scopia® Management](#) on page 223 for details.

Creating and Uploading Scopia® Management's Certificate for Videoconferencing Components

About this task

This section explains how to generate and upload the TLS certificate for Avaya Scopia® Management that is used for encrypting communications between Scopia® Management and other components of your video deployment.

! 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.

To create a TLS certificate, you need to generate a certificate signing request (CSR) and send it to the certification authority (CA) for signing. A CA has its own certificate, known as the CA root certificate. When the CA signed certificate is ready, you upload it into the component for which it was created, together with the CA root certificate. Once this is done, the component can authenticate itself and is ready for TLS connection.

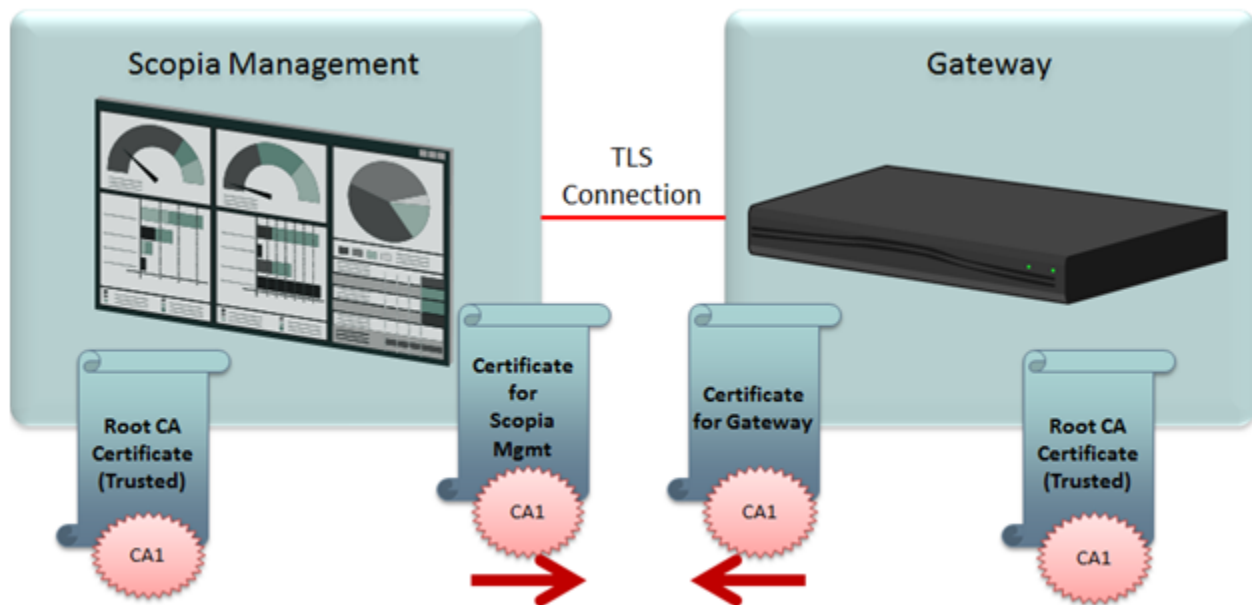


Figure 89: Typical TLS communication with a gateway

However, if the component certificates are signed by a different CA than Scopia® Management's certificate, you may need to upload more certificates to establish authenticity, as described in [Uploading Root and Intermediate Certificates for Scopia® Video Gateway, Avaya Scopia® TIP Gateway or Other Devices](#) on page 155. For more information about which certificates are required, see [Planning the Required Certificates for TLS](#) on page 142.

! Important:

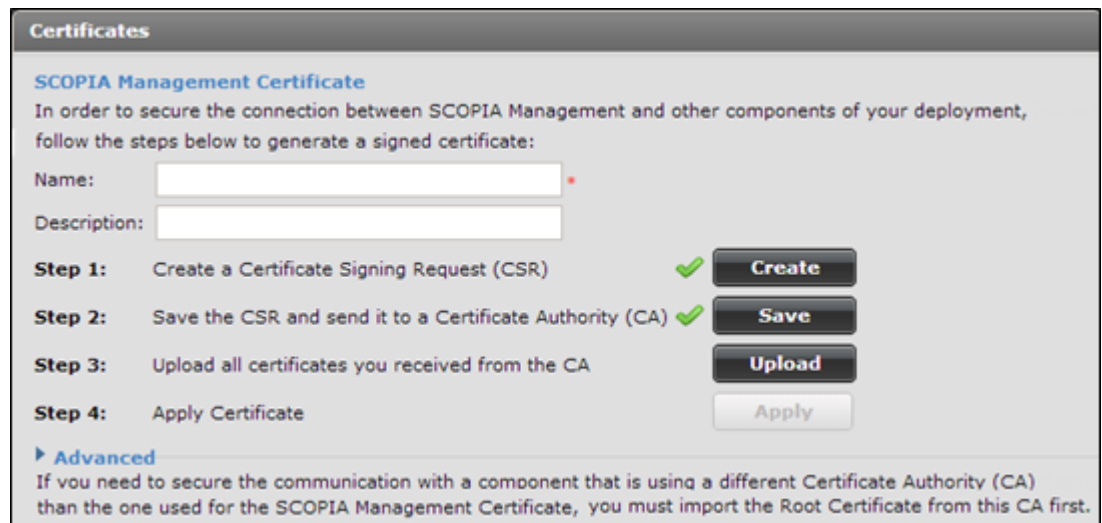
Scopia® Management uses two different TLS certificates for authenticating itself, one for Scopia® Desktop server and another for the rest of the videoconferencing devices. To secure communications between Scopia® Management and Scopia® Desktop server, generate and upload another TLS certificate for Scopia® Management as described in [Creating and Uploading the Scopia® Management's Certificate for Scopia® Desktop server](#) on page 153.

Before you begin

If you have the Scopia® Management redundant solution, it is important to configure redundancy before proceeding with TLS configuration. See [Creating a Redundant Secondary Server for Scopia® Management](#) on page 223 for details.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Security > Certificates**.
The **Scopia® Management Certificate** page appears.
To replace the certificate that is currently installed, select **New**.



The screenshot shows the 'Certificates' section of the Scopia Management administrator portal. It features a title 'SCOPIA Management Certificate' and an introductory paragraph: 'In order to secure the connection between SCOPIA Management and other components of your deployment, follow the steps below to generate a signed certificate:'. Below this are two input fields: 'Name:' and 'Description:'. A four-step process is listed: Step 1: 'Create a Certificate Signing Request (CSR)' with a green checkmark and a 'Create' button; Step 2: 'Save the CSR and send it to a Certificate Authority (CA)' with a green checkmark and a 'Save' button; Step 3: 'Upload all certificates you received from the CA' with an 'Upload' button; and Step 4: 'Apply Certificate' with an 'Apply' button. An 'Advanced' section is expanded, showing a note: 'If you need to secure the communication with a component that is using a different Certificate Authority (CA) than the one used for the SCOPIA Management Certificate, you must import the Root Certificate from this CA first.'

Figure 90: Scopia® Management Certificate

3. Enter a name used to identify this certificate in the **Name** field.
4. If necessary, enter a description of the certificate in the **Description** field.
5. Select **Create**.
The **Generate CSR** window appears.

Figure 91: Certificate Signing Request window

6. In the **Generate CSR** window, enter your organization's details as described below:

Field	Description
Common Name	Enter the Scopia® Management FQDN, for example, rvcn-sm.company.com. For a redundancy deployment, the common name must be the public virtual FQDN.
Country code	Enter the standard country code that consists of two characters, for example <i>uk</i> for United Kingdom or <i>jp</i> for Japan. This field is not case sensitive.
Encryption Strategy	Select the code for your organization's encryption strategy.
Signature Algorithm	Select the algorithm to use when generating the signature on the certificate. This algorithm is a combination of the private keys of both the CA and the device.

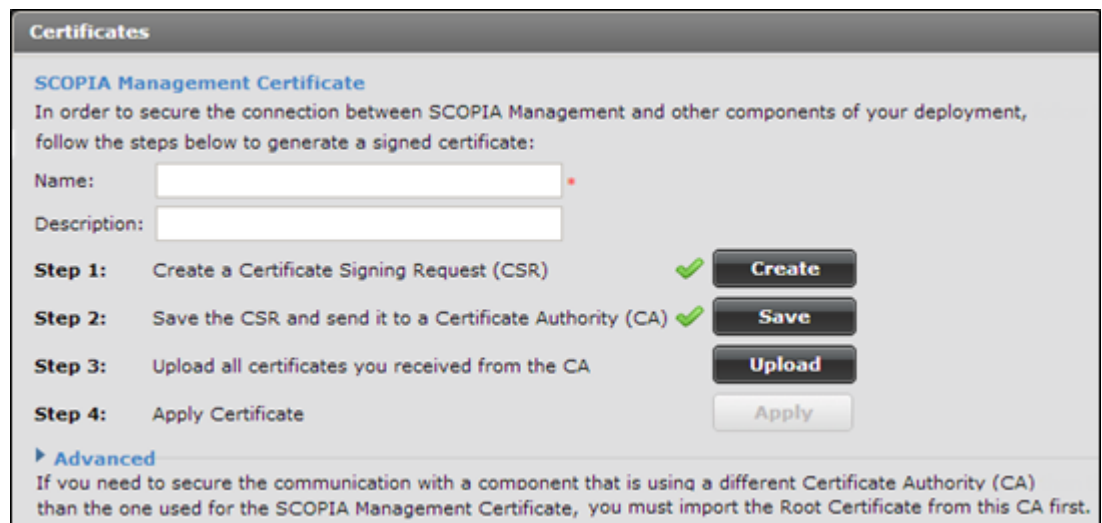
7. Select **Generate CSR**.
8. Select **Save** to view the certificate content. The certificate content is displayed in the **Download** window.
9. Save the certificate in an appropriate folder. The certificate is saved as a text file compatible with Base-64 ASCII code.

10. Send the text file containing the certificate for signing as a certificate compatible with Base-64 ASCII code. Select **Web Server** as the certificate template when submitting a certificate request.

! Important:

If other components communicating with Scopia® Management also have their own certificates, we recommend using a common CA for all certificates for a more efficient implementation.

11. Once the CA returns the signed certificate, copy the CA root certificate and the signed certificate that confirm the identity of Scopia® Management into the Scopia® Management server.
12. In the Scopia® Management administrator portal, select **Settings > Security > Certificates**.



The screenshot shows the 'Certificates' configuration page in the Scopia Management administrator portal. The page title is 'Certificates'. Below the title, it says 'SCOPIA Management Certificate'. The main text reads: 'In order to secure the connection between SCOPIA Management and other components of your deployment, follow the steps below to generate a signed certificate:'. There are two input fields: 'Name:' and 'Description:'. Below these, there are four steps listed with corresponding buttons: Step 1: 'Create a Certificate Signing Request (CSR)' with a 'Create' button; Step 2: 'Save the CSR and send it to a Certificate Authority (CA)' with a 'Save' button; Step 3: 'Upload all certificates you received from the CA' with an 'Upload' button; Step 4: 'Apply Certificate' with an 'Apply' button. There are green checkmarks next to Steps 1 and 2. At the bottom, there is an 'Advanced' section with a blue arrow icon and text: 'If you need to secure the communication with a component that is using a different Certificate Authority (CA) than the one used for the SCOPIA Management Certificate, you must import the Root Certificate from this CA first.'

Figure 92: Uploading certificates into Scopia® Management

13. Select **Upload** to import the certificate files into Scopia® Management. Include the signed certificate, its CA root certificate, and any intermediate certificates if required.

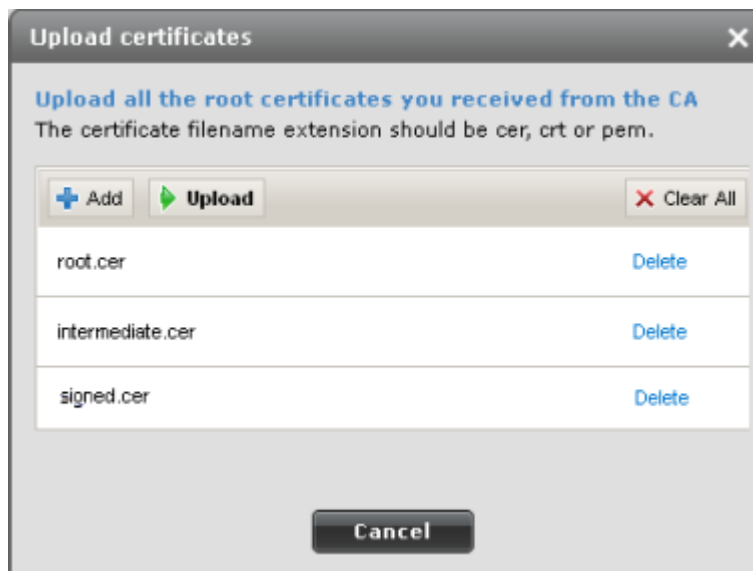


Figure 93: Defining the certificates to be uploaded

Do the following for each certificate:

- a. Select **Add** to browse to the certificate files.
Browse to the certificate.
- b. Select **Open**.
- c. Select **Upload**. Verify the system displays the successful upload message.
The certificate is uploaded into Scopia® Management.

14. Select **Apply**.

15. To finish applying the certificates, select **Yes** to restart Scopia® Management.

16. Continue with generating the CSR for the device's certificates and uploading certificates onto them as described in [Securing Your Video Network Using TLS](#) on page 139.

Creating and Uploading the Scopia® Management's Certificate for Scopia® Desktop server

About this task

This section explains how to generate and upload a certificate signing request (CSR) for Avaya Scopia® Management that is used for encrypting communications between Scopia® Management and Avaya Scopia® Desktop server.

! 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.

To create a TLS certificate, you need to generate a certificate signing request (CSR) and send it to the certification authority (CA) for signing. A CA has its own certificate, known as the CA root certificate. When the CA signed certificate is ready, you upload it into the component for which it was created,

together with the CA root certificate. Once this is done, the component can authenticate itself and is ready for TLS connection.

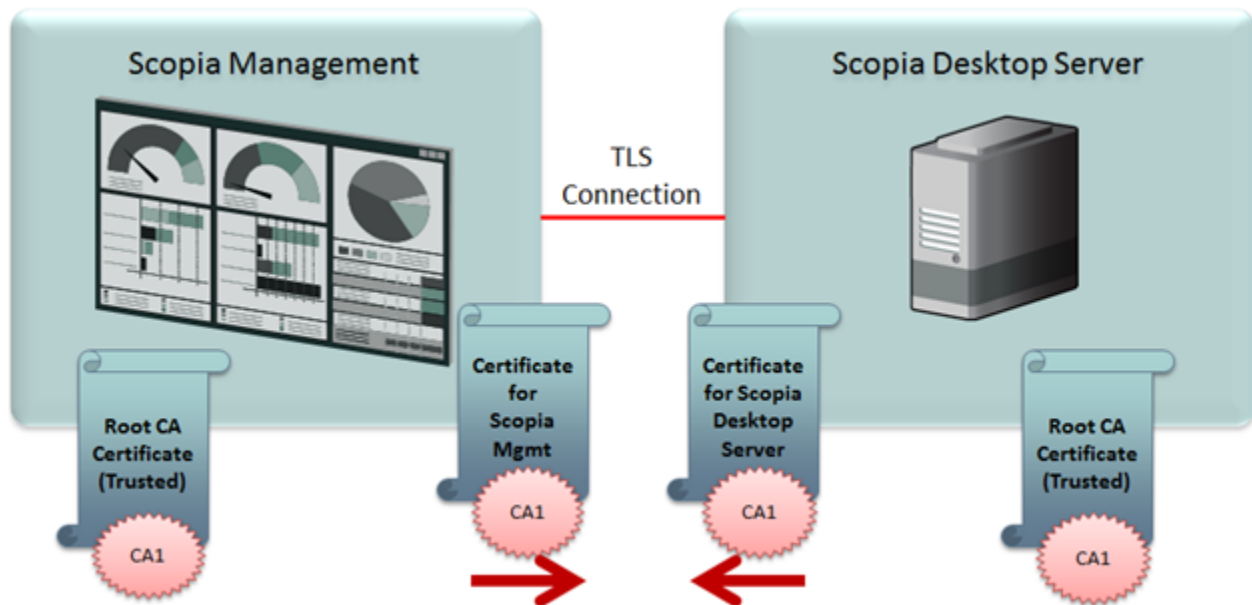


Figure 94: Typical TLS communication with a Scopia® Desktop server

Make sure that you use the same CA for signing certificates for both Scopia® Management and Scopia® Desktop server for a more efficient process.

! Important:

Scopia® Management uses two different TLS certificates for authenticating itself, one for Scopia® Desktop server and another for the rest of the videoconferencing devices. To secure communications between Scopia® Management and videoconferencing components other than Scopia® Desktop server, perform the procedure described in [Creating and Uploading Scopia® Management's Certificate for Videoconferencing Components](#) on page 148.

Procedure

1. Copy the .keystore file located in `<SM_install_dir>\iCM\tomcat\certificate\sds.keystore` to a temporary working folder, for example `C:\cert`. The keystore file holds the certificates on each server. Currently they hold the default non-unique certificates.

! Important:

The password on the .keystore file is radvision.

2. Open a command line window. The keytool utility is located in `<SM_install_dir>\JRE\bin`.
3. Use the keytool utility to remove the pre-installed certificate from the .keystore file with the -delete parameter. The default certificate has an alias of default:

```
keytool -delete -alias default -keystore sds.keystore -storepass radvision
```

4. Generate a unique key pair using an appropriate DN with the `-genkeypair` parameter:

```
keytool -genkeypair -keyalg RSA -alias sds -sigalg MD5withRSA -dname "CN=<FQDN of server>"  
-keystore sds.keystore -storepass radvision -validity 365 -keysize 1024
```

5. Create a certificate signing request file (CSR) for the newly generated key pair using the `-certreq` parameter:

```
keytool -certreq -alias sds -sigalg MD5withRSA -keystore sds.keystore -storepass radvision  
-file C:\cert\certreq.csr
```

6. Send the certificate request to a Certificate Authority.

7. The CA returns the certificate signed in form of `.crt` file, for example `signed_cert.crt`. It also returns a root certificate, `root_cert.crt`.

8. Import the root certificate of the CA into the keystore file using the `-import` parameter:

```
keytool -import -trustcacerts -alias root -file root_cert.crt -keystore sds.keystore  
-storepass radvision
```

where `root_cert.crt` is the trusted root certificate.

The `trustcacerts` parameter instructs `keytool` to check both the specific and the `system.keystore` file for the root certificate.

9. Import the signed certificate into the keystore file. Use the same alias you used in step [8](#).

```
keytool -import -trustcacerts -alias sds -file signed_cert.crt -keystore sds.keystore  
-storepass radvision
```

`Keytool` issues a confirmation message if the certificate was uploaded successfully.

10. Copy the `.keystore` file back to its original location.

11. Restart the services on the Scopia® Management.

Uploading Root and Intermediate Certificates for Scopia® Video Gateway, Avaya Scopia® TIP Gateway or Other Devices

About this task

Perform this procedure only if the component's certificates are signed by a different CA than Scopia® Management's certificate.

This procedure describes how to import the root and intermediate certificates to Scopia® Management for devices in your deployment. Root and intermediate certificates establish the trustworthiness of each CA's signature by vouching for the CA in question. To learn about different types of certificates, read [Planning the Required Certificates for TLS](#) on page 142.

 Important:

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

Before you begin

- Ensure that you have the signed certificate, root certificate, and all intermediate certificates required for proper authentication of the device. The root certificate must be compatible with the Base-64 ASCII code.
- You must first upload the certificate identifying the device, as follows:
 - To upload certificates identifying Scopia® Video Gateway, refer to the the *Lync Deployment Guide for Scopia® Video Gateway* or the *OCS Deployment Guide for Scopia® Video Gateway for Scopia® Video Gateway* .
 - To upload certificates identifying Avaya Scopia® TIP Gateway, refer to the *Deployment Guide for Avaya Scopia® TIP Gateway*.
 - To upload certificates identifying other devices, see the product's Administrator Guide for details.

 Important:

Skip this step for the Microsoft Lync Server and the Microsoft Office Communications Server.

Procedure

1. Copy the CA root, intermediate, and signed certificate that confirms the identity of the CA into the Scopia® Management server.
2. Access the Scopia® Management administrator portal.
3. Select **Settings > Security > Certificates > Advanced**.

Certificates

SCOPIA Management Certificate

In order to secure the connection between SCOPIA Management...

Name: iView Certificate

Description:

Expiration Date: Oct 18, 2013

Status: Valid

New **Download Root Certificate**

▼ **Advanced**

If you need to secure the communication with a component that i...
Certificate from this CA first.

Import **Revoke** **Apply**

	Name	Description
--	------	-------------

Figure 95: Upload certificates for other devices

4. Select **Import**.
5. Select **Add**, browse to the required root or intermediate certificate and select **Open**.
6. Repeat the previous step for every root or intermediate certificate that you need to upload.
7. Select **Upload**.

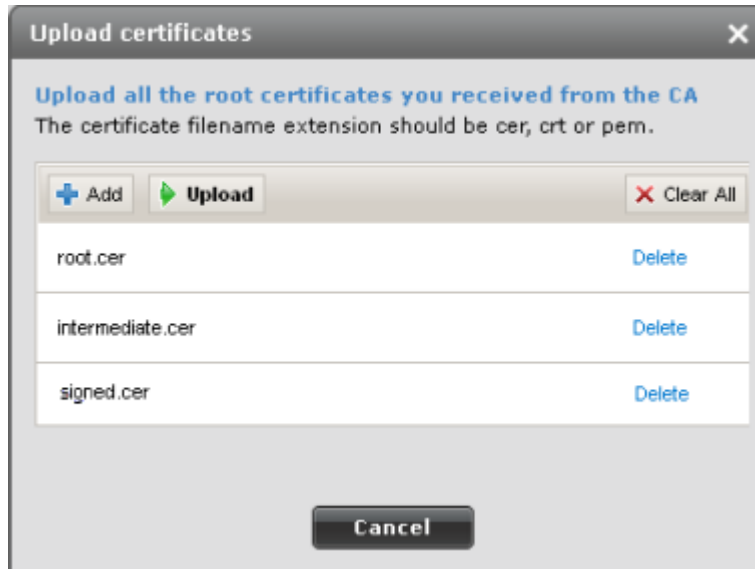


Figure 96: Importing certificates for other devices into Scopia® Management

8. Select all certificates you uploaded and select **Apply**. The system prompts for a restart to implement the newly uploaded certificates.

Enabling the TLS Connection in Scopia® Management

About this task

You can configure your Scopia® Management to use the TLS connection by modifying the configuration of the B2BUA component of the Scopia® Management.

Perform this procedure only if you want to secure your video network using TLS.

❗ 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. Navigate to `<install_dir>\sipserver\conf`.
2. Open the `UpdatedSIPConfig.xml` file in a text editor.
3. Configure FQDN of the B2BUA component by setting the value the `<B2bFQDN>` element as shown in [Figure 97: Adding the B2bFQDN element](#) on page 159. In a redundancy environment, add the FQDN of the public virtual IP address. In a standalone environment, this is automatically added.

```

<SipServerConfiguration>
  <SIPStack>
    <Network>
      <LocalTcpAddressList>127.0.0.1:5060</LocalTcpAddressList>
      <LocalUdpAddressList>127.0.0.1:5060</LocalUdpAddressList>
      <LocalTlsAddressList>127.0.0.1:5061</LocalTlsAddressList>
      <B2bFQDN>rvcndev.radvision.com</B2bFQDN>
    </Network>
  </SIPStack>
</SipServerConfiguration>

```

Figure 97: Adding the B2bFQDN element

4. Configure the DNS of the B2BUA component by setting values in the entire <DNSServerList> element as shown in [Figure 98: Adding the <DNSServerList> element](#) on page 159:

```

<Stack>
  <StackTcpEnabled>true</StackTcpEnabled>
  <StackSendReceiveBufferSize>10000</StackSendReceiveBufferSize>
  <StackTLSEnabled>true</StackTLSEnabled>
  <StackNumOfTlsEngines>2</StackNumOfTlsEngines>
  <StackMaxTlsSessions>1000</StackMaxTlsSessions>
  <TLSMethod>TLS_V1</TLSMethod>
</Stack>
<DNSServerList>
  <DNSServerIP>192.168.227.233</DNSServerIP>
  <DNSServerIP>192.168.227.253</DNSServerIP>
  <DNSServerIP>192.168.225.1</DNSServerIP>
</DNSServerList>
</SIPStack>

```

Figure 98: Adding the <DNSServerList> element

5. Save and close the file.
6. Restart the Scopia® Management service and the Scopia® Management SIP service.

Chapter 5 | Defining and Managing Video Users

This section is relevant for enterprise deployments.

This section explains how administrators can add and manage users.

After adding new users, you can organize users in groups and assign profiles to them. Usually users are grouped based on their location (time zone) or organization unit (for example, a branch, department or workgroup). A user profile is a group of user-related capabilities and rights, such as, available meeting types and ability to schedule meetings ([Figure 99: Using groups and profiles to define a user](#) on page 160).

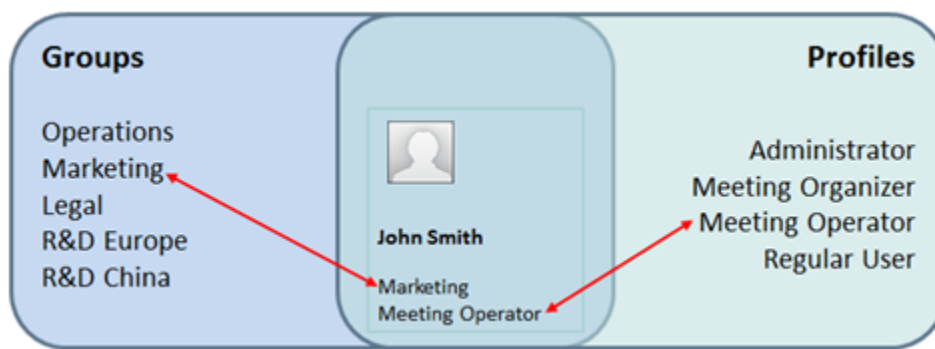


Figure 99: Using groups and profiles to define a user

Users, user profiles and user groups can be defined within Scopia® Management, or sourced directly from the organization's external LDAP server, interfacing with Microsoft's Active Directory or IBM's Domino. When an LDAP is used, the connection between Scopia® Management and the LDAP server must be configured (see [Connecting Scopia® Management with the LDAP Server](#) on page 172).

Licenses are also managed via user profiles. To enable a Scopia® User license for a user or group of users, assign your Scopia® User licenses to a profile, and then assign this profile to this user or group of users. For more information about Scopia® User licenses, see [Planning Licenses for Integration with Aura Collaboration Suite](#) on page 22.

When you add users for the first time in Avaya Scopia® Management, we recommend following this workflow:

1. Upload Scopia® User licenses to the Avaya Web License Manager (WebLM) server (see [Deploying Scopia® User and Endpoint Licenses in Scopia® Management](#) on page 25).
2. Define user profiles as described in [Creating or Modifying a User Profile](#) on page 162. A user profile is a compilation of user-related capabilities and rights, such as the ability to schedule meetings. The purpose of having user profiles in Scopia® Management is to configure and modify rights and capabilities for all users sharing this profile, instead of doing it for every user individually.
3. Define user groups as described in [Creating a User Group](#) on page 169. You can unify users into groups to manage and maintain users on a group level. Usually users are joined together based on their location (time zone) or organization unit (for example, a branch, department or workgroup).
4. If you are using a third-party LDAP server such as Microsoft Active Directory, download users as described in [Downloading Users from the LDAP Server](#) on page 175.

--Or--

If you are using Scopia® Management's internal LDAP server, create users as described in [Creating a User within Scopia® Management](#) on page 178.

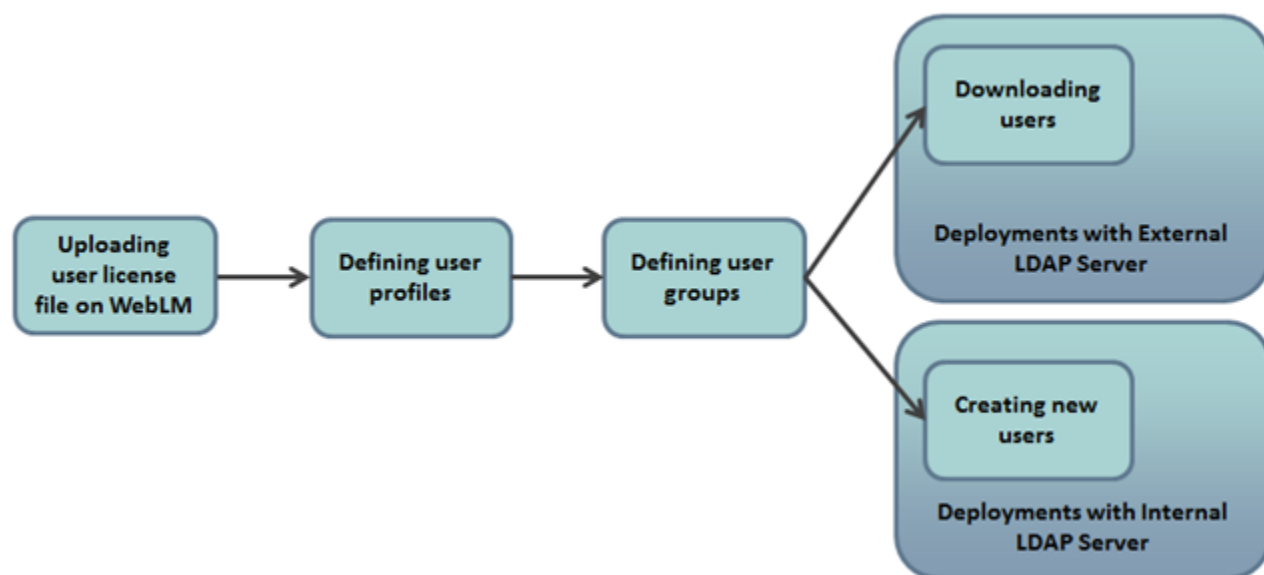


Figure 100: Workflow for defining users in Avaya Scopia® Management

You can modify and delete user profiles and user groups. To delete a user group or a user profile you need to make sure no users are assigned to it.

Navigation

- [Managing User Profiles](#) on page 161
- [Managing User Groups](#) on page 168
- [Managing Video Users](#) on page 171
- [Managing Virtual Rooms](#) on page 184
- [Creating an Invitation Template](#) on page 189

Managing User Profiles

This section is relevant only for enterprise deployments.

A user profile is a compilation of user-related capabilities and rights, such as available meeting types, ability to schedule meetings, access to the Scopia® Desktop and Scopia® Mobile functionality, allowed bandwidth for Scopia® Desktop calls. The purpose of having user profiles in Scopia® Management is to configure and modify rights and capabilities for all users sharing this profile, instead of doing it for every user individually. Typically you create profiles that correlate with user roles in the organization (for example, administrators, read-only users) or profiles using different features (for example, users who use the lecture meeting type and are not allowed to schedule meetings).

There are four preconfigured user profiles:

- Administrator
- Meeting Organizer

- Meeting Operator
- Regular User

You can modify settings for the preconfigured profiles, except their names and short descriptions. You cannot delete preconfigured profiles.

You can assign profiles to individual users and to user groups. When you assign a user profile to a group, you can still assign a different profile to individual users within this group.

Defining user profiles is the first stage of user definition, as shown in [Figure 100: Workflow for defining users in Avaya Scopia® Management](#) on page 161.

Navigation

- [Creating or Modifying a User Profile](#) on page 162
- [Defining Scopia® Desktop Bandwidth for a User Profile](#) on page 164
- [Customizing a User Profile](#) on page 165
- [Deleting a User Profile](#) on page 167

Creating or Modifying a User Profile

About this task

A user profile is a compilation of user-related features and rights, such as available meeting types, ability to schedule meetings, access to the Scopia® Desktop and Scopia® Mobile functionality. This section explains how to create a new user profile or modify an existing one. For more information, see [Managing User Profiles](#) on page 161.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Settings** tab.
3. Select **Users > Profiles**.
4. Select **Add**.
or
Select the user profile that you want to modify.

User Profile: Administrator

General

Profile Name: Administrator *

Description: Used as the default profile for organization adminis

User Capabilities

☒ Can access Scopia Management administrator portal

☒ Full administrator access

☐ Read-only with meeting control access

☐ Read-only

☒ Enable Scopia user licenses

☒ Can schedule meetings

☒ Can invite endpoints and reserve resources

☒ Can view all meetings in the user portal

☒ Can moderate all meetings without entering PIN

Meeting Types

Select the meeting types allowed for this user profile

☒	Meeting Type Prefix	Meeting Type
☒	N/A	Point to Point
☒	71	Default Service

Figure 101: Determining the properties of a user profile

5. Enter the profile name and a short description.
We recommend that the profile name should be self explanatory.
6. Select the user capabilities and functionality that you want to enable for this user:

Table 39: User profile capabilities

Capability	Description
Can access Avaya Scopia® Management administrator portal	A user can log into the Avaya Scopia® Management administrator portal. You can choose from the following permissions: • Full administrator access: A user can view and modify all settings. • Read-only with meeting control access: A user can view all settings without modifying, but can schedule, moderate, and delete meetings. • Read-only: A user can only check settings or monitor meetings in progress, without changing any settings.
Enable Scopia® User licenses	Select to assign those in this profile a Scopia® User license. For information about licenses, see Planning Licenses for Integration with Aura Collaboration Suite on page 22.
Can schedule meetings	A user can schedule meetings from the Avaya Scopia® Management Web Portal.
Can invite endpoints and reserve resources	A user can schedule meetings which require inviting endpoints and reserving resources, for example, an MCU.
Can view all meetings in the user portal	If this option is enabled, a user can view all upcoming and ongoing meetings at the Avaya Scopia® Management portal; if this option is disabled, the user can see only his or her meetings: started by this user or meetings this user joined by the invitation of others.
Can moderate all meetings without entering PIN	A user can have moderator rights in other users' virtual rooms even without entering the moderator PIN.

7. Select the required meeting types.
8. To control consumed bandwidth, configure settings as described in [Defining Scopia® Desktop Bandwidth for a User Profile](#) on page 164.
9. Select **Apply**.

Defining Scopia® Desktop Bandwidth for a User Profile

About this task

Scopia® Desktop bandwidth limits are defined per user profile. This procedure describes how to define bandwidth limits allowed for the following types of Scopia® Desktop users:

- Users authenticated via Scopia® Desktop: Configure bandwidth settings per user profile.
- Users that have not been authenticated via Scopia® Desktop server (guest users): Configure the global bandwidth settings for guests.

❗ Important:

A Scopia® Desktop Pro or Mobile license is required to authenticate users. See the *Installation Guide for Scopia® Desktop* for more details.

Scopia® Management does not manage Scopia® Desktop calls, although you can configure bandwidth for Scopia® Desktop calls within Scopia® Management. This setting is retrieved by the Scopia® Desktop that actually manages the calls.

Procedure

1. Access the Scopia® Management administrator portal.
 2. Select the **Settings** tab.
 3. Define bandwidth for Scopia® Desktop users per user profile, as follows:
 - a. Navigate to **Users > Profiles** from the sidebar.
 - b. Expand the **Advanced** section at the bottom of the **User Profile** page.
 - c. (Optional) To limit desktop and mobile calls to audio-only, select the checkbox.
This option is useful, for example, to keep bandwidth consumption as low as possible.
 - d. Select a value from the **Maximum bandwidth allowed for Scopia® Desktop calls** field.
 - e. Select **Apply** to save your changes.
 4. Define bandwidth for Scopia® Desktop guest users, as follows:
 - a. Navigate to **Users > Policies** in the sidebar menu.
 - b. (Optional) To limit desktop and mobile calls to audio-only, select the checkbox.
 - c. Select a value from the **Maximum bandwidth allowed for Scopia® Desktop calls** field.
 - d. Select **Apply** to save your changes.
-

Customizing a User Profile

About this task

You can customize a user profile for a particular user, if preconfigured profiles do not match needs of this particular user.

! Important:

After you decouple this username from its profile, any future changes to the profile will not impact on this user, since now it has a custom profile. Too many custom profiles will add to the management overhead of user rights.

For example, if you customize the "Guest" profile for one of the users not to view all meetings in the user portal, the rest of the users who are assigned the same profile will still be able to do it.

To edit the properties of a profile for all users in that profile, or to create a new profile, see [Creating or Modifying a User Profile](#) on page 162.

Procedure

1. Access the Avaya Scopia® Management administrator portal.
2. Select the **Users** tab.
3. Select **All** under **Users from Local Directory** or **Users from Active Directory**.
4. Select the user for whom you want to assign a different profile.

The screenshot shows the 'User' settings page in the Avaya Scopia Management administrator portal. The 'User' tab is selected, and the 'Virtual Room' tab is also visible. The form displays the following fields and values:

- Username: London_admin
- First Name: John
- Last Name: Smith
- Password: [Redacted]
- Confirm Password: [Redacted]
- Email: johnsmith@company.com
- Telephone (Office): +121230056
- Telephone (Mobile): +121230057
- Personal endpoint: [Empty]
- Groups: [Empty]
- User Profile: Custom User Profile (selected)
- Time Zone: GMT+08:00 China Standard Time (Asia/Chongqing)
- Location Preference: Auto
- Account Status: Enabled

Buttons at the bottom include 'Assign', 'Edit', 'OK', 'Apply', and 'Cancel'.

Figure 102: User page displaying user settings

5. Select **Custom User profile** from the **User Profile** list.
6. Select **Edit** and modify the user capabilities:

Table 40: User profile capabilities

Capability	Description
Can access Avaya Scopia® Management administrator portal	A user can log into the Avaya Scopia® Management administrator portal. You can choose from the following permissions: • Full administrator access: A user can view and modify all settings. • Read-only with meeting control access: A user can view all settings without modifying, but can schedule, moderate, and delete meetings. • Read-only: A user can only check settings or monitor meetings in progress, without changing any settings.
Enable Scopia® User licenses	You can assign or remove the Scopia® User license for this user. For information about licenses, see Planning Licenses for Integration with Aura Collaboration Suite on page 22.
Can schedule meetings	A user can schedule meetings from the Avaya Scopia® Management Web Portal.
Can invite endpoints and reserve resources	A user can schedule meetings which require inviting endpoints and reserving resources, for example, an MCU.
Can view all meetings in the user portal	If this option is enabled, a user can view all upcoming and ongoing meetings at the Avaya Scopia® Management portal; if this option is disabled, the user can see only his or her meetings: started by this user or meetings this user joined by the invitation of others.
Can moderate all meetings without entering PIN	A user can have moderator rights in other users' virtual rooms even without entering the moderator PIN.

7. Select the required meeting types.
8. To control consumed bandwidth, configure settings as described in [Defining Scopia® Desktop Bandwidth for a User Profile](#) on page 164.
9. Select **Apply**.

Deleting a User Profile

About this task

This section is relevant only for enterprise deployments.

A user profile is a compilation of user-related features and rights, such as available meeting types, ability to schedule meetings, access to the Scopia® Desktop and Scopia® Mobile functionality. For more information, see [Managing User Profiles](#) on page 161.

You can only delete empty user profiles which are not assigned to any users or user groups.

Procedure

1. Access the Scopia® Management administrator portal.
 2. Select the **Settings** tab.
 3. Select **Users > Profiles**.
 4. Select the user profiles you want to delete.
 5. Select **Delete**.
 6. Select **Yes** in the confirmation message.
-

Managing User Groups

You can unify users into groups to manage and maintain users on a group level. Usually users are joined together based on their location (time zone) or organization unit (for example, a branch, department or workgroup). You can assign the same user to more than one group. For example, if you have separate user groups for departments and locations, you can assign a user to both: the "R&D" group and the "China" group.

There are two types of user groups:

- Directory user groups

Directory groups are user groups defined in the external user directory (LDAP server) and imported to Scopia® Management as part of user provisioning. Directory groups cannot be edited or deleted from Scopia® Management. Changes to these user groups must be performed on the LDAP server.

- Local user groups

Local groups are created within Scopia® Management. You can modify and delete these groups in Scopia® Management. You cannot export local user groups into the LDAP server.

This section explains how to create and manage local user groups:

Navigation

- [Creating a User Group](#) on page 169

- [Modifying a User Group](#) on page 169
- [Removing a User Group](#) on page 170

Creating a User Group

About this task

You can unify users into groups to manage and maintain users on a group level. For more information about Scopia® Management user groups, refer to [Managing User Groups](#) on page 168.

Typically, you create user groups before creating or downloading users who need to use these user groups as shown in [Figure 100: Workflow for defining users in Avaya Scopia® Management](#) on page 161.

While creating a new user group, you can assign a user profile to it which allows to define settings for all users in this group, instead of doing it individually for every user. When you assign a user profile to a group all users belonging to this group are automatically assigned the same profile.

Important:

If necessary, you can later assign a profile that is different from the rest of the users in a group to individual users within this group.

User groups are created within Scopia® Management, and are *not* synchronized with LDAP servers, if your organization uses an LDAP server.

Procedure

1. Access the Scopia® Management administrator portal.
 2. Select the **Users** tab.
 3. Select **Group** under **Users from Local Directory** in the sidebar.
 4. Select **Add**.
 5. Enter a name for the group in the **Name** field.
 6. To assign a user profile to all users belonging to this group, select a user profile.
 7. Select **OK** to save your changes.
- The group appears on the **Groups** tab.
-

Modifying a User Group

About this task

Only user groups created within Scopia® Management can be modified. User groups imported from the external active directory cannot be edited or deleted.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Users** tab.
3. Select **Group** under **Users from Local Directory** in the sidebar.
4. Select the link in the **Name** column for the user group you want to modify.
5. Modify the name of the user group.
6. Change the default user profile of the group by selecting a different user profile from the **User Profile** list.
7. To assign the default user profile to users who had different profiles from the rest of the group, select **Reset**.

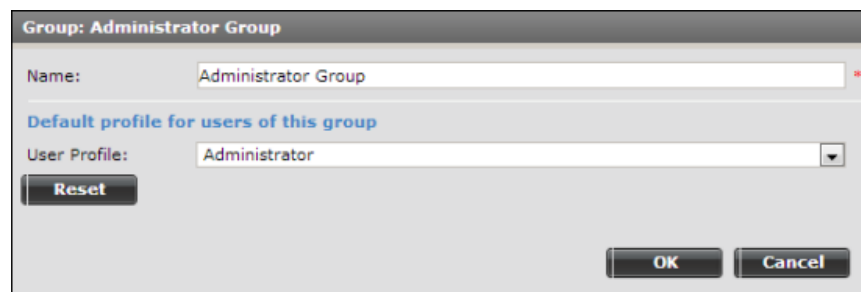


Figure 103: Clearing customized user profiles in a group

8. Select **Apply** to save your changes.

Removing a User Group

About this task

User groups are used to manage and maintain users on a group level. Only user groups created within Scopia® Management can be deleted. User groups imported from the external LDAP server cannot be deleted.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Users** tab.
3. Select **Group** under **Users from Local Directory** in the sidebar.
4. Select the group you want to delete.
5. Select **Delete** and then **Yes**.

The user group is deleted from the scheduler.

Managing Video Users

You can download users from an LDAP server, or you can manually add users to an Scopia® Management local directory.

In both cases you can modify users, however, if your organization is synchronized with an LDAP server to provision users, you can only modify the settings stored in Scopia® Management, such as virtual room, default endpoints, allowed meeting types, groups, and time zone. See [Managing Users from the LDAP Server](#) on page 171. The rest of the settings are overridden each time Scopia® Management synchronizes with the LDAP server.

Navigation

- [Managing Users from the LDAP Server](#) on page 171
- [Managing Users with a Local User Directory](#) on page 178
- [Modifying a User](#) on page 181
- [Assigning Groups to Multiple Users](#) on page 182
- [Searching for a User](#) on page 183

Managing Users from the LDAP Server

Scopia® Management integrates with Microsoft Active Directory and IBM Lotus Domino for easy user provisioning. When your organization uses an LDAP server, each user defined in this directory is downloaded to Scopia® Management, along with all the information associated with it.

You can associate Scopia® Management LDAP users or groups with Scopia® Management profiles and virtual rooms. For example, an LDAP group can have Scopia® Management administrator permissions or can automatically be assigned a virtual room. Endpoints are also defined in the LDAP server as users and can be downloaded and managed by Scopia® Management. See [Importing H.323 Endpoints from an External LDAP Server](#) on page 94.

Once all users are downloaded to Scopia® Management, Scopia® Management frequently synchronizes with the LDAP server to keep this information up-to-date.

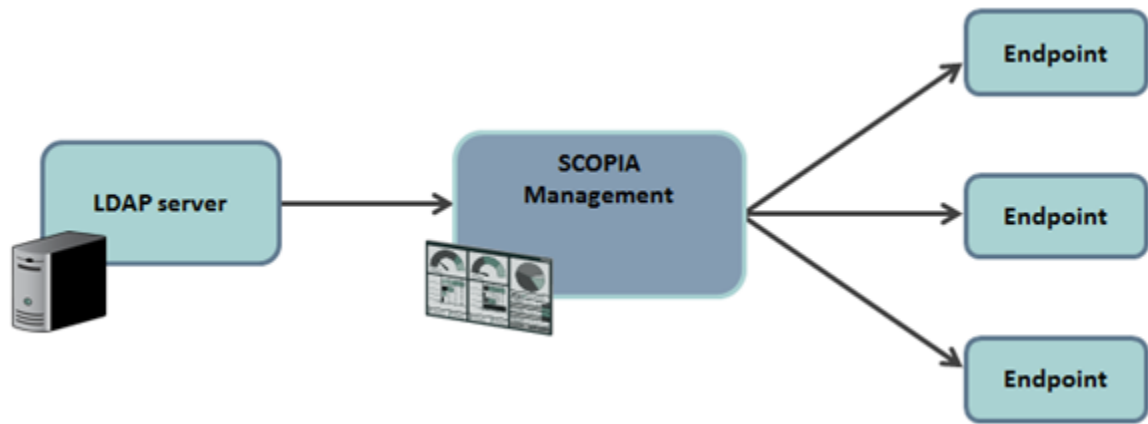


Figure 104: Synchronizing Scopia® Management with the LDAP server

You cannot delete users which are downloaded from the LDAP server.

Navigation

- [Connecting Scopia® Management with the LDAP Server](#) on page 172
- [Scopia® Management LDAP Information Attributes](#) on page 174
- [Downloading Users from the LDAP Server](#) on page 175
- [Synchronizing Users from the LDAP Server](#) on page 177

Connecting Scopia® Management with the LDAP Server

About this task

To allow user provisioning and synchronization of user profiles using an LDAP server, you have to configure the connection between Scopia® Management and the LDAP server.

Before you begin

Depending on your organization's policies and the LDAP server you are using, decide whether to secure its connection with Scopia® Management, as described in [Securing the Connection between Scopia® Management and an LDAP Server](#) on page 139.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Servers > LDAP Servers**.
3. Select **Add** to add a new LDAP server, or select the required LDAP server entry to modify an existing LDAP server connection.
4. Select the type of LDAP server in the **Directory Server Type** field.

If the Scopia® Video Gateway is part of your deployment, select **Active Directory Server**.

The screenshot shows the 'LDAP Server Settings' window with the 'Basic' tab active. The 'Directory Server Type' is set to 'Active Directory Server'. The 'URL/Domain' field contains 'ldap://...'. The 'Login ID' is 'administrator@ex2013' and the 'Password' is masked with dots. The 'LDAP Search Base' is 'CN=Users,DC=ex2013,DC=cn'. A 'Configure' button is located at the bottom right of the form.

Figure 105: Basic LDAP server settings

5. Enter the directory server domain or directory server URL in the **URL/Domain** field, using the *ldap://* prefix.

For a secured connection between the Scopia® Management and the LDAP server, do one of the following:

- Secure the connection with SSL certificates using the *ldaps://* prefix (with an 's'). You need to also set up SSL on the LDAP server itself, as described in its documentation.
- Secure the credentials with MD5 (Microsoft Active Directory only): Enter the FQDN here (not the IP address). You then secure the credentials at a later stage, as part of [Downloading Users from the LDAP Server](#) on page 175.

If securing user credentials, you cannot also secure the connection with the LDAP server.

6. Enter the directory server login ID and password in the relevant fields.

! Important:

The user account needs to have read access to all user accounts that you want to synchronize to Scopia® Management. This user account does not have to be part of the search base.

7. Select **Configure** to configure the **LDAP Search Base** field. The LDAP Tree window appears, showing all OUs (Organization Units) defined on the directory server. [Figure 106: Tree structure in an enterprise deployment](#) on page 174 illustrates the tree structure for an enterprise deployment.

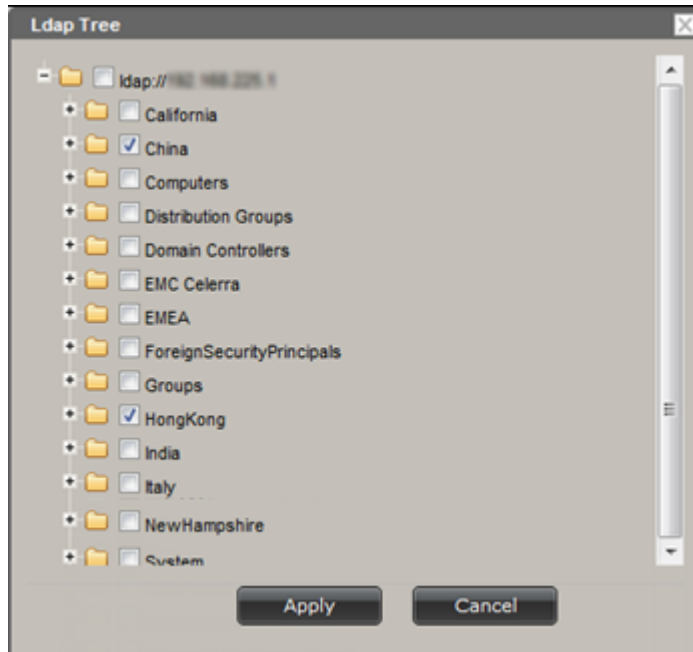


Figure 106: Tree structure in an enterprise deployment

8. Select the OUs whose users you want to download.
9. Select **Apply**. The selected OUs are displayed in the **LDAP Search Base** field.
10. Select **Apply**.
11. After your Scopia® Management is connected to the LDAP server, you can download users, as well as endpoints and virtual rooms:
 - To download users from the LDAP server, see [Downloading Users from the LDAP Server](#) on page 175.
 - To download endpoints, see [Importing H.323 Endpoints from an External LDAP Server](#) on page 94.
 - To download virtual rooms, see [Downloading Virtual Rooms from the LDAP Server](#) on page 184.

Scopia® Management LDAP Information Attributes

The table below presents a list of standard schema attributes and their naming convention used by Scopia® Management to synchronize with the LDAP server.

Table 41: Scopia® Management LDAP Information Attributes

Scopia® Management Name	LDAP Attribute name (Active Directory)	LDAP Attribute name (Domino Directory)
User Login Identifier	userPrincipalName	cn
	sAMAccountName	uid

Scopia® Management Name	LDAP Attribute name (Active Directory)	LDAP Attribute name (Domino Directory)
email	email	email
telephone	telephoneNumber	telephoneNumber
mobile	mobile	mobile
givenName	givenName	givenName
sn	sn	sn
sipUri	msRTCSIP-PrimaryUserAddress	N/A
sipUriEnabled	msRTCSIP-UserEnabled	N/A
Organizational Unit	ou	ou
Role	memberOf	member

Downloading Users from the LDAP Server

About this task

This procedure describes how to download users from the LDAP server. Users are then displayed in the **User** tab and you can modify settings, such as the user profile of a group, and synchronize the database with Scopia® Management. See [Synchronizing Users from the LDAP Server](#) on page 177 for details.

Before you begin

- Make sure your Scopia® Management is connected to the LDAP server as described in [Connecting Scopia® Management with the LDAP Server](#) on page 172.
- You can assign a Scopia® Management user profile to users and user groups defined in the LDAP server. This way, when users are downloaded from the LDAP server to Scopia® Management, roles and permissions are automatically assigned. If user profiles are not defined, a default user profile is assigned to all users. For more information about user profiles, see [Managing User Profiles](#) on page 161.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Settings > Servers > LDAP Servers**.
3. Select the LDAP server from which you want to download users.

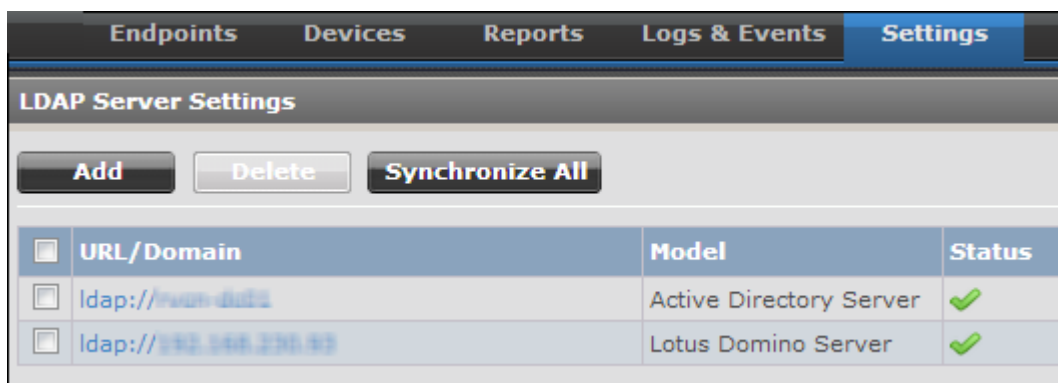


Figure 107: LDAP Server Settings page

- Click **Select** next to each user profile to assign LDAP user groups to a specific Scopia® Management user profile.

Profile Name	Selected Groups	
Administrator		Select
Meeting Organizer		Select
Regular User		Select
Meeting Operator		Select

Default User Profile: Meeting Organizer

Public Virtual Rooms: Select

The system will automatically generate virtual public rooms with the following pattern:

Prefix: + telephoneNumber

☐ Download only users with an email address defined in the LDAP server

☒ Virtual Room Number: Prefix: 6 + telephoneNumber

Update Frequency: Every hour

☐ Secure User Credentials

Apply Cancel

Figure 108: Advanced section of LDAP Server Settings page

You can assign multiple LDAP user groups to each Scopia® Management user profile. By default, all users are assigned the Meeting Organizer profile.

- In the **Default User Profile** field, select a user profile you want to assign to all users for whom you did not specify a user profile, or set the **Default User Profile** field to **Don't download** to instruct Scopia® Management not to download users that are not assigned to any Scopia® Management user type.
- If necessary, assign virtual rooms to the users as described in [Downloading Virtual Rooms from the LDAP Server](#) on page 184.
- To download only LDAP users with an email address to Scopia® Management, select **Download only users with an email address defined in the LDAP server**.

8. Define how often users and meeting rooms are synchronized with the LDAP server by selecting a value from the **Update Frequency** list.
9. (Optional) If using Microsoft Active Directory, you can encrypt the user's LDAP credentials with MD5 by selecting **Secure User credentials**.

! Important:

To use this feature, you must also:

- Define the LDAP server using its FQDN (not its IP address), as described in [Connecting Scopia® Management with the LDAP Server](#) on page 172).
- In Microsoft Active Directory, enable the **Store password using reversible encryption** option.

Do not secure user credentials if you secured the connection between the LDAP server and Scopia® Management.

10. Select **Apply**.
-

Synchronizing Users from the LDAP Server

About this task

This procedure describes how to synchronize the users in your LDAP with Scopia® Management. Perform this procedure if you have added users to your LDAP since you first configured the LDAP server in Scopia® Management, or if you made changes to the user attributes, either in the LDAP server, or in Scopia® Management. For example, if you modified the default user profile, perform this procedure to assign a new profile to users that do not have customized profiles.

Before you begin

Verify that your LDAP server is configured and make any changes, such as the default user profile, before synchronizing. See [Downloading Users from the LDAP Server](#) on page 175 for details.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Servers > LDAP Servers**.

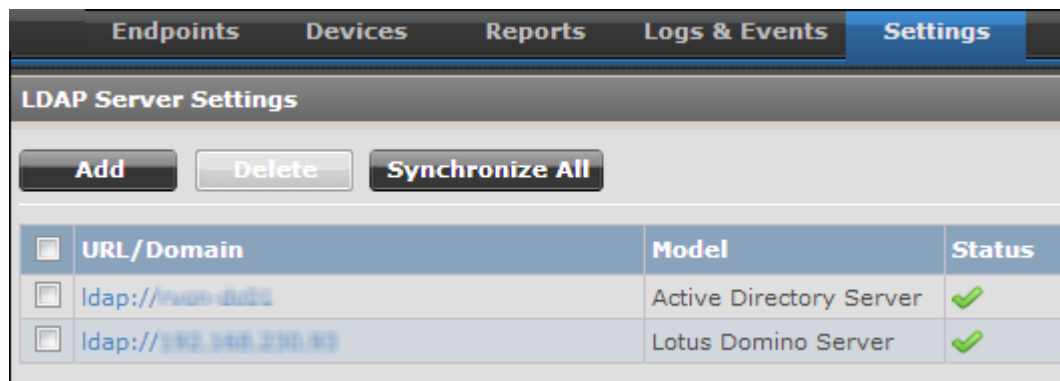


Figure 109: Synchronizing your LDAP database with Scopia® Management

3. Select **Synchronize All**.

The LDAP database is synchronized with Scopia® Management. You can verify that the synchronization completed successfully by checking the result in the **Logs & Events** tab.

Managing Users with a Local User Directory

You can add or modify a user profile if Scopia® Management uses its own database for storing user information.

Navigation

- [Creating a User within Scopia® Management](#) on page 178
- [Removing a User](#) on page 180

Creating a User within Scopia® Management

About this task

You can manually add a user in Scopia® Management when a local database is used for storing users.

During this procedure you must assign a user profile and user groups created earlier as described in [Creating a User Group](#) on page 169 and [Creating or Modifying a User Profile](#) on page 162.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Users** tab.
3. Select **Local Directory > All** from the sidebar.
4. Select **Add** to create a new user.
5. Define settings as described in [Table 42: Defining a new user](#) on page 179.

Table 42: Defining a new user

Field	Description
Login ID	Enter the new user login ID.
First Name	Enter the first name for the new user.
Last Name	Enter the last name for the new user.
Password	Enter the password for accessing Avaya Scopia® Management
Email	Enter the email for the new user. Users who have an email can receive messages and warnings from Scopia® Management.
Telephone (Office) and Telephone (Mobile)	Enter the phone numbers for the new user.
Personal Endpoint	If this user has a personal endpoint, configure it as described below: 1. Select Assign. 2. Select an endpoint. 3. Select OK.
Groups	Assign one or more user groups to the new user: 1. Select Assign. 2. Select one or more user groups. 3. Select Add or Add All. 4. Select OK.
User Profile	Select a user profile depending on what rights and capabilities you want to give to this user: 1. Select a user profile from the list of preconfigured profiles. 2. Select View to check the settings of the profile you selected.
Time Zone	Select the time zone. This setting is used to correctly schedule meetings for this contact.

Field	Description
Location Preference	To use the user's virtual room location for the user's location in a meeting, select Auto , or select another location from the list. Scopia® Management uses this location when selecting the MCU to host meetings.
Account Status	This is relevant for users in the Local Directory only. This is set to Enabled by default. The status changes to Disabled when a user enters an incorrect password more than three times (configurable) and is blocked from the system. Select Enabled to allow the user to access Scopia® Management.

6. If necessary, configure the virtual room for the new user as described in [Creating or Modifying a Virtual Room for a Scopia® Management User](#) on page 187.

7. Select **OK** to save your changes.

The user is saved and Scopia® Management sends the user a notification e-mail containing login access information.

Removing a User

About this task

You can only delete users stored on the local directory server. When Scopia® Management uses an external directory for user provisioning, users must be deleted from the external directory.

You cannot remove a user profile if:

- You are provisioning users via an external directory server—The **Delete** button is hidden.
- The user is the administrator created during installation.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **User** tab.
3. Select **Local Directory > All** or **Group** from the sidebar.
4. Select the check box for the user you want to delete.

Users (2) Pro License(535/1000) Mobile License(0/0)						
Add		Delete		Assign Groups		Search by name
☐	Name	Virtual Room	Email	User Profile	Groups	Endpoint
☐	sysadmin admin			Administrator		
☐	read only			1		

Figure 110: Users tab

5. Select **Delete** and then **OK**.

The user is deleted from the local directory.

Modifying a User

About this task

After a user is created locally within Scopia® Management or downloaded from the external LDAP server, you can modify this user. Note that while for a local user you can modify all settings, for a downloaded user you can only modify these settings:

- Personal endpoint
- Groups
- User profile
- Time zone
- Location preference

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Users** tab.
3. Navigate to the user you want to modify either under **Users from Active Directory** or **Users from Local Directory** on the sidebar.
4. Modify settings as necessary (see [Table 43: Modifying a user](#) on page 181 for details):

Table 43: Modifying a user

Field Name	Description
Login ID	Modify the user login ID.
First Name	Modify the first name for the user.
Last Name	Modify the last name for the user.
Password	Enter the password for accessing Avaya Scopia® Management

Field Name	Description
Email	Enter the email for the user. Users who have an email can receive messages and warnings from Scopia® Management.
Telephone (Office) and Telephone (Mobile)	Modify the phone numbers for the user.
Personal Endpoint	If this user has a personal endpoint, configure it as described below: 1. Select Assign. 2. Select an endpoint. 3. Select OK.
Groups	Assign one or more user groups to the user: 1. Select Assign. 2. Select one or more user groups. 3. Select OK.
User Profile	Assign a user profile depending on what rights and capabilities you want to give to this user: 1. Select a user profile from the list of preconfigured profiles. 2. Select View to check the settings of the profile you selected.
Time Zone	Select the time zone. This setting is used to correctly schedule meetings for this contact.
Location Preference	To use the user's virtual room location for the user's location in a meeting, select Auto , or select another location from the list. Scopia® Management uses this location when selecting the MCU to host meetings.
Account Status	This is relevant for users in the Local Directory only. This is set to Enabled by default. The status changes to Disabled when a user enters an incorrect password more than three times (configurable) and is blocked from the system. Select Enabled to allow the user to access Scopia® Management.

5. To customize the user's capabilities instead of using the capabilities associated with its user profile, see [Customizing a User Profile](#) on page 165.

For example, you can assign or remove the Scopia® User license for this specific user.

6. Select **OK**.

Assigning Groups to Multiple Users

About this task

A user can have more than one group assigned to it. Typically the first group is assigned to a user as you create or download this user. You can assign other groups to the same user at a later stage as described in [Modifying a User](#) on page 181. For more information about user groups in Scopia® Management, see [Managing User Groups](#) on page 168.

This procedure explains how to assign groups to multiple users.

Procedure

1. Access the Scopia® Management administrator portal.
 2. Select the **Users** tab.
 3. Select **All** under **Users from Active Directory** or **Users from Local Directory**.
 4. Select check boxes for users to which you want to assign groups.
 5. Select **Assign Groups**.
The **Select the groups** window opens.
 6. Select check boxes for groups you want to assign and select **OK**.
The groups are assigned.
-

Searching for a User

About this task

You can search the Users list by the user name or the virtual room number assigned to this user.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Users** tab.
3. Select the group in which you want to perform the search.
The default is **All Groups**.
4. Start typing the name or the virtual room number of this user in the **Search** field as shown in [Figure 111: Searching for a user](#) on page 184.

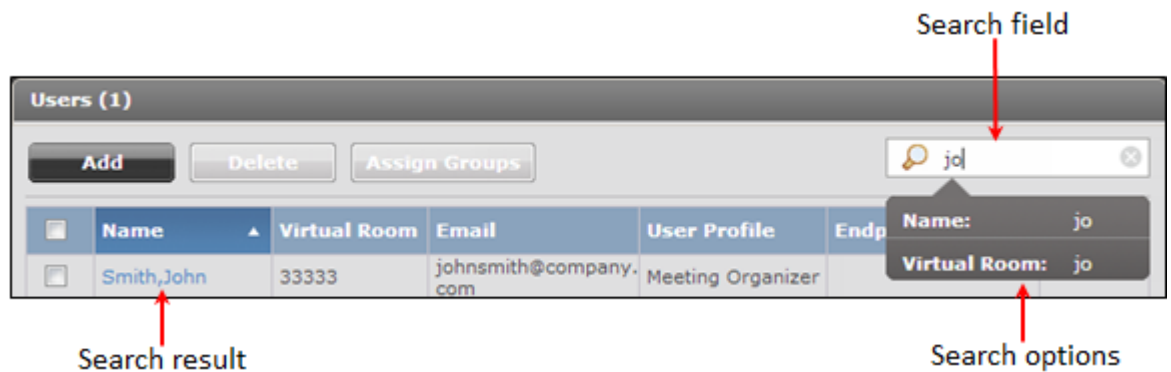


Figure 111: Searching for a user

5. To narrow the search, select **Name** or **Virtual Room** from the **Search options**.
Search results are listed.
6. To return to the complete list of users, clear the **Search** field.

Managing Virtual Rooms

A virtual meeting room is an online space used to connect multiple Scopia® Solution participants in a videoconference. Virtual rooms are hosted by MCUs. In addition to hosting videoconferences, virtual rooms offer features to enhance the videoconferencing experience: it is possible to protect meetings with a PIN number or to put participants who want to join the meeting on hold, in a "waiting room", until the moderator joins the meeting.

! Important:

You can assign virtual rooms only to users for whom you enabled a Scopia® User.

Virtual rooms can be created manually within Scopia® Management, or downloaded from the LDAP server, if your organization uses an LDAP server for user provisioning. If your organization uses an LDAP server, and the virtual rooms are not automatically created for LDAP users downloaded into Scopia® Management, you can manually create virtual rooms for users.

! Important:

Notice that if Scopia® Management is configured to automatically create virtual rooms for users, the configuration settings defined manually are overridden every time that Scopia® Management synchronizes with the LDAP server.

Navigation

- [Downloading Virtual Rooms from the LDAP Server](#) on page 184
- [Creating or Modifying a Virtual Room for a Scopia® Management User](#) on page 187

Downloading Virtual Rooms from the LDAP Server

About this task

Virtual rooms are literally virtual rooms that serve as a meeting place for your video network users. Virtual meeting rooms can be public (available for any user), or personal (assigned to a specific user, who is the only one allowed to schedule meetings in this room).

To download virtual rooms from the LDAP server, the following conditions must be met:

- The value of the LDAP field mapped to the virtual room must be numeric.
- The virtual room number is not editable in the virtual room profile window.
- If the same virtual room number is defined for two users in the LDAP server, the virtual room is created and downloaded to Scopia® Management for only one of the users.

Virtual rooms are available only if an Avaya MCU is deployed.

In deployments using Microsoft Lync, you can add a contact named “My Virtual Room”. This is a personal meeting place where the user can host meetings. When “My Virtual Room” is enabled in the system, it shows its availability in the Contact List (while the user’s personal virtual room indicates an unknown presence).

Before you begin

Check the prefixes used for the auto-attendant and for other components within your network, such as Avaya MCUs, ECS, and Scopia® Gateway. You cannot assign the prefixes already used in the system, because the prefixes assigned to virtual rooms must be unique.

Decide on SIP URIs for the users to whom virtual rooms are assigned (for example, “bfmyvr@lync2010.com”).

For Microsoft Lync and OCS deployments, users can add a contact called **My Virtual Room** to Lync or OCS clients. To enable this setting, verify your Scopia® Management is set for Lync integration. Navigate to **Settings > Unified Communications > Microsoft Lync/OCS**, and select **Enable Microsoft Lync Integration**.

Procedure

1. Access the Scopia® Management portal.
2. Select **Settings > Servers > LDAP Servers**.
3. Select the LDAP server to which organization users were added.
4. Configure personal and public virtual rooms, as described in [Table 44: Configuring settings for downloading virtual meeting rooms](#) on page 186.

Public Virtual Rooms: **Select**

The system will automatically generate virtual public rooms.

Prefix: +

☒ Do not update users without an email address from the LDAP server to SCOPIA

☒ Virtual Room Number: Prefix: +

Update Frequency:

Figure 112: Defining virtual rooms

Table 44: Configuring settings for downloading virtual meeting rooms

Field	Description
Select	Select the LDAP user group to which you assigned the public virtual rooms on the LDAP server. A public virtual room is not associated with any user, and therefore can be assigned to a group of users, like users of the Microsoft Lync client. This is visible only when Microsoft OCS/Lync integration is enabled in Scopia® Management.
Virtual Room Number	This is relevant for both personal and public virtual rooms. Define the virtual room number as follows: 1. Enter a number that you want to use for a prefix. Use any number that is shorter than 11 digits and is not used as a prefix for the auto attendant or for other deployment components. 2. Select the LDAP attribute to use when generating the number of the virtual rooms, according to your dialing plan. Typically, the telephoneNumber attribute is used.

5. Define how often users and meeting rooms are synchronized with the LDAP server by selecting a value from the **Update Frequency** list.
6. Select **Apply**.
7. Select **Synchronize All** on the **LDAP Server Settings** page.
Users from the LDAP server downloaded into Scopia® Management as virtual meeting rooms.
8. Verify that the virtual meeting rooms were downloaded correctly:
 - a. Select **Users > Active Directory > All**.
 - b. Verify that the virtual meeting rooms defined in the LDAP server were downloaded and appear on the Users tab.
9. If necessary, enable additional personal virtual rooms (My Virtual Rooms):
 - a. Select **Settings > Unified Communications > Microsoft Lync/OCS**.

- b. Select **Enable "My Virtual Room" Contact**.



Figure 113: Enabling Microsoft Lync/OCS integration

- c. Enter the SIP URI of My Virtual Room as configured in the Active Directory user, in the **Microsoft Lync Account** field.
- d. Select **Apply**.

Creating or Modifying a Virtual Room for a Scopia® Management User

About this task

After you created or downloaded users into Scopia® Management, you can manually create or assign virtual rooms to them. This procedure is mostly relevant for creating and assigning virtual rooms for local users, as well as assigning additional virtual rooms to users downloaded from the external LDAP server.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Users** tab.
3. Select **Users from Local Directory > All**.
4. Select the link in the **Name** column for the user you require.
5. Enter the user ID and last name in the relevant fields.
6. (Optional) Select the **Virtual Room** tab.

The screenshot shows a 'Virtual Room' configuration window. It has two tabs: 'User' and 'Virtual Room', with 'Virtual Room' being the active tab. The form contains the following elements:

- Virtual Room Number:** A text input field containing '8800123456789'.
- Virtual Room Name:** A text input field containing 'Virtual Room - 123456789'.
- Description:** An empty text input field.
- Meeting Type:** A dropdown menu showing '71 - Default Service'.
- Maximum Participants:** A dropdown menu showing 'Default'.
- Moderator PIN:** A text input field with masked characters (dots).
- Protect meeting with a PIN:** An unchecked checkbox.
- Use permanent PIN:** A selected radio button.
- Use one-time PIN for each meeting:** An unchecked radio button.
- Allow instant meetings:** A checked checkbox.
- Place participants in a 'waiting room' until the moderator joins the meeting:** A checked checkbox.
- Select Endpoints...:** A button at the bottom of the form.

Figure 114: Configuring the user's virtual room settings

7. Configure the virtual room as described in [Table 45: Configuring the virtual room settings](#) on page 188.

Table 45: Configuring the virtual room settings

Field	Description
Virtual Room Number	Enter the number of the virtual room. Users dial this number to start a meeting in this virtual room. You can enter any number that does not start with the prefix of the auto attendant, auto routing, or other deployment components.
Virtual Room Name	Enter the name of this virtual room. This name is displayed during the meeting.
Description	Enter a short description of this virtual room.
Meeting Type	Select the meeting type that can be used by this virtual room.
Maximum Participants	Select the maximum number of participants for an ad-hoc meeting in this virtual room. This setting depends on the number of available ports you want to dedicate to an ad-hoc meeting in this virtual room.
Moderator PIN	Enter the PIN that is used to enable in-meeting control and moderation operations (mandatory).

Field	Description
Protect Meeting with a PIN	If you want to protect meetings using this virtual room with a PIN so that all new participants must enter this PIN to access the meeting. You can define a permanent PIN or to choose the one-time PIN option, when a meeting operator or meeting organizer defines PIN during scheduling. Select this check box and configure the PIN: • Select Use permanent PIN, and enter the number, or • Select Use one-time PIN for each meeting.
Allow instant meetings	Select this check box to allow ad hoc meetings using this virtual room. If not selected, this virtual room can only be used for scheduled meetings.
Place participants in a “waiting room” until moderator joins the meeting	Participants are placed in a waiting room before the moderator joins the videoconference, where they cannot hear or see one another. The meeting begins when the moderator joins (cannot be modified).
Select Endpoints	To automatically invite endpoints to any meeting in this meeting room, assign the endpoints and configure settings as described below: 1. Select the Select Endpoints check box. The Select Endpoints window opens. 2. Select endpoints on the From Directory tab or on the By Address tab. 3. Select Invite Endpoint. 4. Select Save.

8. Select **OK** to save the settings for the virtual room.

Creating an Invitation Template

About this task

Users can invite each other to videoconferences from either the Scopia® Management user portal, or from Microsoft Outlook, using Scopia® Add-in for Microsoft Outlook or Scopia® Plug-in for Microsoft Exchange. You can create the template for the text that is displayed in invitations.

The template text can contain links for participants to easily access the videoconference from different applications and devices. It may also have the link for downloading Scopia® Desktop Client or Scopia® Mobile for guest users.

The screenshot shows an Outlook meeting invitation window. At the top, there are fields for 'To...', 'Subject:', and 'Location:'. Below these are 'Start time:' and 'End time:' fields, both set to 'Wed 05/03/2014' with time slots of '15:30' and '16:00' respectively. An 'All day event' checkbox is also present. The main body of the invitation features a red banner with the text 'AVAYA Scopia Video Collaboration Meeting'. Below this, it says 'Join from Desktop or Mobile' and 'To connect to the conference - from your desktop, tablet or mobile device.' A large red button labeled 'Click to Join' is centered. Below the button, the 'Meeting ID: 665544' and 'Meeting PIN: 1234' are displayed. At the bottom, it says 'Join from a Video Conference System' and 'To join from an endpoint, dial the meeting ID followed by the meeting PIN.'

Figure 115: Example of the template text in the Outlook invitation window

To create a template for the 32-bit version of Scopia® Add-in for Microsoft Outlook, refer to the *Administrator Guide for Scopia® Desktop server*.

Procedure

1. Access the Avaya Scopia® Management administrator portal as described in [Accessing the Administrator Portal to Manage your Video Network](#) on page 33.
2. Select **Settings > Meetings > Invitations**.
The Meeting Invitations window is displayed.

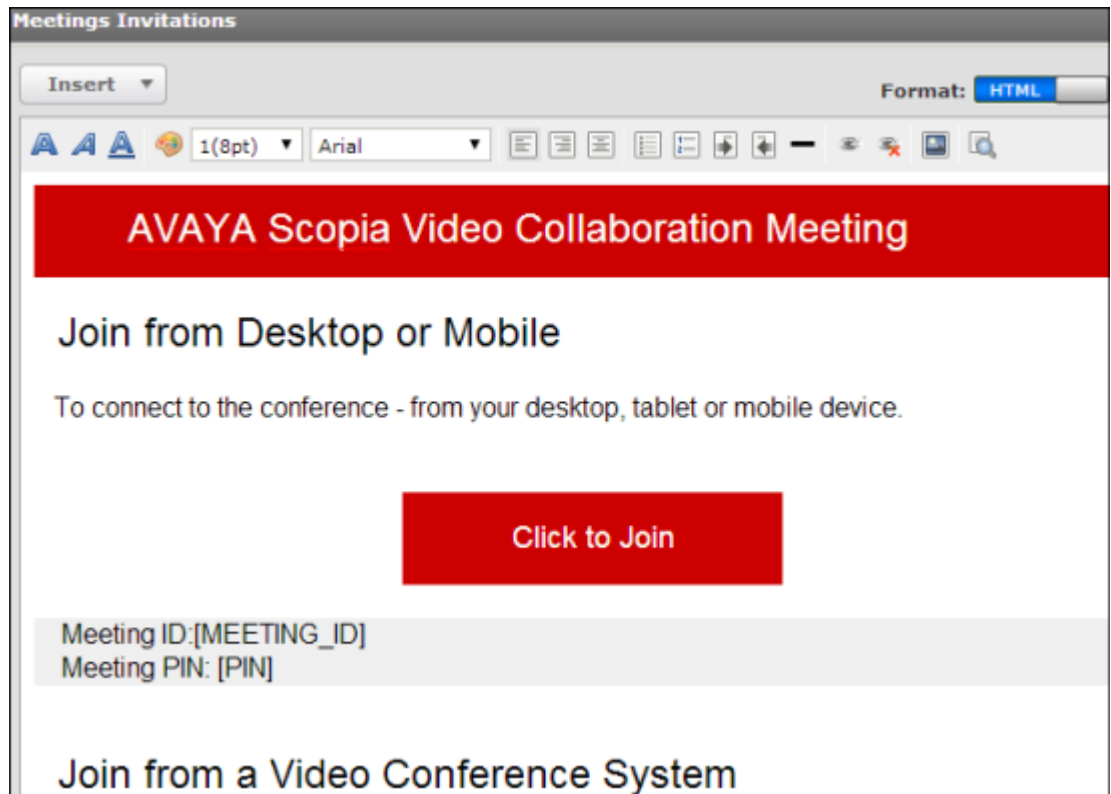


Figure 116: Creating an invitation template

3. (Optional) To use plain text instead of HTML formatting, toggle between the **Format** options. If you use HTML formatting and it is not supported by the user's email client, they see only plain-text formatting.

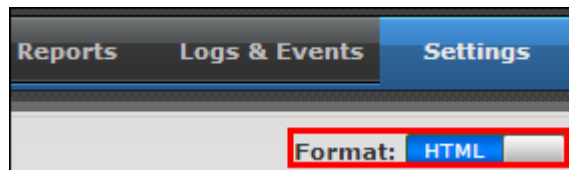


Figure 117: Changing the invitation formatting

4. Use the **Insert** menu to include placeholders for the following links:
 - **Meeting Info:** Meeting ID, PIN and E164 of the videoconference.
 - **Desktop and Mobile Access Links:** Link for participants to install the Scopia® Desktop Client as well as links for accessing the videoconference.
 - **Phone Numbers:** Number for participants who need to dial into the videoconference.
 - **UC Access Links:** Link for participants joining from their unified communications applications: Avaya Aura Conferencing, Lync or OCS applications, for example.
5. To enter a URL for users to join the meeting directly from their computer or mobile device:
 - a. Select **Insert > Desktop and Mobile Access Links** and copy the link address.
 - b. Select the **Click to Join** text.
 - c. Select the **Add Hyperlink** icon:



Figure 118: Adding a URL

- d. Paste the URL and select **OK**.



Figure 119: Entering URL

6. Modify the text of the invitation as necessary.
7. Select **Apply**.
-

Chapter 6 | Scheduling Your Videoconference from the Scopia® Management User Portal

About this task

You can use the Avaya Scopia® Management user portal to schedule meetings and reserve the necessary video network resources for the meeting.

Scheduling a videoconference is similar to creating a regular meeting. You must select the participants, and then set the time, date, and location of your meeting. Often the participants already have their dedicated endpoints associated with their username, so the endpoints are automatically added to the meeting resources. You can also add more resources, like a shared endpoint in a meeting room (room system).

Scopia® Management checks that the required video network resources are available for the scheduled time, including the MCU connections, and then sends the invitation by email to those listed in the **To** field of the invitation.

Important:

Scopia® Management requires Microsoft Exchange in your deployment to send meeting invitations by email.

When you schedule a meeting, Scopia® Management uses the default settings in your user profile and the chosen virtual room, such as the time zone and whether participants need a PIN to join the meeting. You can override the settings for this meeting by defining the meeting properties. To change the default settings in your user profile and virtual room (see *User Guide for Avaya Scopia® Management*). Administrators can also change settings for a user (see [Defining and Managing Video Users](#) on page 160).

As a user, you can only schedule a videoconference if your administrator enabled this functionality in your user profile.

Procedure

1. As a user, access the Scopia® Management user portal and select **Schedule**.

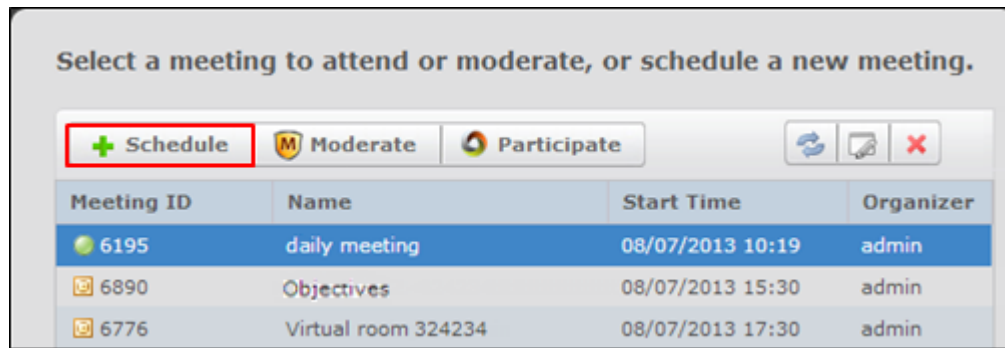


Figure 120: Access meeting scheduling from the Scopia® Management user portal

Or

- As an administrator, access the Scopia® Management administrator portal select **Meetings > Meetings > Schedule a Meeting**.

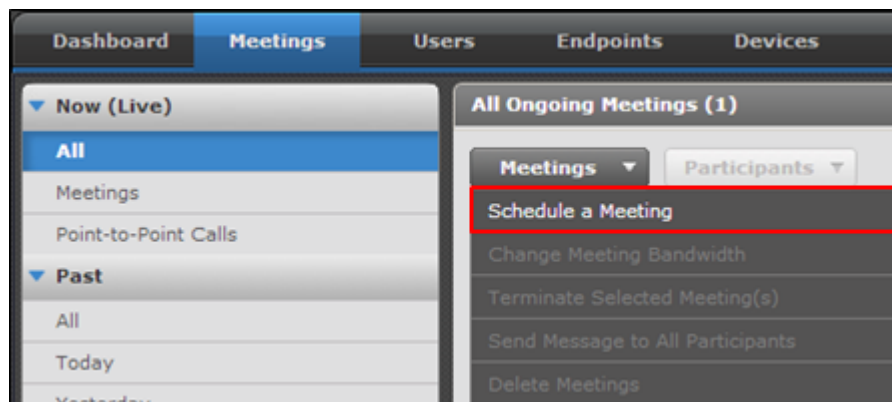


Figure 121: Access meeting scheduling in the Scopia® Management administrator portal

Enter the meeting invitation details.

Schedule a Meeting

Send icon:

To: admin;

Subject: Objectives

Start Time: 04/12/2013 18:16

Duration(minutes): 45

Where: 60001 (60001)

Buttons: Message, Endpoints, Availability, Advanced

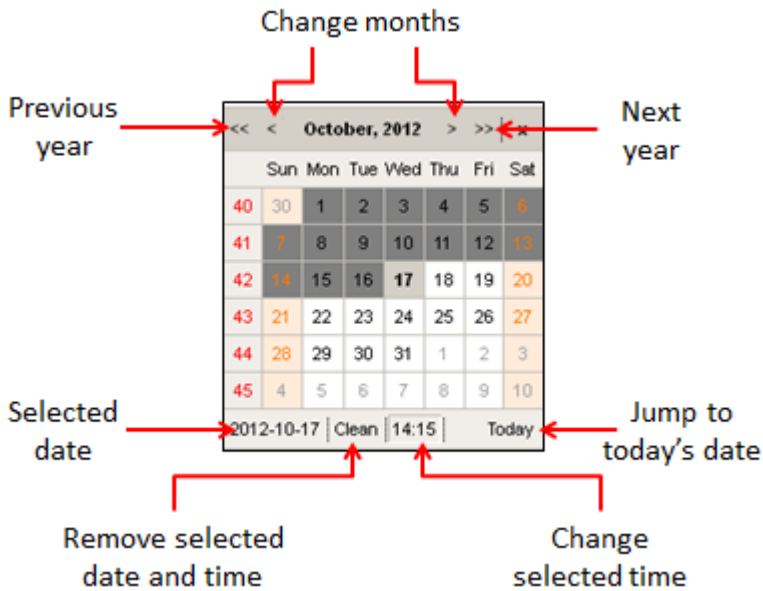
Message body:

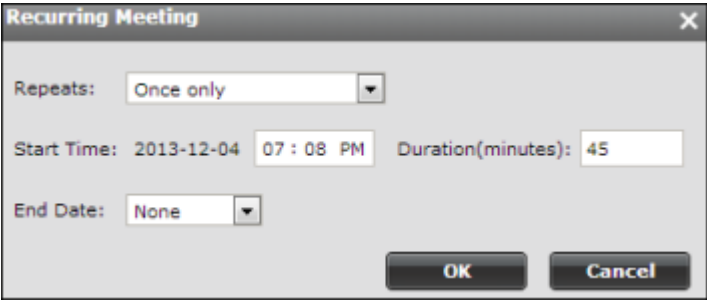
Hi,

Let's meet to discuss objectives.]

Figure 122: The Schedule a Meeting page

- Enter the basic meeting information.

Field	Description
To	Enter the first characters of a participant to choose from the list of users. If this username is associated with a dedicated endpoint, Scopia® Management automatically adds the endpoint to the list of endpoints required for this meeting, listed in the Endpoints tab. + Tip: If you are also one of the participants, add your own name to this list. To designate yourself as the moderator in the Advanced tab, see Configuring Advanced Meeting Properties in the User Portal on page 199).
Subject	Enter the subject of the meeting.
Start Time	Select  to choose the scheduled start time.  • Select << or >> to change the year. • Select < or > to change the month. • Select Today to jump to today's date. • Select Clean to remove the selected date and time. • Select the time at the base of the calendar pane to change the meeting's start time.

Field	Description
Recurring 	Enter information for meetings which take place at regular intervals.  Select Repeats to change the frequency of the recurrence of the meeting: • Once only indicates the meeting does not repeat. • Every <day of week> indicates it repeats once a week. • Day <n> of every month indicates it repeats once a month. • Every day indicates it repeats every day. Enter the meeting's start time in Start Time. You can also enter this value in the calendar window. Enter the meeting duration in Duration. You can also enter it in the main invitation window. By default, Scopia® Management does not end the meeting if participants are still connected and there is no resource conflict with other scheduled meetings. Enter the last date of the meeting's repetition in End Date: • None indicates the meeting repeats indefinitely. • By requires you to enter the last date of the meeting recurrence. • After requires you to enter the number of recurring meetings to schedule.
Duration	Enter the meeting length in minutes. By default, Scopia® Management does not end the meeting if participants are still connected and there is no resource conflict with other scheduled meetings. To end the meeting at the specified time, even if participants are still connected, see Configuring Advanced Meeting Properties in the User Portal on page 199.

Field	Description
Where	If you have more than one participant, select the assigned virtual room as the location of the meeting. Alternatively, for a direct meeting with just one other person, where both participants have a dedicated video endpoint like the XT Series, choose Point to Point Meeting, where the video is not routed via an MCU. ! Important: Both endpoints in this kind of point-to-point meeting must be dedicated video endpoints. If one of the endpoints is a software endpoint, like Scopia® Desktop Client, select the virtual room option. You must also assign two endpoints as part of this meeting in the Endpoints tab (in this procedure).
Message	The system automatically inserts text into the body of the invitation, containing instructions on how to connect to the videoconference. This text is configured by the administrator You can add to this text by entering additional information in this field, such as the list of items on the agenda.

- To reserve a dedicated video endpoint for the meeting, select the **Endpoints** tab above the message body of the invitation.

XT Series endpoints include calendar functionality which alert users when a meeting is about to start.

The figure consists of two side-by-side screenshots of the Scopia Management interface. Both screenshots show the 'Endpoints' tab selected. The left screenshot displays the 'Select endpoint(s) to invite:' form with the following fields: 'Name' (text input), 'Protocol' (dropdown menu showing 'IP (H.323)'), 'Restricted Mode' (checkbox), '3G' (checkbox), 'Address' (text input), and 'Bandwidth' (dropdown menu showing 'Default'). The right screenshot shows a dropdown list of endpoints: Jack Brown, Jake Black, Jill White, and John Grey.

Figure 123: Reserving endpoints for the meeting

Enter the following fields. To associate an endpoint with a user, or for other advanced endpoint options, see [Configuring Advanced Meeting Properties in the User Portal](#) on page 199.

Field	Description
By Directory	Select the endpoint listed in the address book, or use the search field to narrow the list.
By Address	Select this tab to manually enter the endpoint's details if it is not listed in the endpoint directory.
Protocol	Select the videoconferencing standard used to communicate with this endpoint: • Select IP (H.323) if you invite an H.323 endpoint. • Select IP (SIP) if you invite an SIP endpoint. • Select ISDN/PSTN (H.320) if you invite an ISDN/PSTN device, using the H.320 standard for devices outside the organization. • Select Mobile if you invite a 3G device.
Restricted Mode	Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.
Address	Enter the endpoint's address. • If you invite an H.323 or SIP endpoint, enter the E.164 number, IP address or domain name you received for the endpoint. • If the invited endpoint is a mobile device (not Scopia® Mobile) or an ISDN/PSTN device, enter the country code, area code, and phone number for this device.
Bandwidth	Select the bandwidth used to communicate with this device, measured in kbps. Kilobits per second (kbps) is the standard unit to measure bitrate, measuring the throughput of data communication between two devices. Since this counts the number of individual bits (ones or zeros), you must divide by eight to calculate the number of kilobytes per second (KBps). • Default supports all layouts and endpoints with various resolutions. • <bandwidth_values> determines the maximum bandwidth for this endpoint to connect to the meeting.

5. Select the **Availability** tab to check if the endpoints are available and if there are enough MCU resources (displayed in the **Virtual MCU** row) for this meeting.

The system displays the week in which the meeting is scheduled to occur ([Figure 124: Verifying participant availability \(example\)](#) on page 199) and indicates availability using these colors:

- No color indicates the endpoint is available and there are enough MCU resources for this time.
- Blue indicates the endpoint is already booked for another meeting or there are not enough MCU resources for this time.
- In the **Virtual MCU** row only, gray indicates the system does not know the MCU's availability. By default, the system displays availability for the four hours before and after the scheduled time. Time slots outside this period are colored gray.

Message	Endpoints	Availability				Advanced
Busy Unknown		PM	6PM	7PM	8PM	
Endpoints						
XT5000						← Endpoint is available
Virtual MCU		↑ Availability is unknown				↑ Not enough MCU resources

Figure 124: Verifying participant availability (example)

6. (Optional) Select the **Advanced** tab to configure advanced meeting properties (see [Configuring Advanced Meeting Properties in the User Portal](#) on page 199).
7. If you have completed the scheduling procedure, select **Send**.
 If all required resources are available, Scopia® Management schedules the meeting, reserves the resources and sends invitations to the participants. If non-essential resources (such as optional endpoints or users) are not available, Scopia® Management continues to schedule the meeting but notifies you of the conflicts.
 If essential resources are not available, Scopia® Management would not schedule the meeting, but instead notifies you of the clash.
8. To change a scheduled meeting, select **Properties** .
 To delete a scheduled meeting, select **Delete** .

Configuring Advanced Meeting Properties in the User Portal

About this task

As part of scheduling meetings in the user portal to reserve video network resources, you can configure advanced properties to override the default settings of the virtual room, meeting type or user profile.

Before you begin

Define the core meeting parameters including the list of participants, the date and time, and also the virtual location of the meeting (see [Scheduling Your Videoconference from the Scopia® Management User Portal](#) on page 193).

Procedure

1. As a user, access the Scopia® Management user portal and select **Schedule**.

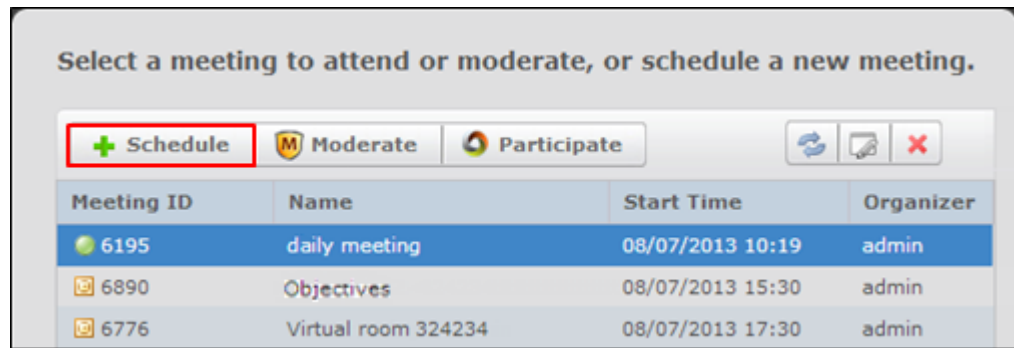


Figure 125: Access meeting scheduling from the Scopia® Management user portal

Or

- As an administrator, access the Scopia® Management administrator portal select **Meetings** > **Meetings** > **Schedule a Meeting**.

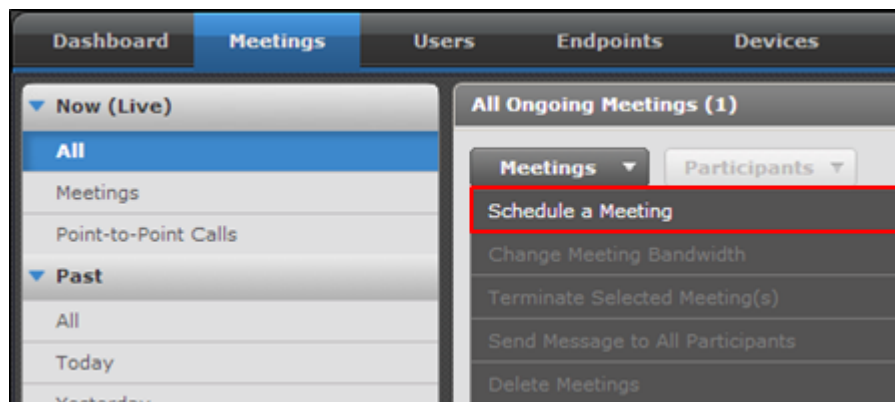


Figure 126: Access meeting scheduling in the Scopia® Management administrator portal

Enter the meeting invitation details.

Schedule a Meeting

Send icon (envelope with green arrow)

To: admin;

Subject: Objectives

Start Time: 04/12/2013 18:16 (calendar icon) Duration(minutes): 45 Where: 60001 (60001) (dropdown)

Buttons: Message, Endpoints, Availability, **Advanced**

Message body: Hi,
Let's meet to discuss objectives.]

Figure 127: The Schedule a Meeting page

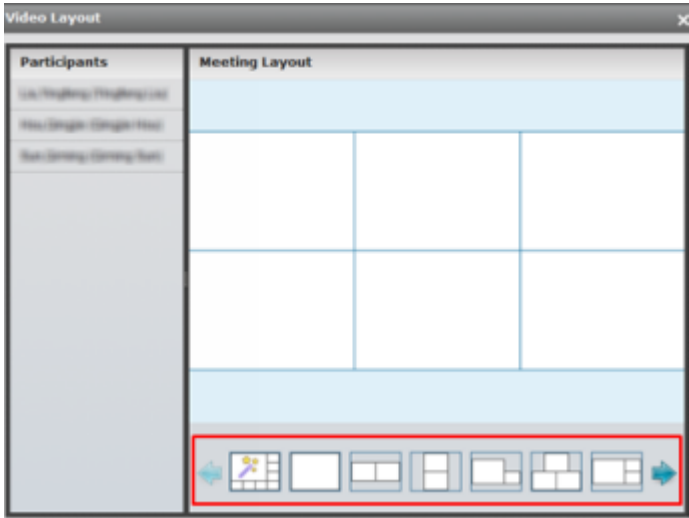
- Select the **Advanced** tab.

Figure 128: Defining advanced meeting properties

Configure advanced meeting properties as described in [Table 46: Advanced meeting properties](#) on page 201.

Table 46: Advanced meeting properties

Field	Description
Meeting PIN	Enter a numeric-only PIN to require participants to enter this meeting a password.
Meeting Host	Choose the moderator of the meeting from the list of participants. A moderator has special rights in a videoconference, including blocking the sound and video of other participants, inviting new participants, disconnecting others, determining video layouts, and closing meetings. From Scopia® Management, moderators can do this by accessing the In-Meeting Control interface. If configured, participants may be required to stay in the waiting room until the meeting's host joins.
Reference Code	Enter a billing code or other internal audit code if required.
Moderator PIN	Enter a numeric PIN in the Moderator PIN field. A moderator PIN also allows you to place participants in a waiting room until the meeting host arrives. A moderator has special rights in a videoconference, including blocking the sound and video of other participants, inviting new participants, disconnecting others, determining video layouts, and closing meetings. A participant who enters the moderator PIN can also unlock the waiting room when joining the meeting.
Place participants in a 'waiting room' until the moderator joins the meeting	Participants are placed in a waiting room before the moderator joins the videoconference, where they cannot hear or see one another. The meeting begins when the moderator joins (cannot be modified).

Field	Description
Terminate at scheduled time and alert in advance (minutes)	Select to end the meeting at the scheduled end time, for example, if the same resources must be freed for another meeting. Enter the number of minutes warning required to notify participants that the meeting will shortly end.
Terminate after all participants left the meeting (minutes)	Select to keep the meeting open until all participants have left, and only then automatically close the meeting. Enter the number of minutes to wait before closing the meeting. If your administrator defined a maximum time for meetings, you cannot automatically extend Scopia® Management meetings beyond this time.
Video Layout	Select from the lower bar at the bottom of this pane to determine the initial video layout for endpoints to which the MCU dials out. A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. If the meeting includes a presentation, a layout can also refer to the arrangement of the presentation image together with the meeting participants.  The screenshot shows a window titled 'Video Layout'. It has two main sections: 'Participants' on the left and 'Meeting Layout' on the right. The 'Participants' section lists three participants: 'Lia Thigley (Thigley Ltd)', 'New Single (Single Host)', and 'New Single (Single Host)'. The 'Meeting Layout' section shows a 3x2 grid of empty slots. At the bottom of the window is a toolbar with several icons for different video layouts, including a dynamic layout icon (a grid with a star) and a presentation icon (a screen with an arrow). The dynamic layout icon is highlighted with a red box. The default dynamic video layout  automatically adjusts based on the number of participants in the meeting. To predetermine a fixed layout, choose one of the layouts in the lower bar. Verify the meeting type (service) on the MCU is not dynamic. Dynamic layout conserves bandwidth, eliminates the display of empty frames in the video image, and makes optimal use of the video image display. Dynamic layout is especially suited to a meeting that has a high rate of participant traffic joining and exiting the meeting, or to an adaptive meeting type that has a variety of meeting sizes. To fix one endpoint's image in a specific subframe of the screen layout, drag and drop the participant name into the meeting layout.

Field	Description
Reserved Ports	Select to reserve more connections on the MCU for this call, for example, if you know some participants may join on Scopia® Desktop Client, or if you might add more participants during the meeting. If a participant leaves a meeting before the end time is reached, Scopia® Management releases the video ports used by the participant immediately. Enter the number of connections at the following video resolutions: • Full High Definition reserves connections at up to full HD 1080p. • High Definition reserves connections at up to 720p. • Standard Definition reserves connections at up to 352p.
Location Preference	In a distributed MCU deployment, select the preferred location of the MCU which would host this meeting. Choosing a specific MCU location limits the availability of MCU connections to just this device. If you select Auto, Scopia® Management knows the endpoints' location and can thus automatically select the MCU closest to the endpoints. For example, if only one endpoint in the meeting is in Europe while the remainder are in the Far East, Scopia® Management selects an MCU located in the Far East. We strongly recommend selecting Auto to let the system choose the optimal settings matching your organization's bandwidth policies. This ensures efficient bandwidth use and maximum quality for the videoconference.
Time Zone	Select a time zone for your meeting if it extends beyond one time zone. The start time of the meeting is expressed in the time zone selected here.
Endpoint	Select a dedicated video endpoint for each participant. The XT Series includes calendar functionality which warns users when a scheduled meeting is about to start. It also offers a very simple way to join a scheduled meeting by selecting Join on the reserved endpoint.

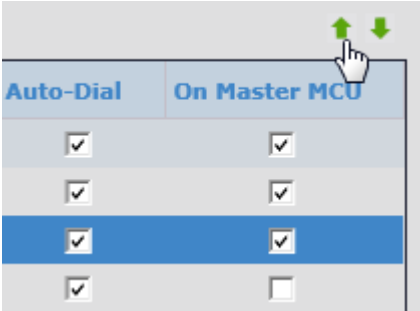
Field	Description										
Auto-Dial	Select to instruct the MCU to automatically dial this endpoint at the start of the meeting. Depending on the settings of the endpoint, it would either ring or join automatically.										
On Master MCU	Select to determine that this endpoint connects only to the master MCU for a higher quality experience in cascaded meetings. If Scopia® Management cascades this meeting across multiple MCUs to reduce bandwidth costs, the meeting would be hosted by a master MCU with one or more slave MCUs. Endpoints connected to a master MCU have their video viewed by all participants, while from the slave MCU, only the active speaker is displayed. You can allocate a higher priority to an endpoint to increase its likelihood of connecting to the master MCU using the green arrows above the endpoint list. The arrows appear after you select an endpoint to connect to the master MCU. <table><thead><tr><th>Auto-Dial</th><th>On Master MCU</th></tr></thead><tbody><tr><td>☒</td><td>☒</td></tr><tr><td>☒</td><td>☒</td></tr><tr><td>☒</td><td>☒</td></tr><tr><td>☒</td><td>☐</td></tr></tbody></table>	Auto-Dial	On Master MCU	☒	☒	☒	☒	☒	☒	☒	☐
Auto-Dial	On Master MCU										
☒	☒										
☒	☒										
☒	☒										
☒	☐										

Figure 129: Prioritizing endpoints' connections to the master MCU

Chapter 7 | Real-time Monitoring

Scopia® Management keeps network administrators informed about events related to video devices that are part of the Scopia® Solution deployment.

All video devices that are managed by Scopia® Management communicate by sending SNMP traps or XML messages to it. Scopia® Management analyzes received information and generates its own messages that allow you to monitor and troubleshoot your videoconferencing deployment:

- Alarms require immediate attention, notify about the video device's abnormal behavior. These could be hardware, software, or environmental problems that affect system operation and require the administrator's intervention. Scopia® Management clears an alarm automatically when the problem causing it is solved and the alarm is no longer relevant.
- Events reflect past alarms and information about general change in a video device's behavior or status. No immediate action is necessary.

For example, if a video device is reported offline, Scopia® Management generates an alarm. After you troubleshoot this video device, the alarm is cleared and an event is generated notifying you that the device is online. The event history shows two events: one recording the alarm and one recording its clearance.



Figure 130: The flow of generating alarms and events in Scopia® Management

Both alarms and events are grouped according to their level of severity which you can customize to better serve the needs of your deployment as described in [Changing the Severity Level of Alarms](#) on page 213.

Alongside the events and alarms, Scopia® Management displays some of the SNMP trap messages from video devices in their original format.

❗ Important:

You can forward SNMP trap messages to a central SNMP trap server as described in [Forwarding Traps to a Third-party Trap Server](#) on page 207.

In addition to displaying messages for real-time monitoring, Scopia® Management provides the following tools for notifying administrators your deployment about alarms and events:

- Generating log files
- Sending email alerts

Navigation

- [Managing Alarm Notifications](#) on page 205
- [Monitoring Network Devices via Scopia® Management](#) on page 210
- [Monitoring Meetings and Calls](#) on page 213

Managing Alarm Notifications

These topics explain how to configure the tools Scopia® Management provides to notify the network administrator of alarms and events that require troubleshooting.

Navigation

- [Configuring the Log Level](#) on page 206
- [Sending Trap Messages](#) on page 206
- [Sending Email Alerts](#) on page 208

Configuring the Log Level

About this task

Scopia® Management is configured to automatically create logs to help maintain your deployment and troubleshoot problems.

You can select three levels of details for a log file. Storing more details will obviously increase the size of the log file.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Settings** tab.
3. Select **Log Level** in the sidebar menu.
4. Select the required level of details for the log files:

Table 47: Log levels

Field Name	Description
Warn	Provides indications on unexpected issues. Service is still provided.
Info	Includes general information.
Debug	Provides detailed information required for troubleshooting.

5. Select **Apply**.

Sending Trap Messages

You can configure Scopia® Management to forward all traps received from managed video devices to another trap server. These include Scopia® Management self-generated traps, such as the one resulting from MCU port usage exceeding the configured threshold.

Navigation

- [Forwarding Traps to a Third-party Trap Server](#) on page 207
- [Removing Trap Forwarding to a Third-party Trap Server](#) on page 207

Forwarding Traps to a Third-party Trap Server

About this task

You can forward traps received by Scopia® Management to one or more third party trap servers.

You first must configure the trap server in Scopia® Management by providing the trap server's IP address and SNMP port (usually, port 162).

You then need to set the alarm threshold of an event that, when reached, causes Scopia® Management to send a trap to the configured trap server(s).

For more information on alarms, events, and traps, see [Real-time Monitoring](#) on page 205.

Procedure

1. Log in to the Scopia® Management administrator portal.
2. Select the **Settings** tab.
3. Select **Alarm > Trap Servers** in the sidebar menu.
4. Do one of the following:
 - To add a trap server, select **Add**.
 - To modify the settings of an existing trap server, select the IP address of the relevant trap server.
5. Specify the IP address and port number of the trap server to which Scopia® Management forwards traps received from managed elements.
6. Select **OK** to save your settings.
7. Enter the threshold value in percent for port usage in these devices:
 - MCU
 - Gateways such as Scopia® Video Gateway and Avaya Scopia® TIP Gateway
 - Scopia® Desktop

Removing Trap Forwarding to a Third-party Trap Server

About this task

You can remove a trap server that is no longer used. Deleted trap servers are removed from the database.

For more information on alarms, events, and traps, see [Real-time Monitoring](#) on page 205.

Procedure

1. Log in to the Scopia® Management administrator portal.
2. Select the **Settings** tab.
3. Select **Alarm > Trap Servers** in the sidebar menu.
4. Select the specific trap server.
5. Select **Delete**.
6. Select **Yes** at the prompt.

The trap server is removed from the database.

Sending Email Alerts

You can configure Scopia® Management to send emails to specific users, with notifications of alarms registered by the system. You can also define the minimum severity level. For example, you can define that notifications are sent only for critical alarms.

Navigation

- [Creating or Modifying an Alert Recipient Profile](#) on page 208
- [Removing an Alert Recipient Profile](#) on page 209

Creating or Modifying an Alert Recipient Profile

About this task

You can define a recipient for email notifications sent by Scopia® Management regarding traps.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Settings** tab.
3. Select **Alarm > Alert Recipients** in the sidebar menu.
4. Do one of the following:
 - To create a new alert recipient profile, select **Add**.
 - To modify an existing alert recipient profile, select the relevant **Recipient Name**.
5. Configure the alert recipient profile as follows:

Field Name	Description
Recipient Name	Enter the name of the alert recipient.
Email Address	Enter the email address of the alert recipient.
Minimum Severity	Select the minimum severity level of alerts to be sent to the alert recipient. The corresponding Alarm Threshold field in the Alert Recipients list indicates the selected severity level.
Notify on alarms clearing	When selected, enables to alert the email recipient that alarms have been cleared. The corresponding Cleared field in the Alert Recipients list is set to yes .
Use custom subject line	To include a custom subject line in the email, select this field and enter a string for the custom subject line in the relevant field.
Include element info	When selected, adds details of the elements reported in the alerts in the custom subject line.
Custom subject line	To include a custom subject line in the email, first select Use custom subject line and then enter a string for the custom subject line in the relevant field.

6. Select **OK** to save your settings.

Removing an Alert Recipient Profile

About this task

You can remove a recipient defined to receive notifications about traps.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Settings** tab.
3. Select **Alarm > Alert Recipients** in the sidebar menu.
4. Select the check box next to the alert recipient you want to delete.
5. Select **Delete**.

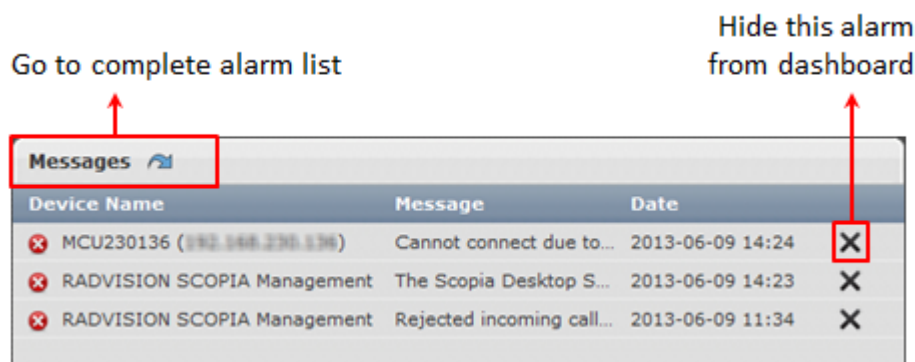
The alert recipient profile is removed from the database.

Monitoring Network Devices via Scopia® Management

You can use the Scopia® Management to monitor the functionality of devices, alarms and events, within your network, and to monitor bandwidth usage and port availability for the videoconferencing network resources. You can monitor your video network devices, including endpoints, in the following ways:

- Recent critical alarms regarding devices

The most recent and critical events and alarms are displayed on the **Dashboard** tab, which appears when you first access Scopia® Management.



Messages			
Device Name	Message	Date	
✖ MCU230136 (92.148.230.136)	Cannot connect due to...	2013-06-09 14:24	✖
✖ RADVISION SCOPIA Management	The Scopia Desktop S...	2013-06-09 14:23	✖
✖ RADVISION SCOPIA Management	Rejected incoming call...	2013-06-09 11:34	✖

Figure 131: Messages area of the Dashboard tab

- All alarms and events for the system

You can view all events and alarms in the system from the **Logs & Events** tab.

- Alarms and events per device

You can monitor the status of video network devices from the **Devices** and **Endpoints** tabs. The device status is indicated by an icon, as described below:

- Online 

The device is online and operating normally. You can use this device to schedule meetings.

- Online with an alarm 

The device is online, but a critical error occurred, such as device failure. Navigate to the list of alarms for more information about the alarm and what to do.

- In a call  (for endpoints only)

The device is in a call.

- In Maintenance 

The device is not online, typically while being upgraded. You cannot use this device to schedule meetings.

- Offline 

The device is offline. You cannot use this device to schedule meetings.

A list of alarms and events is displayed in the device's profile.

Navigation

- [About Management Status of Network Devices](#) on page 211

- [Monitoring Network Events and Alarms](#) on page 211
- [Changing the Severity Level of Alarms](#) on page 213

About Management Status of Network Devices

Video network devices managed by Scopia® Management can send alarms and events to Scopia® Management for monitoring purposes. You can view events, alarms, and network status information for your video network devices in the **Endpoints** and **Devices** tabs. The following video network devices are managed by Scopia® Management:

- Avaya gatekeepers
- Avaya MCUs
- Avaya gateways
- Avaya Scopia® PathFinder server
- Endpoints

You can manually configure Scopia® Management to manage Avaya Scopia® XT Series, Scopia® VC240, and endpoints from Polycom, Tandberg, and LifeSize. For more information about managing endpoints, see [Managing Endpoints using Scopia® Management](#) on page 113.

All network status information is updated in real time by the Avaya Scopia® Management database.

There are two types of network devices management status:

- **Managed**

The device exists in the Avaya Scopia® Management database and provides monitoring information and access to configuration settings.

- **Not managed**

The device exists in the Avaya Scopia® Management database but has no open communication channels with Avaya Scopia® Management and provides no monitoring information or access to configuration settings.

Monitoring Network Events and Alarms

About this task

You can monitor events and alarms reported by the system for the entire network and for specific network devices. You can sort the list of events or alarms according to severity, time, message and device, and filter traps by severity and time interval. See [Real-time Monitoring](#) on page 205 for an explanation of alarms and events.

This procedure describes how to view all network events and alarms, or monitor a specific device, including endpoints.

Procedure

1. Access the Scopia® Management administrator portal.
2. You can monitor alarms or events for a specific device, or on a network level, as follows:

- To monitor a specific device, select the video network device from the **Devices** or **Endpoints** tab, and then select the **Events** or **Alarms** tab to view messages about the device.
- To view the most recent and critical alarms in the network by navigating to the **Messages** area of the **Dashboard** tab ([Figure 132: Messages area](#) on page 212).

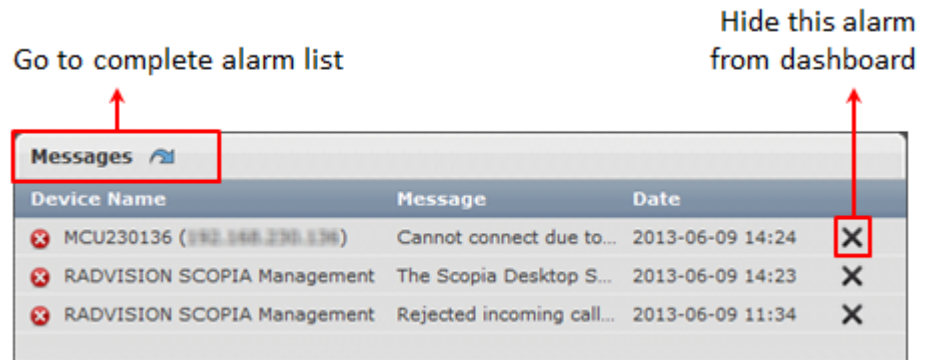


Figure 132: Messages area

- To hide a message from the **Message** area of the Dashboard, select ☒. This message still appears on the **Logs & Events** tab.
- To view detailed information about all network events, select **Messages** (see [Figure 132: Messages area](#) on page 212) or **Logs & Events** tab, which displays the following information:
 - **Severity**
Event or alarm severity level (Cleared, Information, Warning, Critical).
 - **Device Name**
The name of the device that coursed the event.
 - **Time**
Date and time the event or alarm was generated.
 - **Message**
Event or alarm description.

! Important:

Select the column headings in the table to sort the information displayed.

Endpoints	Devices	Reports	Logs & Events	Settings
Alarm List				
Severity	Device Name	Time	Message	
X	EliteMCU230137 (192.168.230.137)	2012-10-16 17:43	Fan failure	
X	EliteMCU23083 (192.168.230.83)	2012-10-16 17:47	Fan failure	

Figure 133: Viewing detailed information about alarms and events

Changing the Severity Level of Alarms

About this task

You can modify the severity level of alarms generated by the system, and create events for a specific alarm.

! Important:

You can disable all Scopia® Management alarms before performing some maintenance procedures, like upgrading endpoints, not to generate hundreds of irrelevant alarms. You can mute Scopia® Management's alarms by selecting **Settings > Alarm > Alarms > Disable All Alarms** in the Scopia® Management administrator portal.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Alarm > Alarms**.
3. Select the alarm whose severity you want to change from the list.

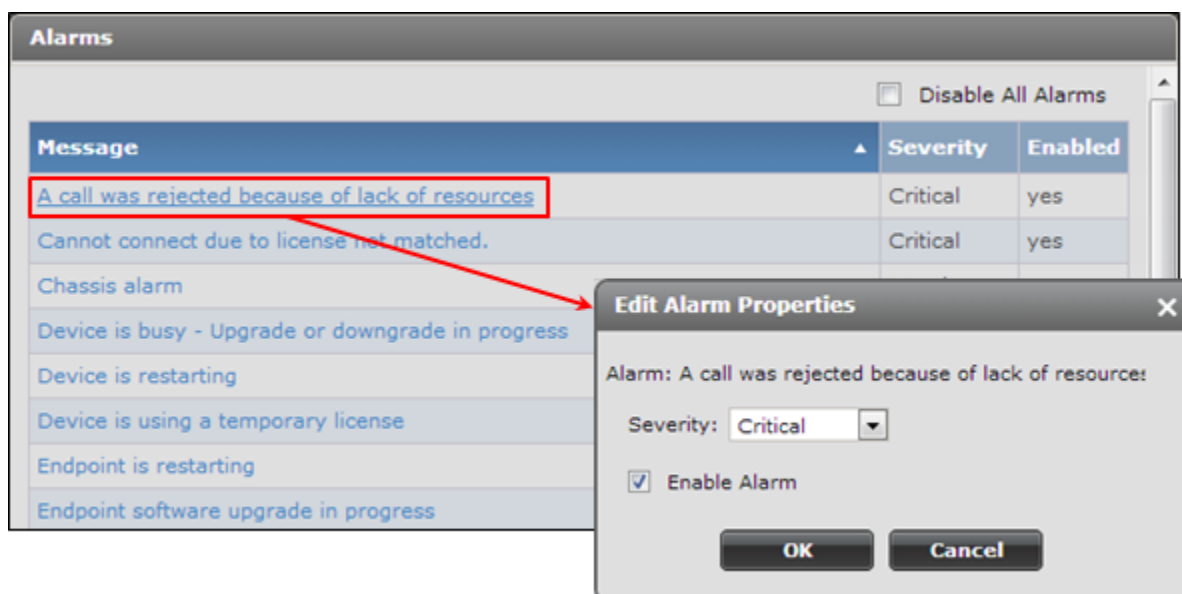


Figure 134: Changing the severity level of an alarm

4. Select the severity level from the **Severity** list.
5. If necessary, you can disable the alarm all together by clearing the **Enable Alarm** check box.
6. Select **OK** to save your changes.

Monitoring Meetings and Calls

You can monitor ongoing meetings and upcoming meetings scheduled in your videoconferencing network. In addition, you can monitor system utilization status.

You can view general information regarding view the overall bandwidth and device usage, and bandwidth for all current and past meetings. For a detailed graphical presentation of meeting and call data, generate a report based on various criteria, as described in [Generating a Report](#) on page 266.

Navigation

- [Monitoring Ongoing Meetings or Calls](#) on page 214
- [Monitoring Bandwidth and Port Utilization](#) on page 216
- [Checking the Status of Meetings](#) on page 217
- [Disconnecting Calls or Meetings](#) on page 217
- [Downgrading the Meeting Bandwidth](#) on page 218

Monitoring Ongoing Meetings or Calls

About this task

You can view and monitor all meetings and calls scheduled in the system by:

- Monitoring bandwidth and port utilization to make sure values do not exceed the limits set for the videoconference
- Becoming a moderator. For more details about moderators, refer to *User Guide for Avaya Scopia® Management*.
- Terminating meetings
- Viewing detailed information regarding meetings and calls as a report, as described in [Generating a Report](#) on page 266.
- Viewing meeting details, such as the meeting ID or hosting MCU, by clicking the meeting link.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Meetings** tab.

Or

Select the link in the **Calls and meetings in progress** section as shown in [Figure 135: Displaying meetings in progress from the Dashboard tab](#) on page 215.

View meetings in progress

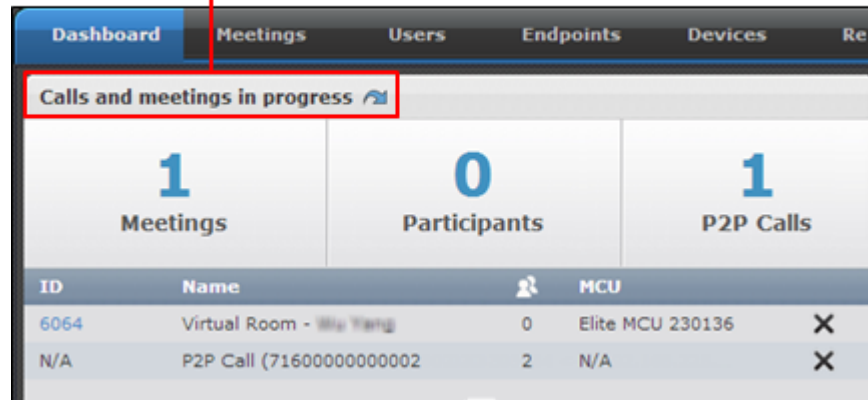


Figure 135: Displaying meetings in progress from the Dashboard tab

The **Meetings** tab opens showing all ongoing meetings. See [Figure 136: Ongoing meetings displayed on the Meetings tab](#) on page 215.

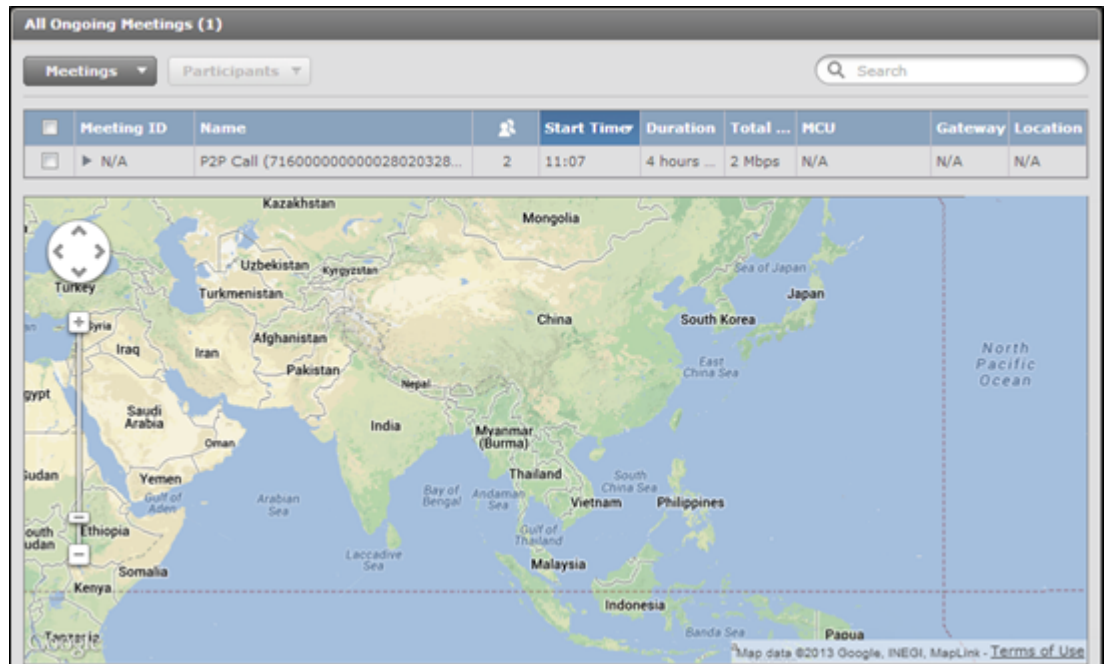


Figure 136: Ongoing meetings displayed on the Meetings tab

3. Select the meeting or call you want to monitor it from the In-meeting Control page.

Use the **Search** field to quickly search by the meeting ID, meeting name, endpoint number or endpoint name.

Use the Advanced Search feature to search by the meeting type or time when the meeting started or ended. See [Figure 137: Using the Search feature on the Meetings tab](#) on page 216

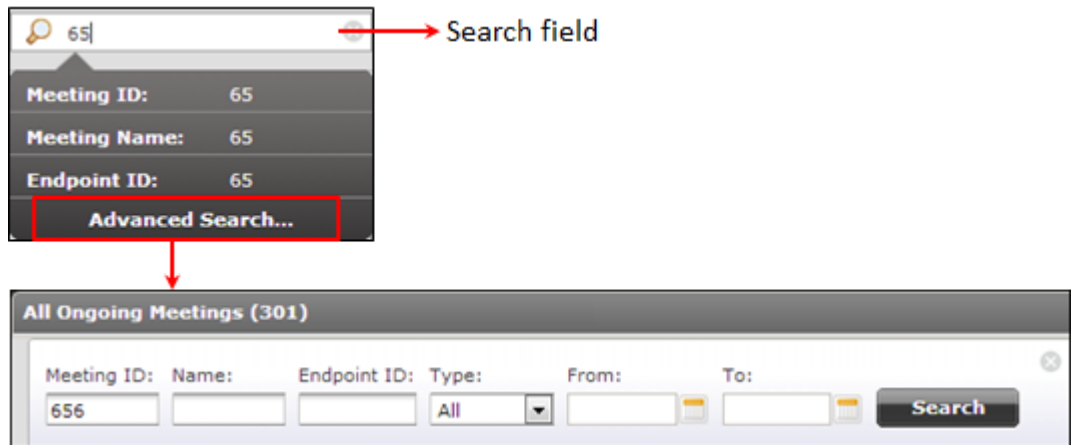


Figure 137: Using the Search feature on the Meetings tab

All host MCUs are listed in the **MCU** column with an indication of whether the meeting is cascaded.

All Gateways are listed in the **Gateway** column.

4. Select **Moderate**.

The In-meeting Control interface is not available for meetings or calls in which you are not a participant or the organizer.

5. Enter the moderator PIN if one is used for this meeting or call.

Monitoring Bandwidth and Port Utilization

About this task

You can monitor port and bandwidth utilization for MCUs, Scopia® Gateways and Scopia® Desktops configured in the system, to make sure that video traffic does not exceed the maximum utilization defined for the devices:

- View the overall bandwidth and device usage.
- View the bandwidth for all current and past meetings.
- View detailed information regarding bandwidth and port utilization as a report, as described in [Generating a Report](#) on page 266.

Procedure

1. Access the Scopia® Management administrator portal.

Overall status for bandwidth and device usage appears in the **Information** area of the **Dashboard** tab ([Figure 138: Bandwidth and Port Utilization](#) on page 217).

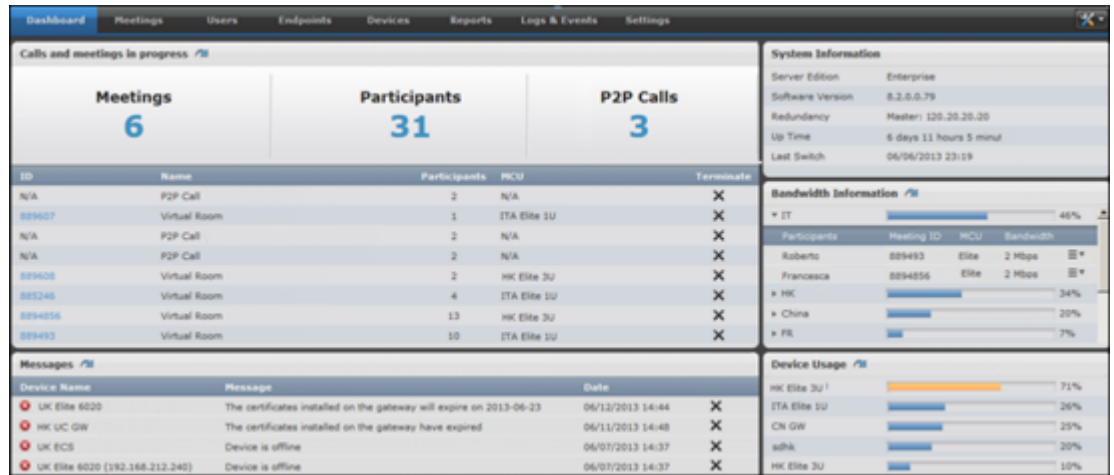


Figure 138: Bandwidth and Port Utilization

2. To view bandwidth utilization per meeting, select the **Meetings** tab.
The bandwidth for each meeting is displayed.

Checking the Status of Meetings

About this task

You can monitor the status of ongoing and upcoming meetings, and view the reason of a failure status.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Meetings** tab.

A list of all ongoing meetings appears.

If a meeting failed to create, for example, because of an MCU failure, the  icon appears next to the **Meeting ID**.

If meeting creation fails due to device failure, Scopia® Management attempts to recreate the meeting whenever it receives a dial-in call from a meeting participant. This allows the system multiple attempts at creating the meeting after the initial failure.

3. Select **Meetings** or **Point-to-Point calls** to filter the results for ongoing meetings.
4. Select **Future > All** to see all meetings that have not yet started.

Disconnecting Calls or Meetings

About this task

You can disconnect ongoing calls or meetings when a threshold is exceeded, for example, when the duration of the call exceeds the limits, or when the bandwidth used for that meeting or call exceeds the maximum bandwidth set for it.

Procedure

1. Access the Scopia® Management administrator portal.
2. If the meeting you want to disconnect appears in the **Calls and meetings in progress** section of the **Dashboard** tab, select the **Terminate** button as shown in [Figure 139: Disconnecting a meeting from the Dashboard tab](#) on page 218.

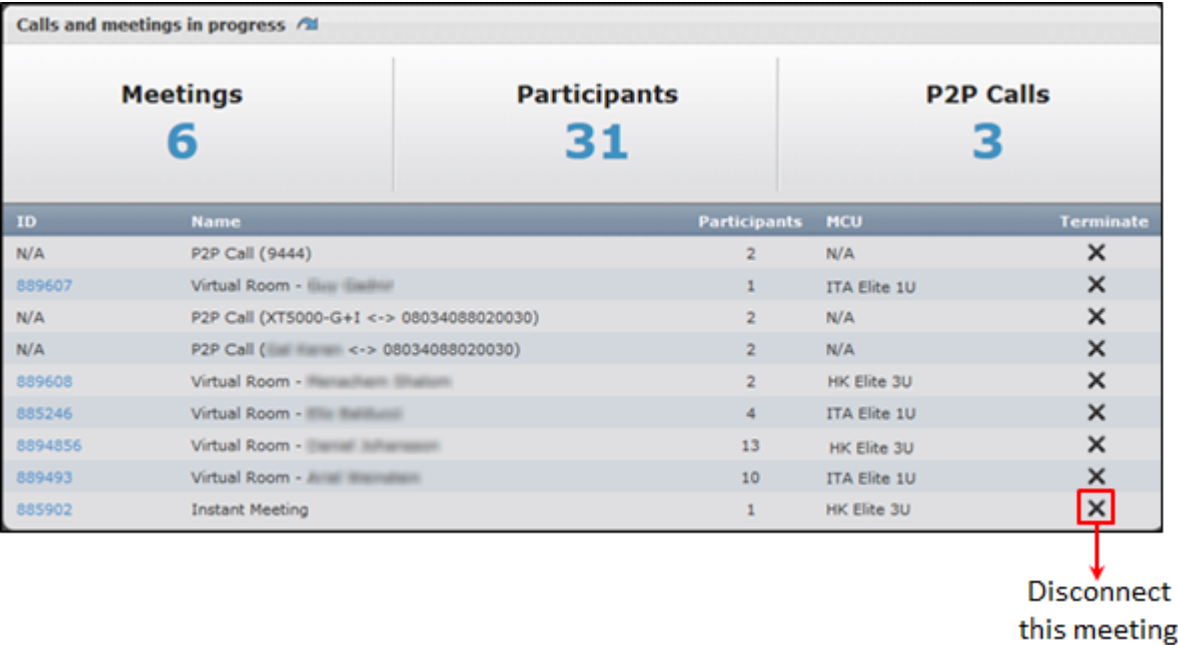


Figure 139: Disconnecting a meeting from the Dashboard tab

3. If the meeting you want to disconnect does not appear on the **Dashboard** tab, select the **Meetings** tab.
4. Select the meeting or call you want to disconnect.
5. Select **Meetings > Terminate Selected Meeting(s)**.

Downgrading the Meeting Bandwidth

About this task

You can downgrade the bandwidth for current meetings if, for example, the bandwidth is exceeded, or you want more bandwidth available for another meeting occurring at the same time. If you downgrade the bandwidth for a meeting, all participants are downgraded to the same bandwidth.

Procedure

1. Access the Scopia® Management administrator portal.
The Dashboard tab appears.
2. Select the meeting for which you want to downgrade bandwidth in the **Bandwidth Information** section of the **Dashboard** tab as shown in [Figure 140: Locating the Bandwidth Information section of the Dashboard tab](#) on page 219.

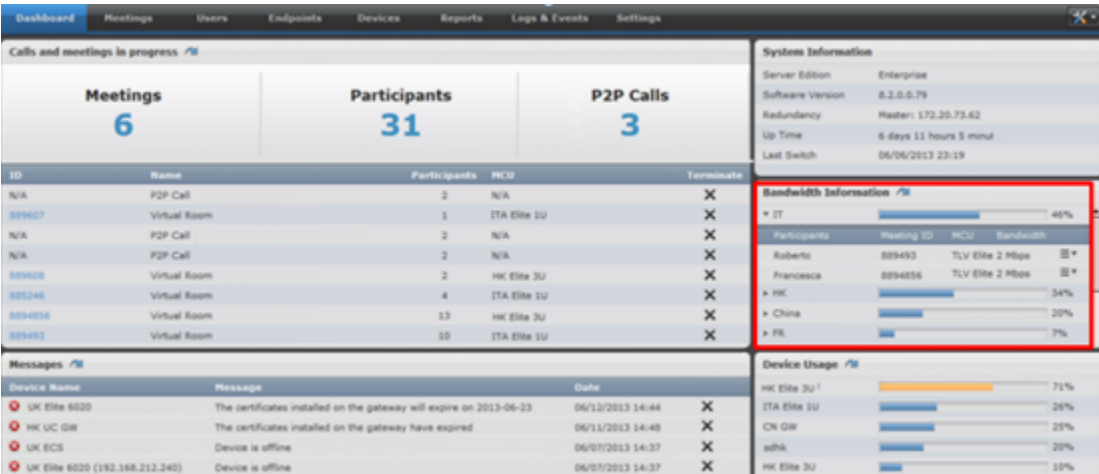


Figure 140: Locating the Bandwidth Information section of the Dashboard tab

3. Select the **Actions** button and then select **Change Meeting Bandwidth**. See [Figure 141: Downgrading the meeting bandwidth from the Dashboard tab](#) on page 219

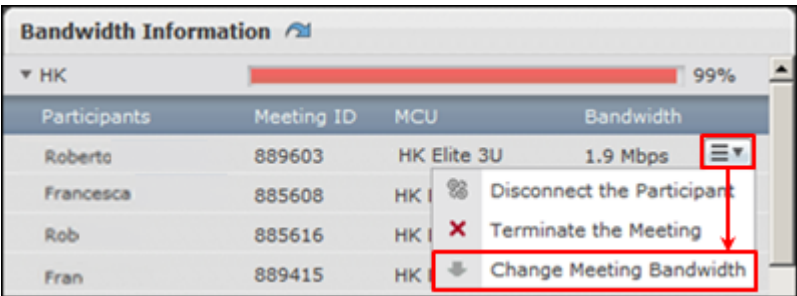


Figure 141: Downgrading the meeting bandwidth from the Dashboard tab.

The **Select Meeting Bandwidth** window appears.

4. Select the new meeting bandwidth.

5. Select **OK**.



Chapter 8 | Maintaining your Videoconferencing Network

This section details the ongoing administrator tasks required to maintain your video network, including backing up, restoring, and reflecting changes in the video devices and topology of your video network.

Navigation

- [High Availability of Scopia® Management](#) on page 221
- [Upgrading, Backing up and Restoring Scopia® Management Data](#) on page 239
- [Upgrading, Backing Up and Restoring Video Device Software](#) on page 244
- [Daily Maintenance of your Video Network](#) on page 252
- [Defining Video Usage Defaults](#) on page 254
- [Maintaining Scheduled Meetings](#) on page 259
- [Retrieving the Customer Support Package](#) on page 261
- [Uninstalling Avaya Scopia® Management](#) on page 262

High Availability of Scopia® Management

To provide high availability and continued service, you can deploy redundant Avaya Scopia® Management servers, in one of the following ways:

- Local redundancy

Deploy two Scopia® Management servers in the same location: a primary server and a secondary server. If the primary server fails, the secondary server automatically takes over without disrupting Scopia® Management functionality (does not include load balancing).

- Geographic redundancy

Deploy three Scopia® Management servers. Set up two servers as primary/secondary servers in the same location (local redundancy), and deploy the third as an off-site backup server in a different location. You can manually activate this server if the other servers fail, ensuring continued service even if there is a major failure or disaster at the main location.

[Figure 142: Local and geographical redundancy](#) on page 222 illustrates the different options of deploying Scopia® Management redundancy.

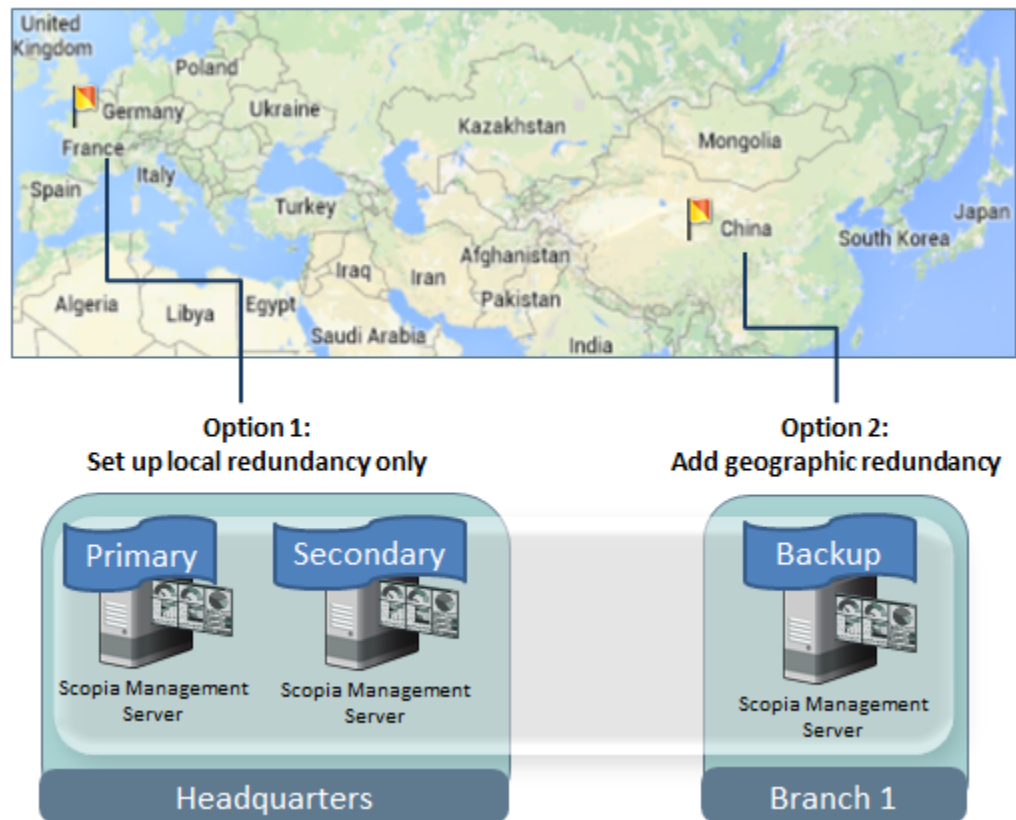


Figure 142: Local and geographical redundancy

Scopia® Management's redundant solution requires a license, but does not require third-party load balancers. Data is continuously synchronized between all Scopia® Management servers, including the internal database, system property files, and device upgrade packages.

Deploy your Scopia® Solution by referring to component names rather than IP addresses. Using a server name (or FQDN), like *smgmt.company.com* reduces maintenance when servers switch to their backups.

Avaya Scopia® Management retrieves licensing information from the Avaya Web License Manager (WebLM). If the primary Avaya Scopia® Management fails, the secondary Avaya Scopia® Management connects to the WebLM and uploads the same licenses to ensure continuity of the licensing policy (see [Figure 143: Retrieving licensing information in case of primary Avaya Scopia® Management failure](#) on page 223).

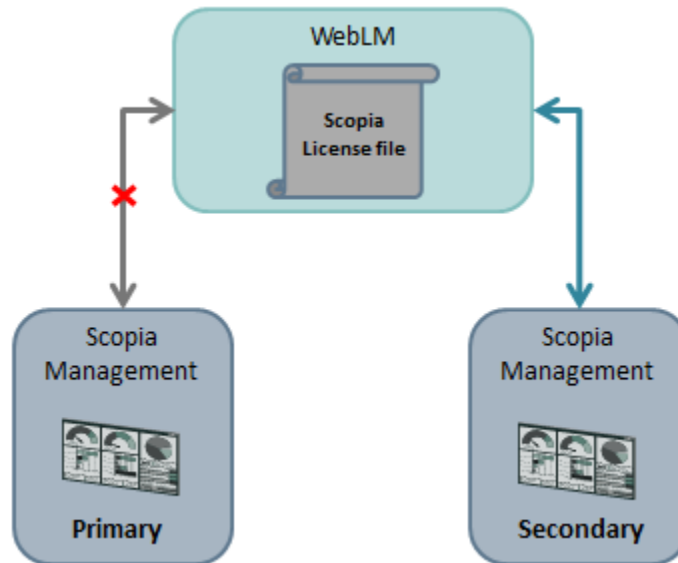


Figure 143: Retrieving licensing information in case of primary Avaya Scopia® Management failure

Once Scopia® Management's high availability is configured, you can view the redundancy status in real-time, including the current status and server addresses (see [Monitoring Redundancy Status](#) on page 230 for details).

These topics describe redundancy configuration and monitoring:

Navigation

- [Creating a Redundant Secondary Server for Scopia® Management](#) on page 223
- [Creating an Off-Site Backup Server for Scopia® Management](#) on page 228
- [Monitoring Redundancy Status](#) on page 230
- [Manually Promoting the Off-Site Backup Server](#) on page 233
- [Restoring Primary Server from Off-Site Backup Server](#) on page 236
- [Disabling Redundancy](#) on page 237

Creating a Redundant Secondary Server for Scopia® Management

About this task

You can deploy two Avaya Scopia® Management servers in the same location, one as the primary server and the other as a secondary server (local redundancy). If the primary server fails, the secondary server automatically takes over. For increased reliability, deploy a third server as an off-site backup (geographic redundancy). For details, see [High Availability of Scopia® Management](#) on page 221.

This procedure describes how to deploy two Scopia® Management servers in the same location for high availability (does not include load balancing functionality). Even if you are deploying geographic redundancy, you must first set up local redundancy as described below.

Before you begin

- Verify the same version of Scopia® Management is installed on two separate servers, in the same location and subnet.
- Decide on the primary Scopia® Management server, and set up all video network devices and users on this server first, following the instructions in [Initial Configuration Workflow](#) on page 36.
- When converting a standalone Scopia® Management deployment into a redundant deployment, we recommend using the previous standalone server as the primary server, to preserve existing data. Allocate a new private IP address to it, and use the previous IP address as the public virtual IP address of both servers, so that other components do not need to be reconfigured.

For example, if the previous Scopia® Management IP address was 1.2.3.4, this IP address is now used as the virtual IP address of both servers. Allocate a new private IP address to both the primary (1.2.3.5) and the secondary server (1.2.3.6).

- Decide whether to deploy local redundancy or geographic redundancy (see [High Availability of Scopia® Management](#) on page 221).
- For servers running Windows Server 2008, install WinPcap version 4.1.2 to enable the network switch to update its cache when a failover occurs. Download WinPcap from <http://www.winpcap.org/install/default.htm>.

! Important:

If you are securing your network using TLS, you must first configure redundancy, and then generate and install your TLS certificates (see [Securing Your Video Network Using TLS](#) on page 139). Otherwise, you will need to reconfigure TLS on the other Scopia® Management servers.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select  > **Redundancy Setup** ([Figure 144: Setting up local redundancy](#) on page 224).

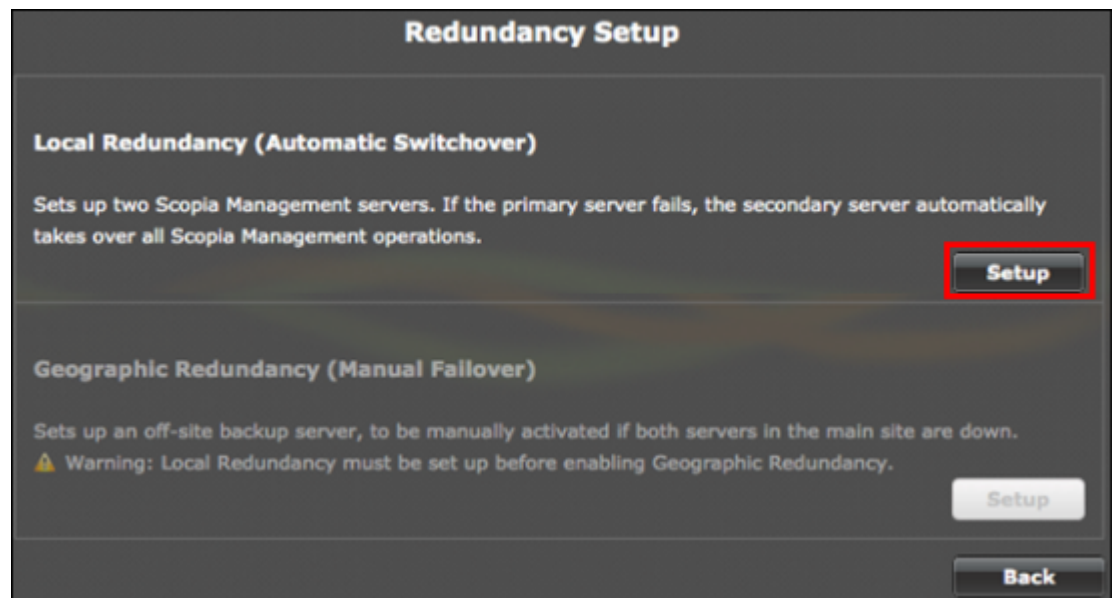


Figure 144: Setting up local redundancy

3. In the **Local Redundancy** area, select **Setup**.

Even if you are deploying geographic redundancy, you must first set up local redundancy.

4. Select the IP address of the primary Scopia® Management server from the list, and select **Next**.

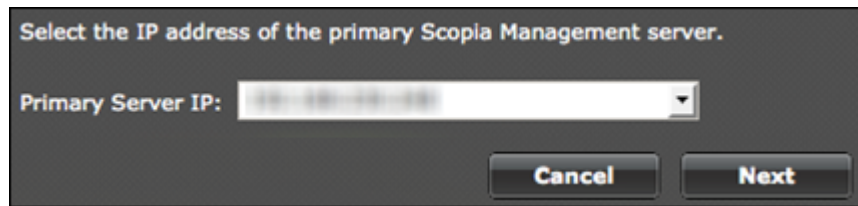


Figure 145: Selecting the primary server

5. Enter the following information for the secondary Scopia® Management server, and then select **Next**.

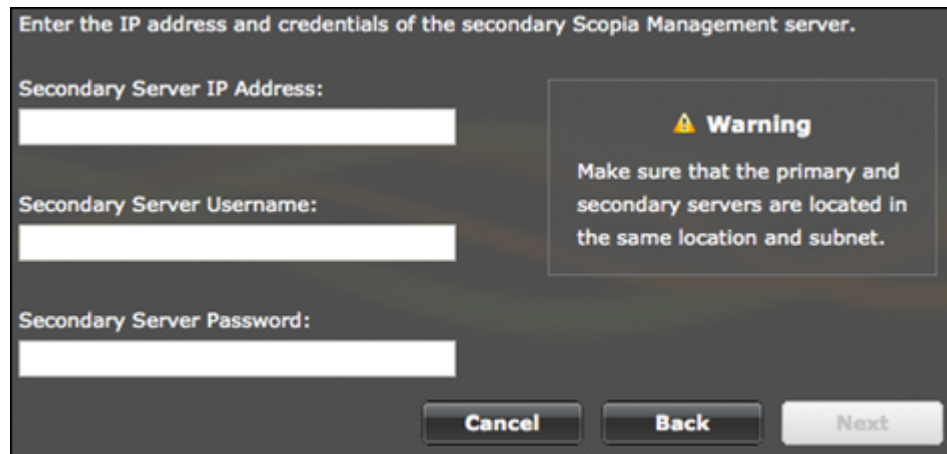


Figure 146: Setting up the secondary server

Table 48: Setting up the secondary server

Field	Description
IP Address	Enter the IP address of the secondary server.
Username	Enter the administrator login credentials required to access the secondary server.
Password	

6. Enter the virtual IP and FQDN as described below, and then select **Next**.

This creates a common destination address to represent the redundant servers to other components.

The virtual IP is shared by the primary and secondary Scopia Management servers, and is automatically used by the server that is active.

Virtual IP:

To access the server that is active using the FQDN, configure the FQDN on the DNS to point to the virtual IP.

FQDN URL:

Cancel **Back** **Next**

Figure 147: Setting up the virtual IP

Table 49: Setting up the virtual IP

Field	Description
Virtual IP	Enter the public virtual IP address representing both the primary and secondary Scopia® Management to other components. When converting a standalone Scopia® Management deployment to a redundant deployment: we recommend using the IP address of the previous standalone server as the new public virtual IP address of both servers, so that other components do not need to be reconfigured.
FQDN URL	Enter the URL that represents the virtual IP, as defined on your DNS server. If you are deploying an off-site backup server as well, this URL represents all redundant Scopia® Management servers. We recommend accessing Scopia® Management via its FQDN, which represents all Scopia® Management servers and always redirects to the server that is currently active.

- Enter the following settings for the subnet that the primary and secondary Scopia® Management servers belong to, and then select **Next**.

The primary server continuously pings the gateway to indicate that it is connected. If it fails to do so, the secondary server automatically takes over.

Enter the details of the subnet where Scopia Management is located.
Scopia Management pings the gateway to check the network connection.

Gateway IP Address:

Network Mask:

Port:

Warning

If the primary server fails to ping the gateway, the secondary server automatically takes over.

Figure 148: Configuring gateway settings

Table 50: Configuring gateway settings

Field	Description
Gateway IP Address	Enter the subnet's gateway (router) IP address.
Network Mask	Enter the dedicated subnet mask, which represents the range of IP addresses in the network.
Port	Enter the port Scopia® Management uses to check whether the specific gateway is available.

8. Select **Proceed** to finish setting up local redundancy.

The system confirms that the secondary server is now set up.

9. To test, access the Scopia® Management cluster from a web browser by entering the URL of the newly assigned virtual IP or FQDN.

The dashboard shows the **System Information** section in the top right hand side of the screen listing the redundancy status ([Figure 149: Redundancy status in System Information section of the dashboard](#) on page 227). Select the **Active** link for details.

System Information

Server Edition: Enterprise With GK

Software Version: 8.3

Redundancy: Active: 10.123.124.125

Up Time: 21 Minutes

Last Switch: 11/25/2013 16:46

Figure 149: Redundancy status in System Information section of the dashboard

10. (Optional) You can now secure your network with TLS, using Scopia® Management's FQDN (see [Securing Your Video Network Using TLS](#) on page 139).

If you are deploying an off-site backup server, you can configure TLS now or after setting up the backup server.

11. (Optional) For increased reliability, add an off-site backup server in a different location (see [Creating an Off-Site Backup Server for Scopia® Management](#) on page 228).

Creating an Off-Site Backup Server for Scopia® Management

About this task

You can deploy two Avaya Scopia® Management servers in the same location, one as the primary server and the other as a secondary server (local redundancy). If the primary server fails, the secondary server automatically takes over. For increased reliability, deploy a third server as an off-site backup (geographic redundancy). For details, see [High Availability of Scopia® Management](#) on page 221.

If the secondary server fails, you need to manually promote the backup server to become active (see [Manually Promoting the Off-Site Backup Server](#) on page 233). We recommend accessing Scopia® Management via its FQDN, which represents all Scopia® Management servers and always redirects to the server that is currently active.

Scopia® Management's internal database is synchronized between all redundant Scopia® Management servers. You do not need to configure an additional database for the off-site backup server.

Before you begin

- Set up two Scopia® Management servers in the main site, as described in [Creating a Redundant Secondary Server for Scopia® Management](#) on page 223.
- Verify that a third server (with the same version of Scopia® Management) is installed in a different location.

Procedure

1. Access the Scopia® Management administrator portal using the FQDN.
2. Select  > **Redundancy Setup** (see [Figure 150: Setting up geographical redundancy](#) on page 229).

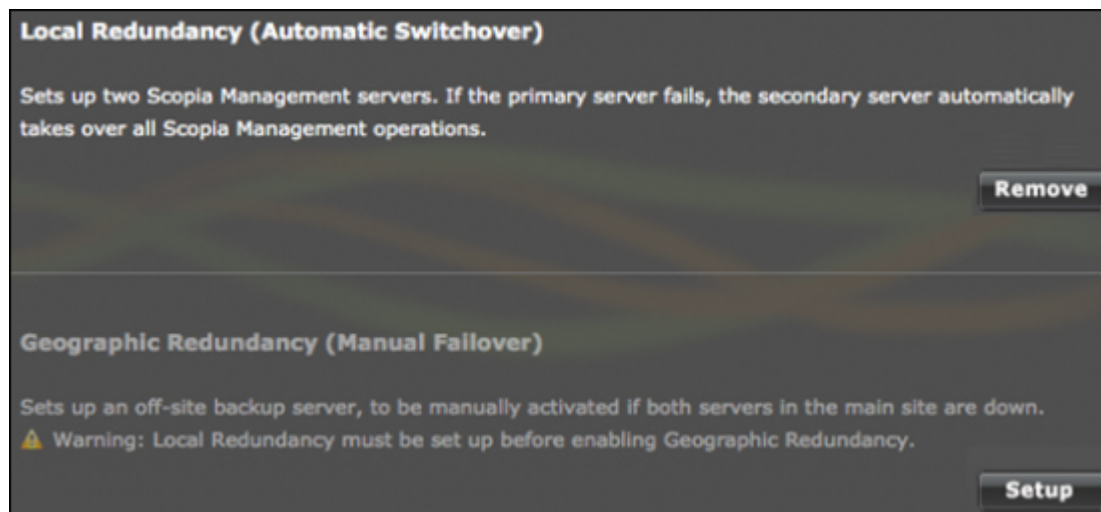


Figure 150: Setting up geographical redundancy

3. In the **Geographical Redundancy** area, select **Setup**.
4. Enter the following information for Scopia® Management's off-site backup server, and then select **Next**.

Figure 151: Setting up the backup server

Table 51: Setting up the backup server

Field	Description
IP Address	Enter the IP address of the off-site backup server.
Username	Enter the Scopia® Management login credentials required to access the off-site backup server.
Password	

5. Select **Proceed** to finish setting up geographical redundancy.
The system confirms that the off-site backup server is now set up.
6. Configure Scopia® Management's FQDN on the DNS server to point to both the virtual IP address (as the first IP address) and the off-site backup server's IP address. This ensures

that the FQDN always automatically directs you to the Scopia® Management server that is currently active.

7. (Optional) You can secure your network with TLS, using Scopia® Management's FQDN (see [Securing Your Video Network Using TLS](#) on page 139).

Monitoring Redundancy Status

About this task

Once you configure redundancy, Scopia® Management alerts you if it is not working properly. System administrators receive email alerts when:

- A switch occurs between the primary and secondary servers.
- The CPU on the active Scopia® Management server reaches 100% (contact Customer Support to configure).

To customize the email alert, see [Creating or Modifying an Alert Recipient Profile](#) on page 208. Scopia® Management also generates an alarm that is added to the event log, and can be forwarded to a third-party SNMP server (see [Real-time Monitoring](#) on page 205).

You can always check the redundancy status in the **System Information** area of the **Dashboard**:

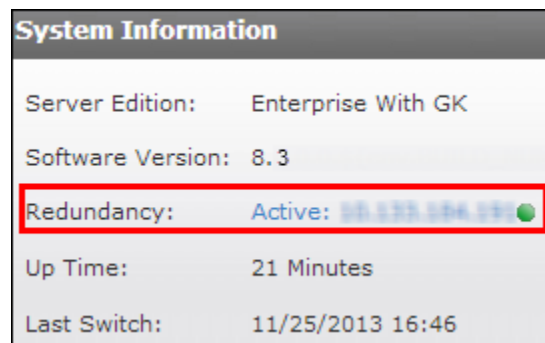


Figure 152: Redundancy status

The green  icon indicates that the active server is currently connected and functioning properly. The red  icon indicates an error and you should select the **Active** link for more details:

- Connection status of each redundant Scopia® Management server
- IP address of the current active server
- Time that the server has been active
- Date of the last hot swap
- Details of the redundancy configuration (such as the IP address of the standby server, the virtual IP address, and the FQDN)
- Data synchronization status

Procedure

1. Access the Scopia® Management administrator portal using the FQDN.
2. Navigate to the **System Information** area in the **Dashboard** tab ([Figure 152: Redundancy status](#) on page 230) to see the following information:

Table 52: Basic redundancy details

Field Name	Description
Redundancy	The IP address for the Scopia® Management server that is currently active. Typically, this is the IP address of the primary server, unless it is down. The green  icon indicates that the active server is currently connected and functioning properly, and the red  icon indicates a failure, either with one of the Scopia® Management servers or with the database synchronization.
Up Time	The period of time that the current server has been active (since the last switch).
Last Switch	The time and date of the last switch between the redundant Scopia® Management servers.

3. Select the IP address of the active server to view the following details:

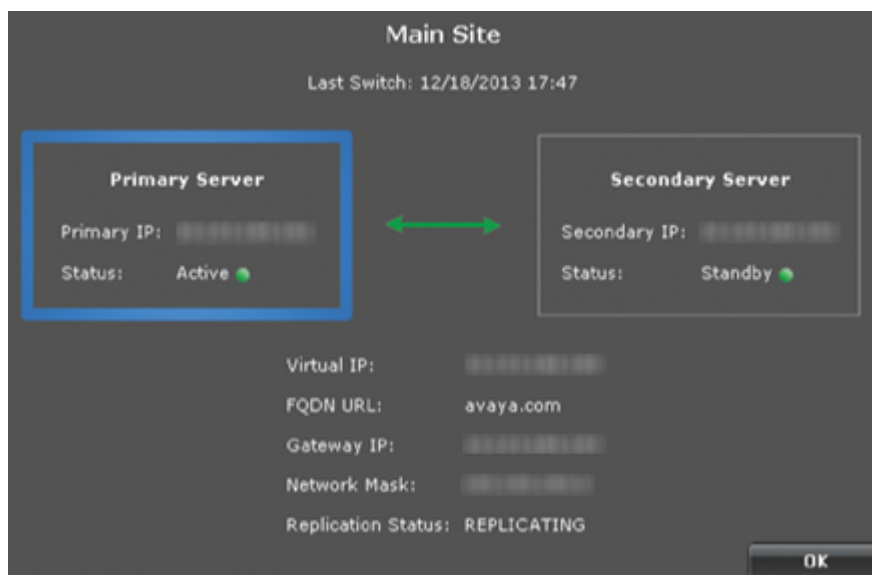


Figure 153: Detailed redundancy information

Table 53: Monitoring redundancy status

Field Name	Description
Last Switch	The time and date of the last switch between the redundant Scopia® Management servers.
Master Server/Standby Server	• Master IP/Standby IP: IP address of the primary/secondary Scopia® Management server. • Status: Indicates whether the server is currently active, or is in standby mode. The green  icon indicates that the server is currently connected and functioning properly, and the red  icon indicates a failure, either with one of the Scopia® Management servers or with the database synchronization.
Virtual IP	The public virtual IP address representing the primary and secondary Scopia® Management servers to other components.
FQDN URL	The URL that represents the virtual IP on your DNS server.
Gateway IP	The gateway (router) IP address used for the subnet to which your virtual IP address is part of.

Field Name	Description
Network Mask	The dedicated subnet mask, which represents the range of IP addresses in the network.
Replication Status	Indicates whether data is successfully synchronized between the redundant servers, with the following possible states: • Error: Data failed to synchronize due to an internal database error. • Replicating: Data synchronized and up to date on all redundant servers. • Syncing: Data is currently being synchronized between the redundant servers. • Waiting: Data is not being synchronized between redundant servers, possibly due to a failure in the network or in one of the servers. Check that the secondary and off-site backup servers are functioning.

Manually Promoting the Off-Site Backup Server

About this task

This procedure describes how to manually promote the off-site backup server, which is necessary if both Scopia® Management servers in the main site failed. This is not relevant if you deployed local redundancy only.

When the primary server in the main site fails, the secondary server automatically takes over. If both the primary and secondary servers fail (due to a major failure or disaster, for example), you need to change the role of the off-site backup server to active. The off-site backup server cannot automatically take over since the connection with the main site failed.

[Figure 154: When to promote the off-site backup server](#) on page 234 illustrates the event flow that occurs before you need to activate the backup server.

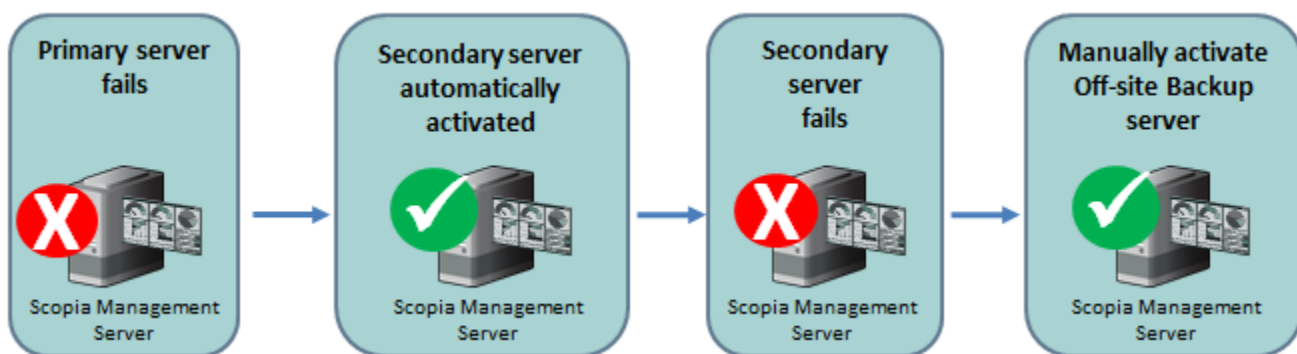


Figure 154: When to promote the off-site backup server

Before you begin

- You must have deployed an off-site backup server, as described in [Creating an Off-Site Backup Server for Scopia® Management](#) on page 228.
- Verify that both the primary and secondary servers on the main site are not functioning, as described in [Monitoring Redundancy Status](#) on page 230.
- Verify that you configured Scopia® Management's FQDN on the DNS server to point to both the virtual IP address (as the first IP address) and the off-site backup server's IP address. This ensures that the FQDN always automatically directs you to the Scopia® Management server that is currently active.

Procedure

1. Access the administrator portal of the off-site backup Scopia® Management server.
The redundancy status appears.

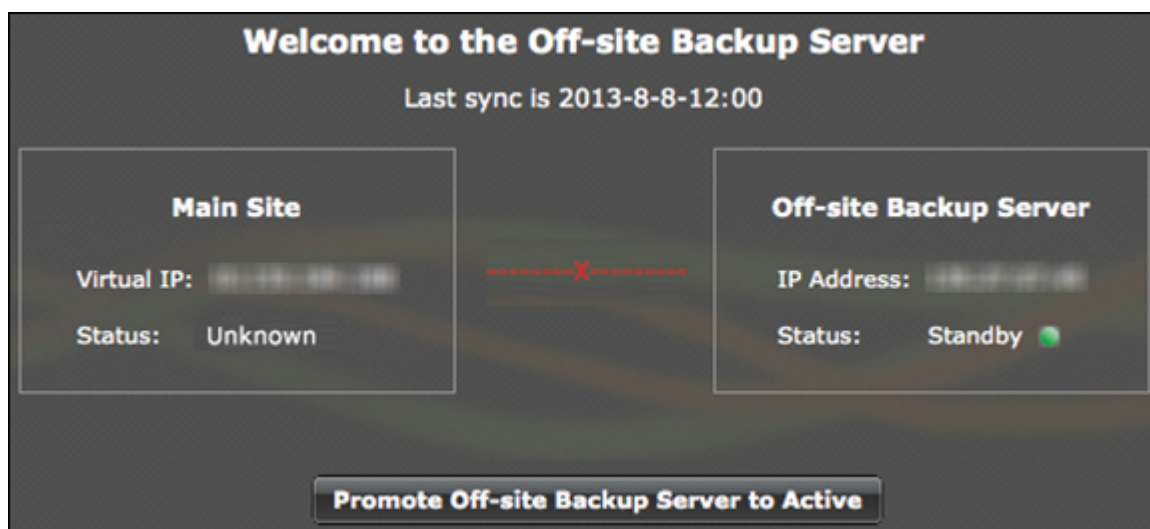


Figure 155: Promoting the off-site backup server

2. Select **Promote Backup Server to Master**, and then select **Process**:

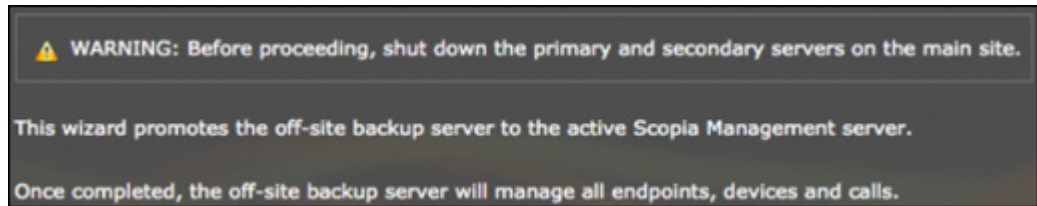


Figure 156: Geographic redundancy promotion wizard

3. In the confirmation prompt, select **Yes** to promote the off-site backup server.
A confirmation page appears, indicating that the backup server is now running as the active Scopia® Management server.
4. (Recommended) Verify that all devices are working properly as described in [Monitoring Network Devices via Scopia® Management](#) on page 210.
5. If there is any gatekeeper that is not functioning properly after promoting the backup server, move all endpoints and devices registered to it to another gatekeeper, as described below.
This is necessary if you are using the internal gatekeeper of the main site's Scopia® Management servers, or a standalone gatekeeper that is not running due to a general network failure at the main site.
If there is a network failure at the main site, you cannot move devices and endpoints in that location since they are offline.
 - a. Access the administrator portal of the off-site backup Scopia® Management server.
 - b. Select **Devices > Manage > Transfer all Registered Elements to**, and choose the target gatekeeper ([Figure 157: Moving devices to a functioning gatekeeper](#) on page 236).
This process typically takes a few seconds, and may take up to a few minutes.

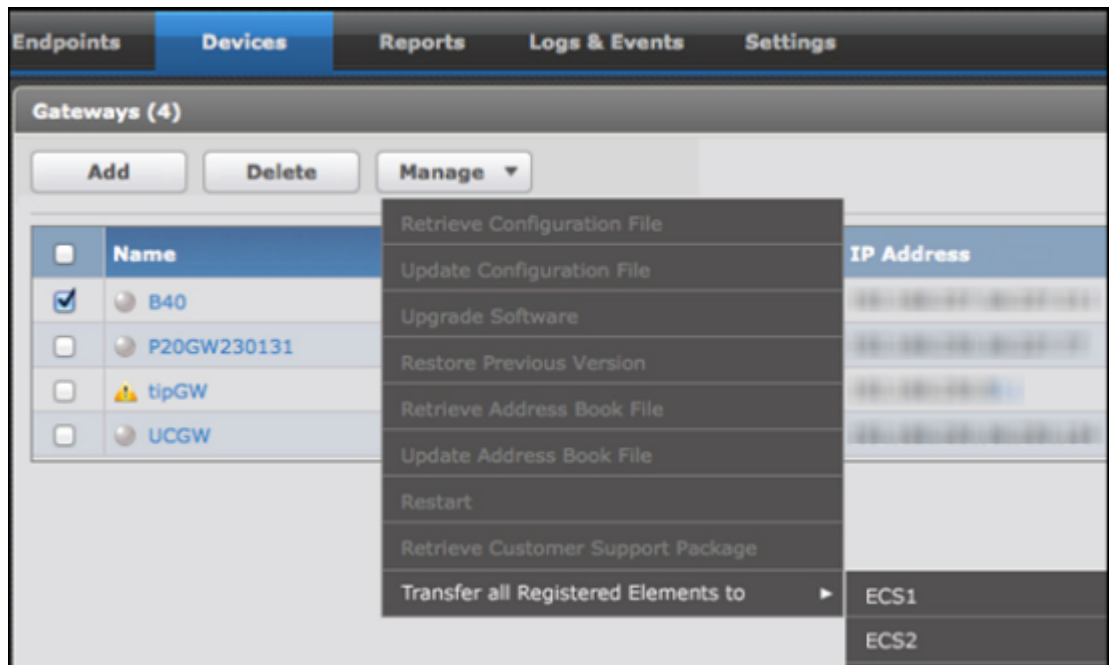


Figure 157: Moving devices to a functioning gatekeeper

6. When the primary Scopia® Management is functioning properly again (the main site's redundancy status displays a green  icon and switches to **Standby**, see [Monitoring Redundancy Status](#) on page 230), you can restore its role as the active server as described in [Restoring Primary Server from Off-Site Backup Server](#) on page 236.

Restoring Primary Server from Off-Site Backup Server

About this task

The off-site backup server takes over when the primary and secondary server have failed. Once the primary server is functioning properly, restore its status to active.

This is not relevant for local redundancy, where the primary server automatically resumes its active role once it is functioning.

Alternatively, you can create a new location with two new Scopia® Management servers as the primary and secondary servers (for example, if there was a natural disaster at the main location).

Before you begin

Verify that the primary Scopia® Management is functioning properly (the main site's redundancy status displays a green  icon and switches to **Standby**, see [Monitoring Redundancy Status](#) on page 230).

If you are creating a new location with two new Scopia® Management servers as the primary and secondary servers, install the same version of Scopia® Management on two separate servers, in the same location and subnet (see *Installation Guide for Avaya Scopia® Management*).

Procedure

1. Access the administrator portal of the off-site backup Scopia® Management server.
2. Select  > **Redundancy Setup**.
The **Redundancy Setup** page appears.

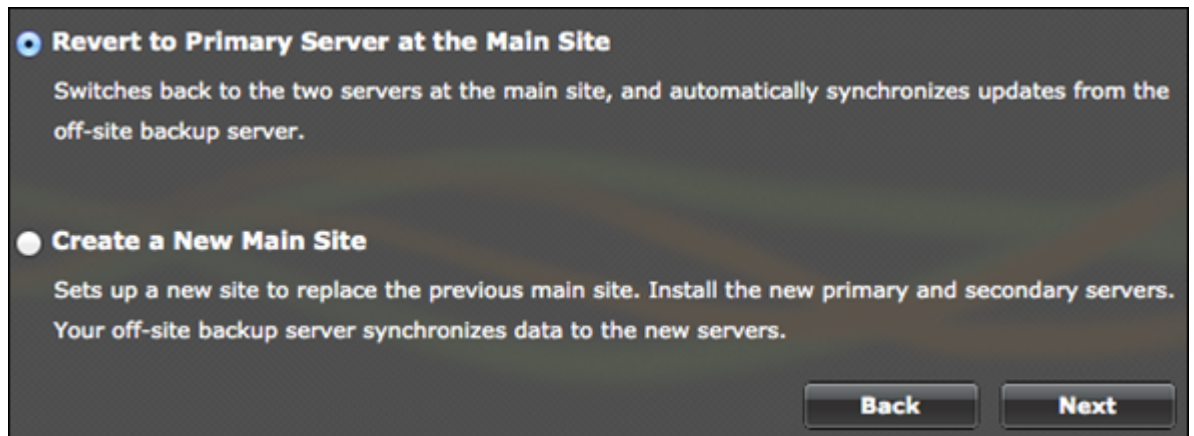


Figure 158: Setting up local redundancy

3. Select one of the following, and then **Next**.
 - **Revert to Primary Server at the Main Site:** Restores the original redundancy setup, where the primary server is active and the secondary and backup servers are in standby.
 - **Create a new Main Site:** Creates a new location with new Scopia® Management primary and secondary servers. The off-site backup server in the original setup continues functioning as the backup server. This option is typically used only if there is a natural disaster at the main site.

If you create a new main site, the wizard guides you through reconfiguring local redundancy, as described in [Creating a Redundant Secondary Server for Scopia® Management](#) on page 223.
4. If restoring the servers at the main site, select the IP address of the server to use as the active primary server, and then **Next**.

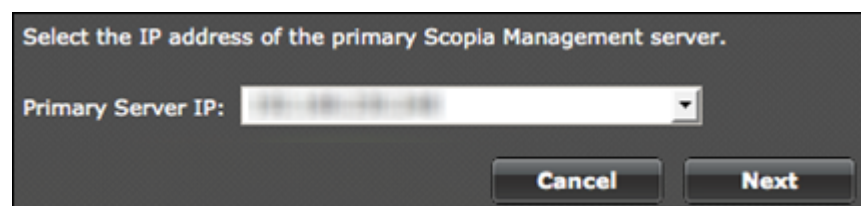


Figure 159: Selecting the primary server

A confirmation page appears, indicating that the primary and secondary servers are now functioning properly and the primary server resumed its role as the active server.

Disabling Redundancy

About this task

When disabling redundancy, you remove the connection between the redundant Scopia® Management servers. This is necessary, for example, if you need to replace the secondary server.

If you deployed an off-site backup server, first disable its redundancy, and then remove the secondary server's redundancy.

❗ Important:

Once you disable redundancy, you cannot restore it. To set up redundancy later, you need to reconfigure it from the beginning (see [Creating a Redundant Secondary Server for Scopia® Management](#) on page 223).

Procedure

1. Access the Scopia® Management administrator portal using the FQDN.
2. Select  > **Redundancy Setup**.
3. If you configured an off-site backup server, select **Remove** next to **Geographic Redundancy (Manual Failover)**, and then **Yes** at the prompt.

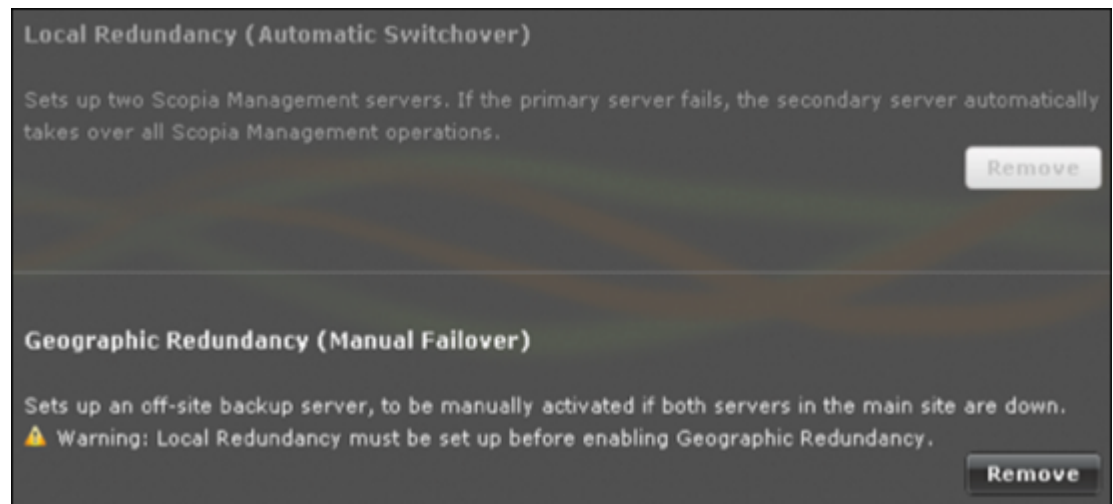


Figure 160: Disabling redundancy in Scopia® Management

The system confirms when geographic redundancy has been disabled.

4. Select **Remove** next to **Local Redundancy (Automatic Switchover)**, and then **Yes** at the prompt.

The system confirms when local redundancy has been disabled.

5. If you are replacing the secondary server, reconfigure redundancy as follows:
 - a. Uninstall the current secondary server (see [Uninstalling Avaya Scopia® Management](#) on page 262).
 - b. Install a new secondary server (see *Installation Guide for Avaya Scopia® Management*).

- c. Reconfigure redundancy (see [Creating a Redundant Secondary Server for Scopia® Management](#) on page 223).
-

Upgrading, Backing up and Restoring Scopia® Management Data

You can restore the Avaya Scopia® Management database and configuration files from a backup copy. You should back up your database and configuration files on a regular basis.

There are many reasons for performing system backups on a regular basis, such as:

- Hardware failure
- Software failure
- Data corruption
- User errors
- Before a software upgrade

Navigation

- [Backing Up Scopia® Management Manually](#) on page 239
- [Backing up Avaya Scopia® Management Automatically](#) on page 240
- [Restoring a Scopia® Management Backup File](#) on page 241
- [Upgrading Scopia® Management](#) on page 243

Backing Up Scopia® Management Manually

About this task

The backup procedure saves Scopia® Management's internal database and settings, which contains configuration and meeting scheduling information stored in local text files (known as property files).

Scopia® Management backs up all configuration files.

We recommend that you back up Avaya Scopia® Management manually before you perform maintenance procedures such as upgrade to save the latest configuration.

In redundant deployments, back up the primary Scopia® Management server only.

Procedure

1. Access the Scopia® Management administrator portal (on the primary server, for redundant deployments).
2. Select  > **Backup**.
The **Backup Database** window appears.

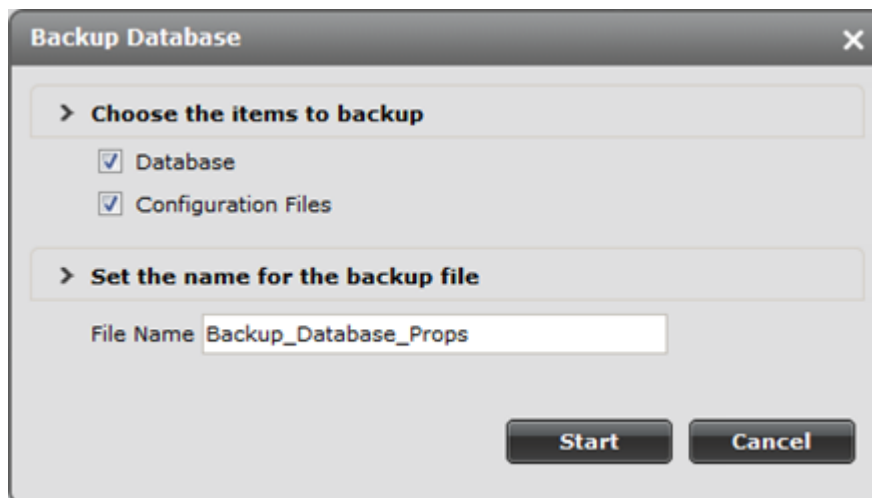


Figure 161: Backup Data Base window

3. Select the type of files you want to back up by selecting **Database** and **Configuration Files**.

4. Enter a filename for your backup file.

By default the file name format is Backup_Database_Props. After the backup process is completed, the current date (YYYYMMDD) and time (1421) stamps are automatically added to the file name. For example, Backup_Database_Props_20091215_1421.zip.

5. Select **Start**.

The backup process begins. Upon completion a result message is displayed and the backup file is downloaded.

Backing up Avaya Scopia® Management Automatically

About this task

To ensure that the files are backed up regularly, we recommend that you configure your Avaya Scopia® Management to perform the backup procedure automatically. If necessary, you can also perform the backup procedure manually as described in [Backing Up Scopia® Management Manually](#) on page 239.

In redundant deployments, back up the primary Scopia® Management server only.

Procedure

1. Access the Scopia® Management administrator portal (on the primary server, for redundant deployments).
2. Select **Settings > Maintenance > Backup**.

The Backup window opens.

Figure 162: Defining settings for the automatic backup

3. Select **Enable Auto Backup**.
4. Define the backing up settings as described in [Table 54: Configuring Avaya Scopia® Management to perform automatic backup](#) on page 241.

Table 54: Configuring Avaya Scopia® Management to perform automatic backup

Field Name	Description
Frequency	Set the days on which Avaya Scopia® Management performs automatic backup.
Start	Set the time when Avaya Scopia® Management performs automatic backup.
Destination	Select the location where Avaya Scopia® Management stores the backup file: Select Default to use the predefined location: <installation folder>/RADVISION/SCOPIA Management/ICM/Backup. Or Select Other and enter the path to the location on the network where you want to save the backup file (cannot be a local path).
Maximum storage size allocated to the backup data disk	Enter the value for the maximum storage space on the Avaya Scopia® Management server. When backup files reach this size, Avaya Scopia® Management starts overwriting the oldest backup files with the new ones.

5. Select **OK**.

Restoring a Scopia® Management Backup File

About this task

You can restore a previously backed up Scopia® Management server, including its internal database, configuration files and branding, using the Scopia® Management Backup and Restore tool. After the backup file is successfully restored, the Scopia® Management server automatically restarts.

In redundant deployments, restore the backup file only on the primary Scopia® Management server. The restored backup file is later transferred to the other Scopia® Management servers during synchronization.

Before you begin

Verify the following before restoring:

- The backup file you are restoring is from the same Scopia® Management edition (either standalone or with multi-tenant support), the same version, and the same database type as your current implementation.
- If you deployed Scopia® Management redundancy, you restore the backup file on the primary server only. Therefore, you must stop the following Scopia® Management services: first on the off-site backup server (only for geographic redundancy), and then on the secondary server. Otherwise, it can damage the internal database.

Procedure

1. Access the Scopia® Management administrator portal (on the primary server, for redundant deployments).
2. Select  > **Restore**.

The **Restore** window appears with the list of backup files.

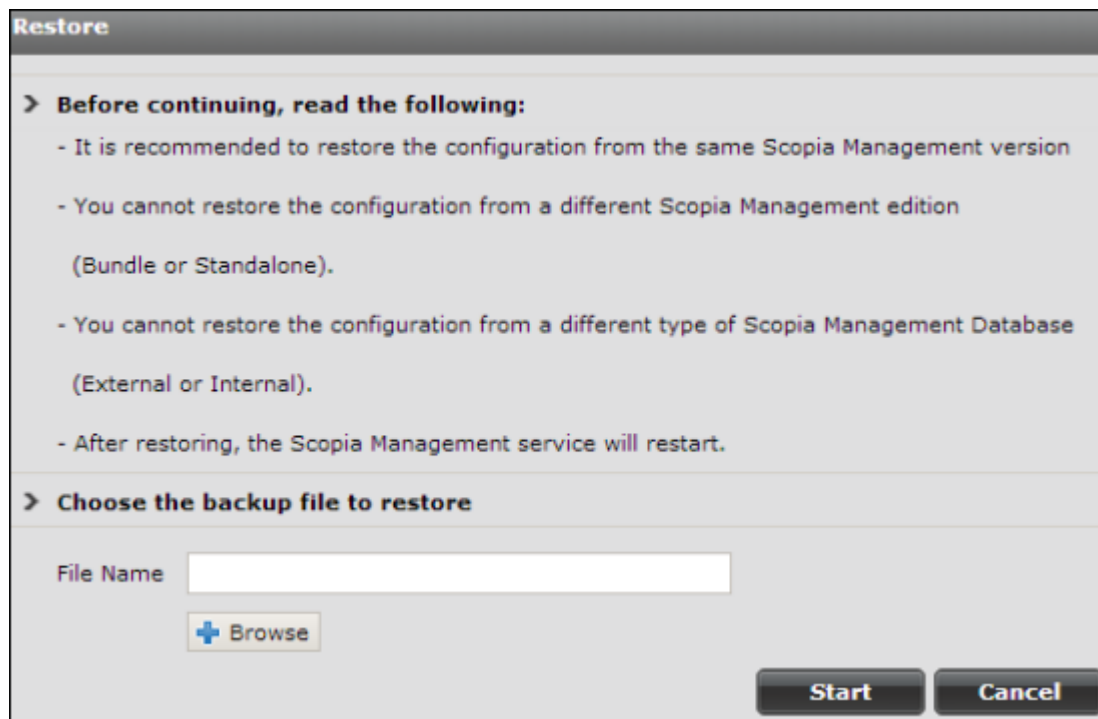


Figure 163: Restore window

3. Select **Browse** to locate and upload the backup file to restore.

! Important:

The backup file must be from the same edition, version, and database type as your current Scopia® Management.

4. Select **Start**.

The restore process begins. The system confirms when the restore is completed, and the Scopia® Management server restarts.

5. If restoring the backup file in a redundant deployment, complete the procedure as follows:
 - a. Verify that the primary Scopia® Management service restarted correctly.
 - b. Start the Scopia® Management services on both the secondary server and the off-site backup Scopia® Management server (for geographic redundancy only), to automatically synchronize restored settings to that server.

Upgrading Scopia® Management

About this task

The upgrade procedure may vary depending on the release number and the size of the jump from the current installation to the new release. The upgrade procedure may take up to ten minutes. For more information on the upgrade procedure, see the *Release Notes for Avaya Scopia® Management* for the relevant version.

! Important:

Do not attempt to restore the database and configuration files from an old Scopia® Management version. You can only back up and restore database and configuration files within the same Scopia® Management release number.

Before you begin

- Back up your Scopia® Management configuration files before performing the upgrade, as described in [Backing Up Scopia® Management Manually](#) on page 239.
For redundant deployments, back up on the primary server only.
- If you are upgrading Scopia® Management from a version below 8.2.0.0.122, you must first perform that upgrade first, and then upgrade to a later version.
- For redundant deployments, you must upgrade the servers in the following order: first the off-site backup server (if deployed), followed by the secondary server, and then the primary server. This ensures a successful upgrade.

Upgrading, Backing Up and Restoring Video Device Software

Scopia® Management enables you to manage software upgrades for MCUs and gateways, as well as Avaya and third party endpoints. Upgrades are managed by applying an upgrade file to chosen devices in Avaya Scopia® Management.

Before upgrading these devices, you must retrieve their configuration file using Scopia® Management.

Navigation

- [Editing Upgrade History of Video Devices](#) on page 244
- [Upgrading the Software File of a Video Device](#) on page 245
- [Removing a Software Upgrade File from a Video Device](#) on page 248
- [Backing Up and Duplicating a Video Device Configuration](#) on page 249
- [Updating License Keys of Avaya MCUs or Gateways](#) on page 250
- [Restoring the Previous Software Version of a Network Device](#) on page 250
- [Downgrading your Your Network Device](#) on page 252

Editing Upgrade History of Video Devices

About this task

You can view or remove entries from the Device Upload log, which displays the history of all your attempts to upload a software upgrade file, update configuration files, update the endpoint's address book file, and shows all scheduled future upload attempts, via Scopia® Management.

If using Application Server P/N 55876-00002, make sure to remove log files on a regular basis to ensure that there is enough disk space.

You can view and edit the upgrades of the following devices:

- Gatekeepers
- MCU
- Avaya Scopia® SIP Gateway
- Scopia® Video Gateway
- Endpoints: Avaya Scopia® XT Series, Scopia® VC240, Polycom, Tandberg, and Sony endpoints only.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Logs & Events** tab.
3. Select **Upgrade Results** or **Configuration Updates** from the sidebar.
4. Select the type of device from the dropdown list.

The device history is displayed, with a log of each attempt to upload a software upgrade file, update configuration files, update the endpoint's address book file, and all scheduled future upload attempts.

5. (Optional) You can delete upload logs that are no longer necessary by selecting the relevant logs and **Delete**. To delete all upload logs for this device, select **Delete All**.

Upgrading the Software File of a Video Device

About this task

You can quickly and easily perform remote software upgrades of video devices from Avaya Scopia® Management by uploading an upgrade file and applying it to the device. Upgrade files are supplied by the device vendor.

You can upgrade the following devices via Avaya Scopia® Management:

- Scopia® Elite MCU
- Gateways, including Scopia® Video Gateway, Avaya Scopia® SIP Gateway, Avaya Scopia® TIP Gateway
- Room systems and personal endpoints, including Avaya Scopia® XT Series, Scopia® VC240, and third-party endpoints from Sony or Polycom.

Important:

For gateways, perform the upgrade remotely using the Scopia® Management. You cannot upgrade the firmware of the gateway directly on the device.

Depending on your support contract, you can upgrade to:

- The next major version.

Upgrading a major version requires a new license.

This kind of upgrade changes one of the first two digits in a version number. For example, upgrading from version 8.0 to version 8.1 requires a new license.

- An incremental version.

Upgrading an incremental version does not require a new license.

This kind of upgrade changes the third, fourth and fifth digits in the version number. For example, upgrading from 8.0.0.34.0 to 8.0.0.36.1 or to 8.0.0.36.2 does not require a new license.

Upgrades may require first applying the major upgrade and then the incremental upgrade within that major version. For example, to upgrade from 8.0.0.38.2 to 8.1.0.0.1, first apply the major upgrade to 8.1.0.0.0, and then the incremental upgrade to 8.1.0.0.1.

Before you begin

Before upgrading your video network devices, including endpoints, do the following:

- Before upgrading a video device software, back up its configuration by retrieving its configuration file. For more information on remote backups, see [Backing Up and Duplicating a Video Device Configuration](#) on page 249.
- Go to <http://licensing.radvision.com/> to apply for and download your upgrade package.
- If you upgrade to a major version, ensure you have a new license key. The upgrade procedure is different when upgrading to a major new version compared with smaller incremental upgrades. See [Updating License Keys of Avaya MCUs or Gateways](#) on page 250 for details.
- Navigate to the device and select the **Access** tab. Enter a name and password for automatic login to the video device during the upgrade process. We recommend using the same name across the deployment.
- If you are upgrading endpoints, verify that it is managed by Avaya Scopia® Management. See [Managing Endpoints using Scopia® Management](#) on page 113 for details.
- If you are simultaneously upgrading multiple endpoints (of the same type), it is useful to first assign labels to the endpoints, to help you quickly select these endpoints. See [Organizing Endpoints into Groups with Labels](#) on page 129 for details.

Procedure

1. Access the Avaya Scopia® Management administrator portal.
2. Select the **Endpoints** or **Devices** tab.
3. Locate the video device as explained in [Searching for a Video Device](#) on page 252.
4. Select the device to be upgraded.

Important:

You can simultaneously upgrade all endpoints of the same type.

You cannot upgrade LifeSize endpoints via Scopia® Management.

5. Select **Manage > Upgrade Software**.

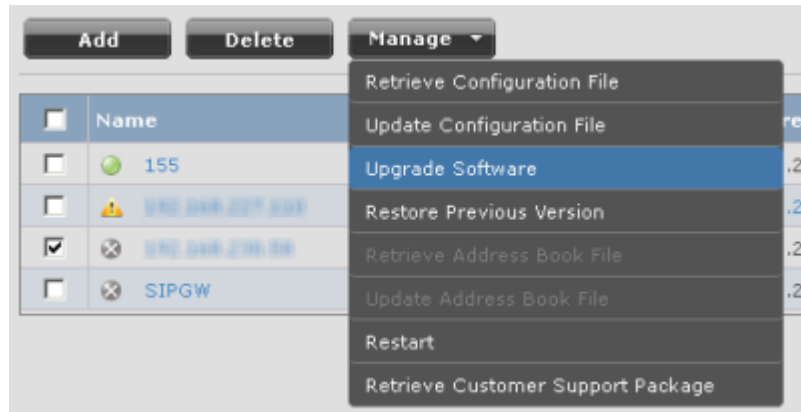


Figure 164: Upgrading the software file of a device

6. At the prompt, select **OK** to shut down the video device for a few minutes. This disconnects all active calls.
7. If there is no upgrade package in the dialog box, select **Add**.
8. Select **Browse** to search for the package you want to upload.

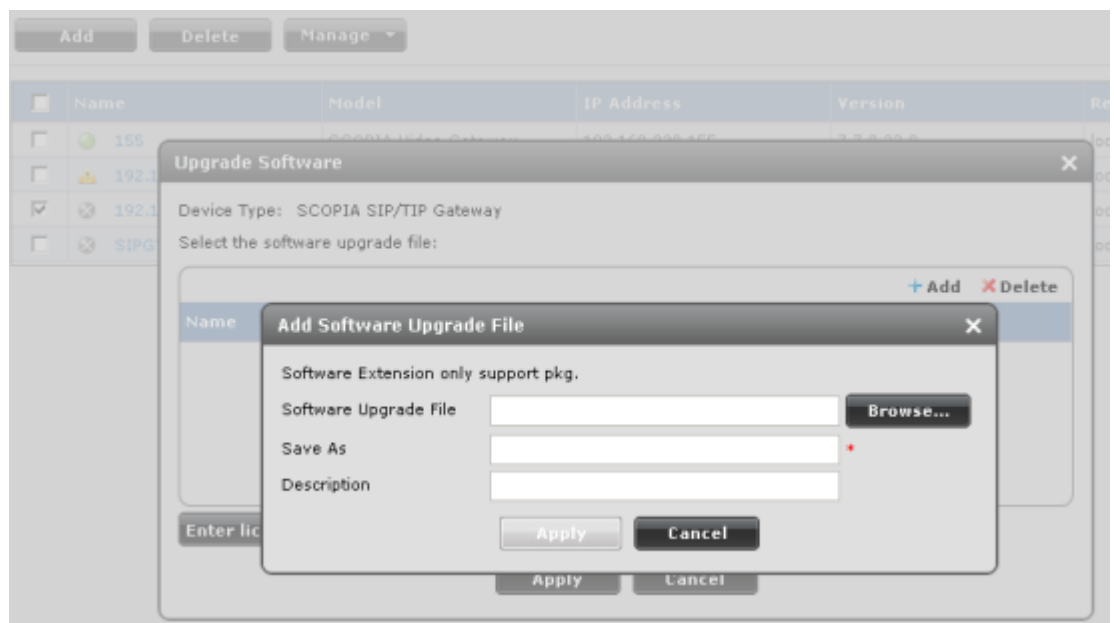


Figure 165: Uploading software update

Table 55: Entering browsing details

Field	Description
Software Upgrade File	This field is automatically filled when you select the software upgrade file.
Save As	Enter the name of the software upgrade file.

Field	Description
Description	Enter a free text description of the upgrade package (for example, the version number).
Version	This is the version number of the package you are upgrading too. For Polycom and Tandberg endpoints, enter the version number of the upgrade file in the F7.2 PAL/NTSC format. See the supplier's documentation for more information on these formats.

9. Select **Apply** to save the upgrade file and its information in Scopia® Management.
10. If required, enter license keys.
11. Select **Apply**.

The system notifies that the video device shuts down for several minutes, causing all the active calls to be disconnected.

If using Application Server P/N 55876-00002, make sure to remove upgrade packages on a regular basis to ensure that there is enough disk space.

Removing a Software Upgrade File from a Video Device

About this task

You can quickly and easily perform remote software upgrades of video devices from Avaya Scopia® Management by selecting the video device and applying an upgrade file. Upgrade files are supplied by the vendor of the video device.

For example, you can upgrade the Scopia® Elite MCU, Scopia® Video Gateway, Avaya Scopia® SIP Gateway, Avaya Scopia® TIP Gateway, room systems such as the Avaya Scopia® XT Series, and endpoints like the Scopia® VC240 or third party endpoints from Sony or Polycom.

This section describes how to remove the software upgrade file if it is no longer required in Scopia® Management's list of upgrade files.

If using Application Server P/N 55876-00002, make sure to remove upgrade packages on a regular basis to ensure that there is enough disk space.

Procedure

1. Log in to the Scopia® Management administrator portal.
2. Select the **Endpoints** or **Devices** tab.
3. Select the video device(s).

Important:

You can narrow your search of video devices by sorting them with one of the sidebar menu tabs. See [Searching for a Video Device](#) on page 252 for more information.

4. Select **Manage > Upgrade Software**.
 5. At the prompt select **OK** to shut down the video device for a few minutes. This disconnects all active calls.
 6. Select the software upgrade file you require.
 7. Select **Delete**.
 8. Select **Apply** to save your changes.
- The software upgrade file is removed from the database.
-

Backing Up and Duplicating a Video Device Configuration

About this task

You can retrieve the configuration file for purposes of backup, before upgrade, or for remote configuration.

For example, you can retrieve and backup the configuration settings of Scopia® Elite MCU, Scopia® Video Gateway, Avaya Scopia® SIP Gateway, Avaya Scopia® TIP Gateway, room systems such as the Avaya Scopia® XT Series, and endpoints like the Scopia® VC240 or third party endpoints from Sony or Polycom.

You can also apply those configuration settings across multiple video devices in your organization. The retrieved settings are only generic, therefore settings such as the endpoint's IP address are not stored.

This procedure describes how to retrieve the configuration file and store it in Scopia® Management, and how to apply the settings to other video devices.

Procedure

1. Login to the Avaya Scopia® Management administrator portal.
2. Select the **Endpoints** or **Devices** tab.
3. Select the specific, online video device.

Important:

You can narrow your search of video devices by sorting them as explained in [Searching for a Video Device](#) on page 252.

4. Follow these steps to retrieve the configuration file:
 - a. Select **Update > Retrieve configuration file**
 - b. Select **Yes**
 - c. If required, change the filename and a description of the new configuration file.
 - d. Select **OK** to save the file in the Scopia® Management database.
5. Follow these steps to apply or retrieve a configuration file to other online video devices:
 - a. Select the devices you want to update.
 - b. Select **Update > Update configuration**.

- c. Select **Yes** to start updating the video device configuration.
- d. Select the file with which to update the selected video devices.

The Update Configuration window shows a list of the configuration files that were previously retrieved, and are associated with the selected video device types.

- e. Select **Apply**.
-

Updating License Keys of Avaya MCUs or Gateways

About this task

Network administrators can update license keys from Scopia® Management when they increase capacity or increase ports with a flexible license.

The remote license update functionality is available for these network devices:

- MCUs, except Scopia® MCU
- Scopia® Video Gateway
- Avaya Scopia® SIP Gateway
- Avaya Scopia® TIP Gateway

Before you begin

Go to <http://licensing.radvision.com/> to apply for and download your upgrade package. If you upgrade to a major version, ensure you have a new license key.

Procedure

1. Login to the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. Select the **MCUs** or **Gateways** tab in the sidebar menu.
4. Select the link in the **Name** field of the required MCU.
5. Select the **Licensing** tab.

If the license is temporary, the **Remaining Days** field will display the number of days before the license expires.

6. Enter the new license key in the **Update License Key** field.
7. Select **Apply**.

The system confirms the license has been updated. If there are any problems with this process, verify the license key is accurate and that the system can properly access the MCU.

Restoring the Previous Software Version of a Network Device

About this task

This section explains how to restore a previous software version after you upgrade your network device. You can restore the same software version only once.

During this procedure the network device shuts down for a few minutes causing all active calls to be disconnected.

Some parameters are not backed up and cannot be restored:

- IP address
- Scopia® Video Gateway IP mask
- Default router IP address
- MTU size - the size of the packets received from the gateway
- DNS suffix
- DNS primary address
- DNS secondary address

Procedure

1. Access the Scopia® Management administrator portal.
2. Search for an online network device as explained in [Searching for a Video Device](#) on page 252.
3. Select the network device whose software version you want to restore.
4. Select **Manage > Restore Previous Version**.

The system informs you that all active calls on the device will be disconnected when you begin the process.

5. Select **Yes** in the confirmation message.

The **Update Log** window opens showing the task progress ([Figure 166: Progress of restoring a software package](#) on page 251).



Figure 166: Progress of restoring a software package

Downgrading your Your Network Device

If necessary, you can downgrade your network device in one of the following ways:

- To downgrade one version back after you upgraded your network device, perform the procedure in [Restoring the Previous Software Version of a Network Device](#) on page 250.
- To downgrade to a version earlier than the previous version, see [Upgrading the Software File of a Video Device](#) on page 245.

Daily Maintenance of your Video Network

This section provides daily procedures for maintaining your network devices, meeting types, meeting groups and scheduled meetings.

Navigation

- [Searching for a Video Device](#) on page 252
- [Removing a Video Device from Scopia® Management](#) on page 253
- [Preparing a Device for Maintenance](#) on page 254
- [Managing Bandwidth in your Network](#) on page 254

Searching for a Video Device

About this task

You can search for a specific endpoint or network device and modify some of its settings, such as maximum bandwidth, or location.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Endpoints** or **Devices** tab.
You can search through the displayed list, or narrow the list by selecting one of the tabs in the sidebar menu.
3. For a basic search, enter the first few characters of the device's name or IP address in the **Search** field.
4. For an advanced search, select the  and enter the following information, as required:

Table 56: Searching for a video device

Field Name	Description
Name	Enter the first few characters of the device you want to find.
Dialing Info	Enter the first few characters of the endpoint's dialing string.
Version	Enter the first few characters of the device's software version number.
IP Address	Enter the first few characters of the device's IP address.
Vendor	Search for the required endpoint in the supplier global list by selecting All . You can narrow your search by selecting an endpoint from the supplier's list.

5. Select **Search**.

Removing a Video Device from Scopia® Management

About this task

Deleted video devices are not added to the Scopia® Management database in any subsequent auto-detect operations.

You can add a deleted video device manually by selecting the **Add** icon in one of the device views.

Before you begin

- If you are removing an endpoint that is still listed in your organization's LDAP server, you must first remove the endpoint from the LDAP server, and then remove it from Scopia® Management. Otherwise, the endpoint will be added back to Scopia® Management the next time it is synchronized with the LDAP server.
- If you are removing an endpoint that is still registered to your gatekeeper, we suggest that you first remove the endpoint from the gatekeeper, and then remove it from Scopia® Management. Otherwise, you must deselect the endpoint the next time Scopia® Management is synchronized with the gatekeeper, to prevent the endpoint from being added back.

Procedure

1. Log in to the Scopia® Management administrator portal.
2. Select the **Endpoints** or **Devices** tab.
3. Search for an online video device as explained in [Searching for a Video Device](#) on page 252.
4. Select the video device to be removed. To remove all the devices, select the list heading.

Only service providers or administrators of a distributed environment can delete network devices.

5. Select **Delete**.
6. At the prompt select **Yes**.

The device profile, as well as any information about the device, is removed from Scopia® Management.

Preparing a Device for Maintenance

About this task

Before performing maintenance on MCUs and Gateways, you can change their status to **In-maintenance**. For example, this feature is used for upgrading the device. When a device's status is in-maintenance, it is still part of the network, and can be put back online at any time.

Scopia® Management cannot schedule meetings for an MCU that is in-maintenance. Scopia® Management attempts to reschedule upcoming meetings for these MCU on other MCUs that use the same services and have sufficient, available resources. If no replacement MCUs are available when the MCU status is changed back to online, upcoming meetings are lost and not restored.

Procedure

1. Log in to the Scopia® Management administrator portal.
 2. Select the **Devices** tab.
 3. Select the **MCUs** or **Gateways** tab in the sidebar menu.
 4. Select the link in the **Name** column for the relevant device.
 5. Select the **Configure** tab.
 6. Select the **In Maintenance** checkbox.
 7. Select **Apply** to save your changes.
-

Managing Bandwidth in your Network

Bandwidth for in-zone, cross-zone and pro-to-pro calls are managed within Scopia® Management. The following topics describe how to configure bandwidth thresholds.

- [Defining Bandwidth Limits for a Location](#) on page 39
- [Defining Scopia® Desktop Bandwidth for a User Profile](#) on page 164

Defining Video Usage Defaults

About this task

As part of managing your MCU and other video network resources, you can define meeting policies for both scheduled and instant meetings (initiated spontaneously). This is especially useful if you have limited MCU capacity or want to limit the bandwidth consumption.

These settings allow you to carefully monitor how meetings start and end, and their duration. You can also limit the number of participants in an instant meeting, or the default duration of meetings.

We recommend using Scopia® Management meeting reports to inform you about the videoconferencing usage in your organization ([Tracking System Usage with Reports](#) on page 264). Devise company policies based on the reports, and then adjust the default meeting policies to suit the needs of your organization. For example, if management decides to cut on bandwidth costs and reports show some video meetings last several hours, you can limit the default meeting duration to help participants focus on shorter meetings.

Procedure

1. Access the Scopia® Management administrator portal.
2. Select **Settings > Meetings > Policies**.
3. Define settings for meetings that users schedule in advance to reserve video network resources, such as MCUs and endpoints.

Scheduled Meetings

Default Duration: Minutes

Default Dialing Mode: ☒ Dial-out ☐ Dial-in

Termination: ☐ At scheduled time, alert minutes before meeting ends
☒ 0 minutes after all participants have left the meeting

Maximum Recurring Meetings Duration days

Launch Meetings Minute(s) Before Scheduled Start Time

☐ Waiting Room Timeout Minute(s) After The Waiting Room Start

Meeting Auto Extend Length Minutes

Maximum Length of Meeting Extension Hours

☐ Delete meetings older than days

Figure 167: Defining policies for scheduled meetings

Table 57: Defining policies for scheduled meetings

Field	Description
Default Duration	Enter the default meeting duration for all meetings scheduled from the Scopia® Management user portal. Users can modify this when scheduling a meeting. A few minutes before the default end time, users see an alert and can extend the meeting. For example, if management decides to cut on bandwidth costs and reports show some video meetings last several hours, you can limit the default meeting duration to help participants focus on shorter meetings. This does not apply to meetings scheduled from Microsoft Outlook.
Default Dialing Mode	Define how participants join a videoconference, based on your corporate culture: • Dial-out: The system automatically calls out to each participant on their dedicated endpoint or Scopia® Desktop Client. This option is best if most users just want to join in the quickest way possible, without having to look up the meeting information. • Dial-in: Each participant joins the videoconference from the meeting invitation link or by dialing the meeting ID. This option is best if most users prefer to control when they join the meeting, without any disruptions.

Field	Description
Termination	Define when the videoconference ends, according to the available resources in your organization: • At scheduled time: Select this option to end meetings automatically at the scheduled end time. Even if a meeting ends early, the resources are reserved for this meeting until the end time. Select the number of minutes before the meeting ends, to send an alert to the meeting moderator/organizer. • After all participants left the meeting: Enter the number of minutes after participants left to end the meeting. If a meeting ends early, the resources can be used for other videoconferences.
Maximum Recurring Meetings Duration	Define the maximum number of occurrences a user can schedule for recurring meetings. This can be useful to keep more time slots open for future meetings, and prevent users from cluttering the meeting slots by scheduling meetings very far in advance.
Launch Meetings [] Minute(s) Before Scheduled Time	Define when participants can join the meeting, if they try to join before the scheduled time. If there are many meetings scheduled for adjacent time slots, this can help manage resources by preventing users from starting meetings before the designated time. If the virtual room is already being used for another meeting, users cannot join until that meeting ends.
Waiting Room Timeout	You can define a time by which, if the host does not enter the waiting room, the meeting automatically ends. This frees up resources used by a meeting that is not taking place.
Meeting Auto Extend Length	Define the number of minutes to automatically extend a videoconference if participants are still connected.
Maximum Length of Meeting Extension	Define the maximum time that a videoconference can be automatically extended beyond its original end time.
Delete Meetings Older than	Define when to delete meetings from the list in the Meeting tab. This is useful when monitoring bandwidth and other statistics from past meetings (see Monitoring Meetings and Calls on page 213). You can modify this value depending on whether you want a more comprehensive list, or you are tracking only the most recent meetings.

4. Define settings for instant meetings, which are initiated spontaneously by users without reserving MCU and other video network resources:

Instant Meetings

Maximum Participants

☒ Allow endpoint initiated Point to Point calls

☒ Allow endpoint initiated multipoint calls

☐ Allow only endpoint initiated Virtual Room meetings

Default duration of instant meetings Minutes

Termination Policy: instant meetings are terminated when all participants have left the meeting

Figure 168: Defining policies for instant meetings

Table 58: Defining policies for instant meetings

Field	Description
Maximum Participants	Define the maximum number of participants that can be invited to a meeting initiated spontaneously. When meeting organizers reach the limit, they receive an error message when trying to invite additional participants. This is useful to manage resources, since larger meetings must be scheduled in advance.
Allow endpoint initiated Point to Point calls	Allow dedicated video endpoints to initiate direct calls to another endpoint, without routing it via an MCU. Disable this option to allow only calls that go through the MCU. For example, you may want to disable this field to conserve bandwidth, using it only for meetings with more than two participants.
Allow endpoint initiated multipoint calls	Allow dedicated video endpoints to start a meeting with multiple endpoints. Disable this option to make sure that all meetings with more than two participants are scheduled.
Allow only endpoint initiated Virtual Room meetings	Allow dedicated video endpoints to initiate meetings with multiple endpoints from a virtual room only, allowing you to maintain stricter control over how videoconferences are started. Endpoints cannot dial other endpoints or the MCU to start a meeting. You may want to disable this field, for example, to allow users without a virtual room to start meetings.
Default duration of instant meetings	Enter the default meeting duration for all instant meetings. Participants are notified when this time is reached, and if there are enough resources, meetings are auto-extended until all participants disconnect. For example, if you see from the meeting reports that most meetings last longer than 30 minutes, you can increase the default end time.

5. Select **Apply**.

Maintaining Scheduled Meetings

This section explains how to maintain scheduled meetings.

Navigation

- [Searching for a Meeting](#) on page 259
- [Modifying Upcoming Meetings](#) on page 260

Searching for a Meeting

About this task

You can search for a specific meeting, to monitor or terminate the meeting. You can also access meeting information by selecting the meeting name link.

Procedure

1. Log in to the Scopia® Management administrator portal.
2. Select the **Meetings** tab.
The list of all ongoing meetings is displayed in the window.
3. Select the **Now (Live)** tab in the sidebar menu to narrow the meeting search to current multipoint or point-to-point videoconferences, as required.
4. Select the **Past** or **Future** tabs to search for past or upcoming meetings, respectively.
5. Perform any of the following:
 - Enter the partial or complete name of the meeting in the search field.
If any part of the meeting name matches the search string, the meeting record is displayed in the search results.
 - Select the  icon to set up any of the advanced search fields described in this table:

Table 59: Searching for a meeting

Field Name	Description
Name	Enter the partial or complete name of the meeting in the field.
Meeting ID	Enter the partial or complete meeting ID in the field. If any part of the meeting ID matches the search string, the meeting record is displayed in the search results.

Field Name	Description
E.164	Enter the E.164 number of an attending endpoint in the field. If any part of the E.164 number matches the search string, the meeting record is displayed in the search results.
Type	Search in one of these meeting lists: – All the meetings – Multipoint meetings – Point-to-point calls
From	Select the calendar icon in the From field, and select a date and time in the window that opens. Meetings scheduled after the selected time are listed.
To	Select the calendar icon in the To field, and select a date and time in the window that opens. Meetings scheduled before the selected time are listed.

Modifying Upcoming Meetings

About this task

You can reschedule upcoming meetings to another time, change meeting parameters or delete the meeting request through the user portal. See the *User Guide for SCOPIA Management* for more information.

You can access the user portal from the administrator web interface by selecting the Avaya logo.

You can also delete an upcoming meeting from the administrator web interface as described in this procedure.

Procedure

1. Log in to the Scopia® Management administrator portal.
2. Select the **Meetings** tab in the sidebar menu.
3. Display the list of future meetings by selecting one of these tabs under the **Future** tab in the sidebar menu:
 - **All** lists future meetings.
 - **Tomorrow** displays meetings scheduled for the following day.
 - **Next Week** lists meetings scheduled for the upcoming week.

4. Select the meeting you want to delete. To delete all the meetings in the current view, select the list heading.
 5. Select **Delete**.
 6. At the prompt, select **Yes**.
The participants receive a meeting cancelled email.
-

Retrieving the Customer Support Package

About this task

The customer support package is a zipped file of bundled logs and configuration files which you can download and send to Customer Support for debugging. You can retrieve the package for these products:

- Scopia® Video Gateway
- Avaya Scopia® SIP Gateway
- Avaya Scopia® TIP Gateway
- Avaya Scopia® XT Series
- MCU products, except Scopia® MCU
- Avaya Scopia® PathFinder server

Procedure

1. Access the Scopia® Management administrator portal.
2. Select the **Devices** tab.
3. On the right pane, select the type of the device. For example, MCUs or Scopia® Desktop servers.

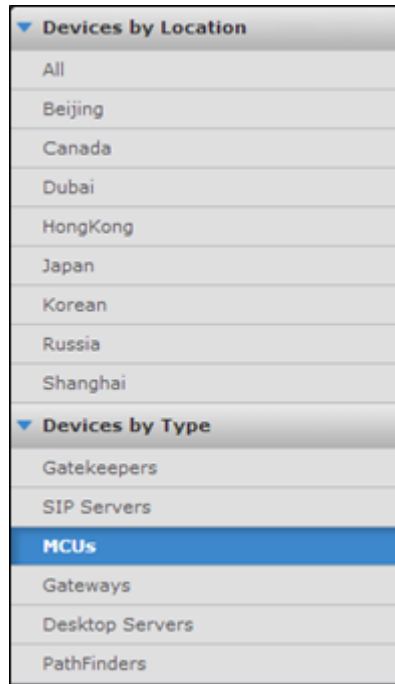


Figure 169: Selecting the type of device

4. Select the device for which you want to retrieve the customer support package.
5. Select **Manage > Retrieve Customer Support Package**.
6. At the prompt select **Yes**.
7. At the prompt select the link to download the file.
8. Select **Save** to download the file to your PC.

The file has the format **<product name_CS_Package_<product name IP Address>_<date and time of download>.zip**.

Uninstalling Avaya Scopia® Management

About this task

Uninstalling Scopia® Management has been made simple with an uninstall utility, which can be accessed in the **Start** menu in the same folder as the application itself.

Procedure

1. Select **Start > All Programs > Scopia® Management**.
2. Launch **Uninstall Scopia® Management**.

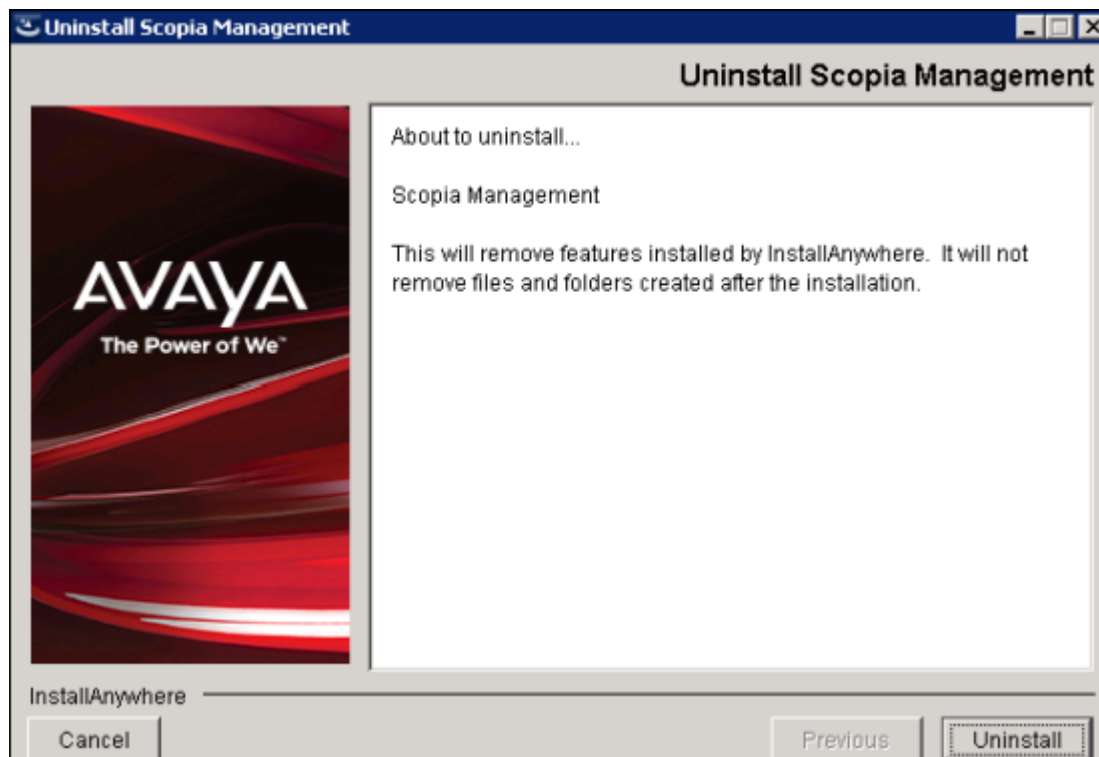


Figure 170: The Scopia® Management Uninstall Utility

3. Select **Uninstall**.

Chapter 9 | Tracking System Usage with Reports

The reports in Scopia® Management provide information about your video network, including the frequency of videoconferences and device usage. Reports are an essential part of managing and administering your video network, and can be used to reassess bandwidth policies, decide which endpoints should always use the highest bandwidth (even in poor network conditions), or even decide whether you should switch to a distributed deployment topology.

After viewing and analyzing the report results, there are many possible follow up actions you may want to take. We list a few examples in the report descriptions below:

- **Calls (Multipoint or Point-to-Point):** Shows the total number or duration of videoconferences, for either meetings with more than two endpoints (**Multipoint**) or calls between two endpoints (**Point-to-Point**).

Use this to track trends of videoconference usage, such as identifying the most popular time of day for calls (peak usage time), the average meeting duration, or average number of participants per meeting.

You can respond by, for example, implementing maximum bandwidth ceilings at different times or different days of the week. You may even decide to use off-site MCUs at specific times of day to help with the load.

- **Device Usage:** Shows the total number or length of calls for one or more devices, or the average capacity usage of a server. For maximum capacity, see the **Usage Peak** report.

Use this to track trends of device usage, such as the number of calls hosted by the most active MCUs, the number of calls an endpoint participated in, or the peak and average capacity reached by the Scopia® Desktop server.

After viewing the report results, you may want to (for example):

- Decrease the bandwidth of endpoints that are frequently used for very long durations.
- Change your topology to allocate resources differently among various locations.

For example, if you see that an MCU is consistently close to reaching its full capacity, you may want to deploy more MCUs or implement cascading to share the load with other MCUs. If cascading is already enabled, you can reserve additional resources for cascading MCUs (see [Increasing MCU Capacity by Cascading Multiple MCUs](#) on page 69).

- **Meeting Statistics:** Use this to track meeting trends and which meeting features are most used. For example, you can see how often various meeting types were used and how many meetings were cascaded.

The reports include a detailed breakdown of the way people in your organization are participating in videoconferences:

- Number of total meetings, with a breakdown of how many were scheduled or instant meetings (initiated spontaneously)
- Number of meetings that were cascaded among multiple MCUs
- Number of meetings that used the Auto-Attendant (IVR) function
- Total meeting duration for all meetings combined
- Maximum and average duration of meetings
- Maximum and average number of calls (participant connections) within one meeting

You can use meeting reports to show the impact of introducing videoconferencing on your organization and how often employees use its services.

- **General:** Shows how many times each meeting type (MCU service) was used, and the breakdown between scheduled and instant meetings.

If you see that most meetings were instant and not scheduled, you may want to provide users with more information about how and why to schedule meetings (to make sure that the required resources are available for the meeting).

If there is a frequently used meeting type that you did not already synchronize across all MCUs, you may want to do so to provide more resources for this meeting type (see [Synchronizing MCU Meeting Types with Scopia® Management](#) on page 63).

- **Virtual Rooms:** Shows the number of meetings and total time spent in calls for one or more virtual rooms, and is used to track the activity of virtual rooms.

If, for example, you see that many users are using virtual rooms extensively, you may want to roll out virtual room ownership to more users in your organization. This may require deploying additional Scopia® Desktop servers.

- **Meeting Size:** Use this to track the range of meeting sizes across the organization.

Based on the report results, you may want to:

- If you see that there are only small meetings, you can promote video in your organization. If you see that there are many large meetings, you can use this report to show how implementing videoconferencing saved money on transportation costs.
- Limit the number of maximum participants for instant meetings (see [Defining Video Usage Defaults](#) on page 254). This requires users to reserve resources for larger meetings by scheduling it beforehand.

- **Meeting Duration:** Shows the length of meetings across the organization.

Based on this analysis, for example, if you see that most meetings last longer than 30 minutes, you can increase the default end time for both scheduled and instant meetings (see [Defining Video Usage Defaults](#) on page 254). Or, for example, if management decides to cut on bandwidth costs and reports show some video meetings last several hours, you can limit the default meeting duration to help participants focus on shorter meetings.

- **System:** Shows the maximum capacity reached per device (**Usage Peak** report), or the average/peak bandwidth used by video network devices, internally and cross-location (**Bandwidth Used** report). To see a device's average usage, see the **Device Usage** report.

For example, you can view the an MCU's peak capacity over a specific time period, or track the bandwidth used for each location.

You can use this analysis to reevaluate whether your current topology is suited for your organization. For example, if you see that an MCU is consistently reaching capacity, you may want to add another MCU. If you see that a location is consistently reaching its bandwidth, you may want to adjust your bandwidth policies or upgrade the bandwidth for this location.

[Figure 171: Report data](#) on page 266 shows a few examples of generated reports. Depending on the report, the data is displayed as either a bar graph or a pie chart.

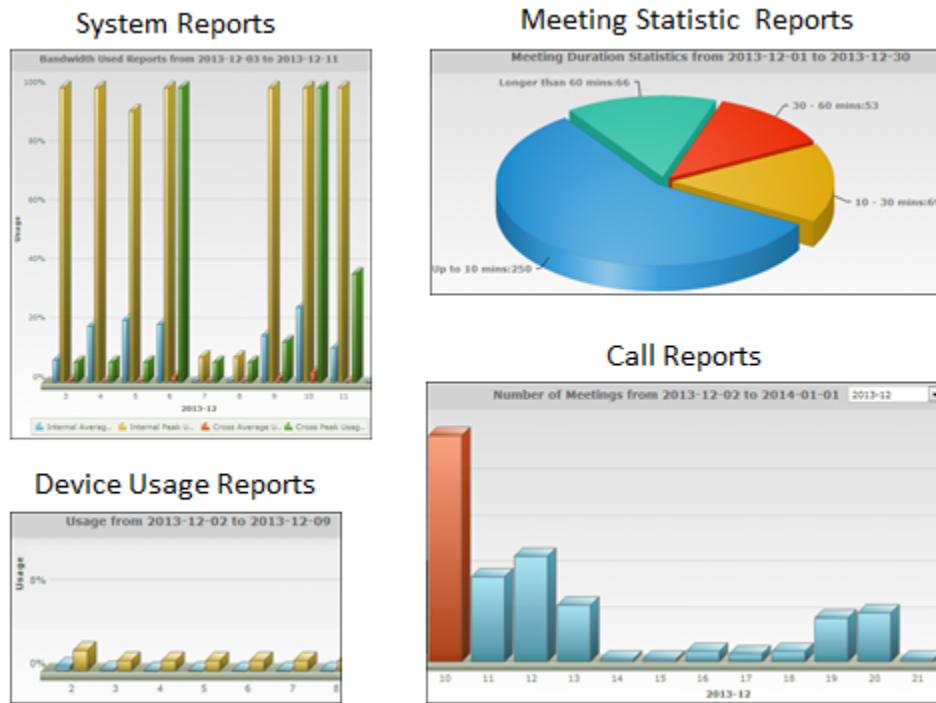


Figure 171: Report data

To generate a report, follow the instructions described in [Generating a Report](#) on page 266.

Generating a Report

About this task

This procedure describes how to generate Scopia® Management reports based on various criteria. For example, you can generate a report to see the call duration of all meetings that included a specific endpoint within a time period. For an explanation of all reports, see [Tracking System Usage with Reports](#) on page 264.

Procedure

1. Access the Scopia® Management administrator portal.
The **Dashboard** tab is displayed.
2. You can access the **Bandwidth Used** and **Usage Peak** reports directly from the dashboard. Select the links as shown and continue with step [5](#) to enter the required information for the report.

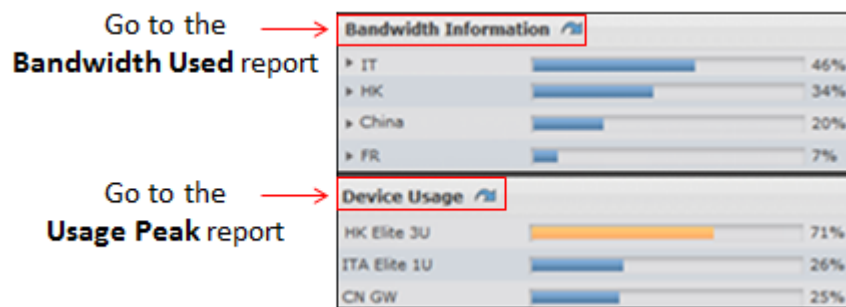


Figure 172: Accessing reports from the Dashboard

- To access all other reports, select the **Reports** tab.
- Select the report type in the sidebar menu. For an explanation of all reports, see [Tracking System Usage with Reports](#) on page 264.

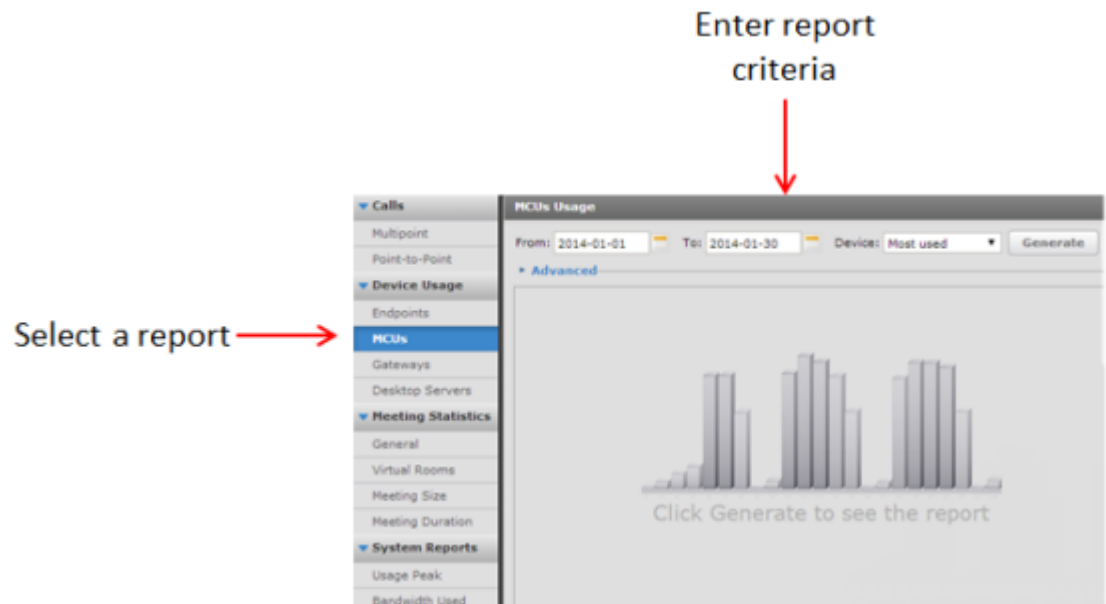


Figure 173: Selecting the report type

- Enter the required criteria in the fields above the report area (see [Table 60: Setting basic report criteria](#) on page 268).

Figure 174: Setting basic report criteria

Not all the fields are visible for every type of report.

Table 60: Setting basic report criteria

Field Name	Description	Reports
From	Select a start date for the report.	All
To	Select an end date for the report.	All
Endpoint/Device	Select the devices to be included in your report: • Most Used to include only the most active endpoints/MCUs in the report. • Least Used to include only the least active endpoints/MCUs in the report. • Select and choose up to five endpoints or a specific MCU for which you want to generate the report. The most and least used devices can refer to either the number of calls, call duration, or percentage of total capacity used (MCUs only). You can define this by selecting Advanced (see step 6).	Device Usage reports for: • Endpoints • MCUs
Device	Select All or the specific device for which to generate the report.	Device Usage reports for: • Gateways • Scopia® Desktop servers
Virtual Room	Select up to five virtual rooms for which you want to generate the report, and select OK .	Virtual Rooms report
Device Type	Select All or specify the type of video network device (MCU, gateway, or Scopia® Desktop server) for which to generate the report.	Usage Peak report
Locations	This field is only relevant for deployments with multiple locations. Select All or choose a specific location from the list.	Bandwidth Used report

6. (Optional) Select **Advanced** to narrow the focus of your report by entering additional criteria. For example, you can view the data for a specific location only, or by day of the week.

The screenshot shows a report generation interface. At the top, there are date pickers for 'From' (2013-12-02) and 'To' (2014-01-01), followed by a 'Generate' button. Below this is a section titled 'Advanced' which is highlighted with a red box. Under the 'Advanced' section, there are three dropdown menus: 'Show:' set to 'Number of Meeting', 'Display by:' set to 'Time of the Day', and 'Locations:' set to 'All'.

Figure 175: Setting advanced report criteria (example)

The advanced criteria varies according to the report you are generating, and is available only for **Calls**, **Device Usage**, and **Virtual Room** reports.

Table 61: Setting advanced report criteria

Field Name	Description
Show	Select the information to display in the report, as follows: • Number of Calls: Shows the number of active endpoint connections in calls. For multipoint meetings, this refers to the number of endpoints connected to the MCU. Each point-to-point call includes only one connection between two endpoints, and is counted as one call. • Number of Meetings: Shows the number of meetings matching the report criteria (only available for Multipoint reports). • Call Duration (Mins): Shows the total call duration, in minutes, matching the report criteria. • Usage: Shows the percentage of total connections used by the device (available for MCUs, gateways, and Scopia® Desktop servers). The options available depend on the report selected.
Display by	Select how to display the data: by date, time of day, day of week or month, or month of the year. For example, you can see which hours the highest number of meetings are held by selecting Time of the day.
Locations	This field is only relevant for deployments with multiple locations. Select All or choose a specific location from the list.

7. Select **Generate**.

Reports are displayed in either graph or chart format, depending on the report.

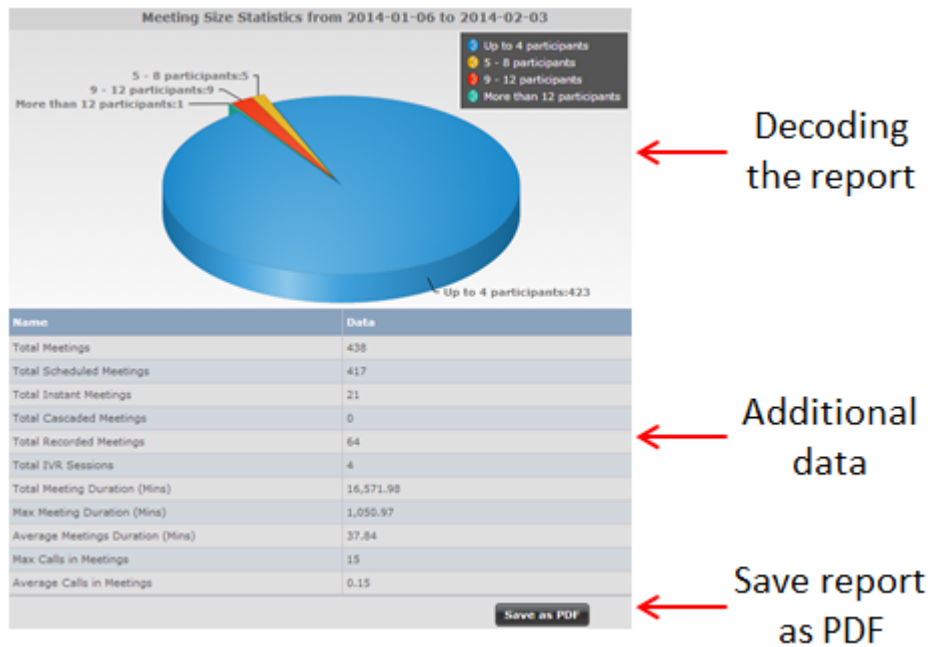


Figure 176: Example of a generated report

- You can view additional information below the graph or chart, such as the number of scheduled meetings, for **Meeting Statistic** reports ([Figure 176: Example of a generated report](#) on page 270).
- For **Call** and **Device Usage** (based on most and least used) bar graphs, the red bars indicate the top 20% of data values, the yellow indicates the middle 20-50%, and the blue bars indicate the bottom 50% (as shown in [Figure 177: Bar graph values](#) on page 271). For example, if you generated a report showing the number of meetings for a specific time period, as below, the red bar is used for the dates which had the highest number of meetings.

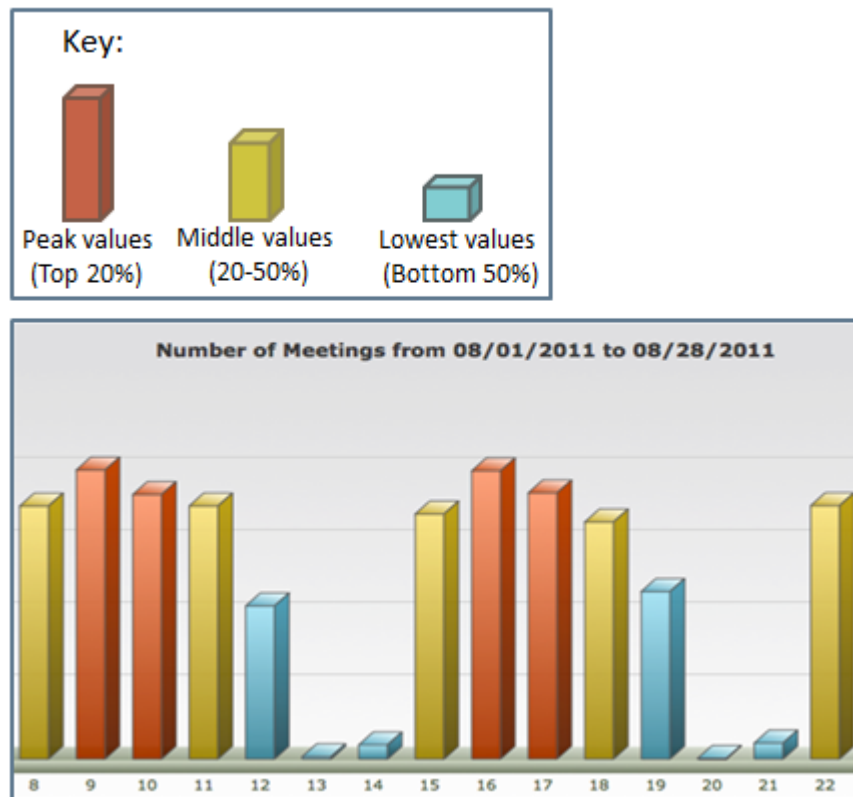


Figure 177: Bar graph values

- **Usage Peak, Bandwidth Used, and Device Usage** (for all or a specific device) bar graphs have their own color scheme, shown directly below the graph:

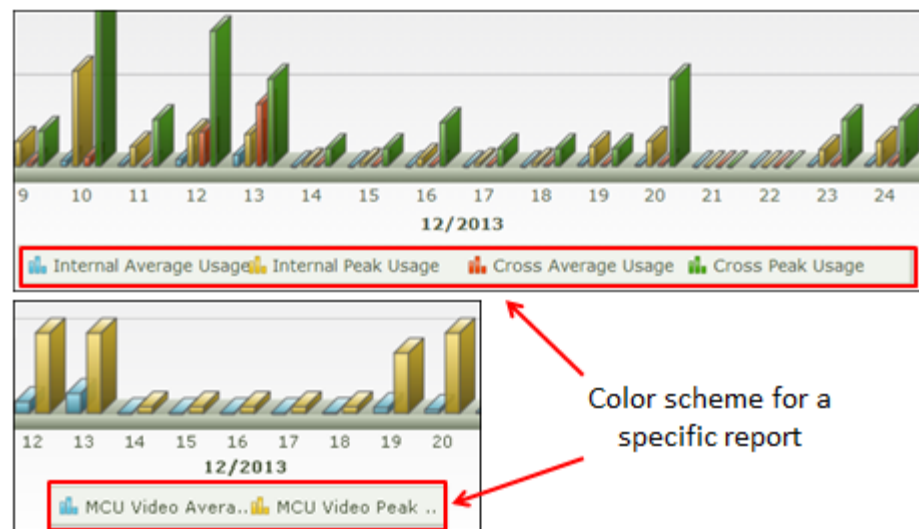


Figure 178: A report's color scheme

- For **Device Usage** reports:
If the MCU and Endpoint report is based on most or least used devices, the report displays the average value. For **MCU** reports based on all or a specific MCU, the report displays both the average and peak values.

Scopia® Desktop server and Gateway **Device Usage** reports display both the average and peak values.

8. (Optional) Select **Save as PDF** to export your report to PDF ([Figure 176: Example of a generated report](#) on page 270).

Or

For further analysis of meeting data, you can save export it as a CSV file and view the details in Microsoft Excel. Select **Advanced > Export Raw Data (CSV)** from the sidebar menu, enter the required information (see [Table 62: Exporting report data to a CSV file](#) on page 272) and select **Generate**.

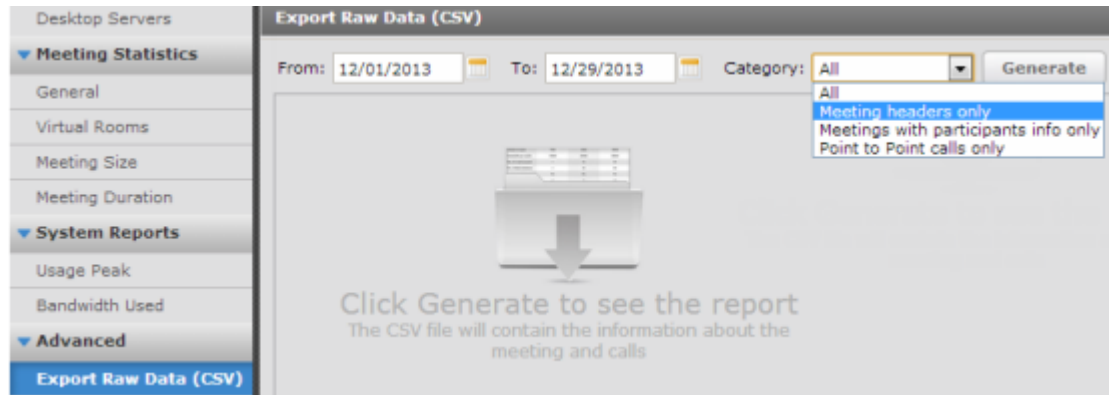


Figure 179: Exporting report data to a CSV file

Table 62: Exporting report data to a CSV file

Field	Description
From	Select a start date for the report.
To	Select an end date for the report.
Category	Select whether to generate data for meetings, calls, or both: • Meeting headers only: Includes the following details regarding multipoint meetings: the meeting ID and name (subject), duration and start time, the bandwidth used, the hosting MCU, and the location. • Meetings with participants info only: Includes all the information for multipoint meetings listed in Meeting headers only, as well as information about each participant (identified as the party name) in the meeting. For meetings that include Scopia® Desktop Clients, the Scopia® Desktop server is counted as a connection and therefore listed as a participant. • Point to Point calls only: Includes the following details for calls between two participants only: the name and number of each participant, the duration and start time, the bandwidth consumed, and the location of the initiating endpoint. • All: Includes the Meetings with participants info only and Point to Point calls only reports, as two separate Microsoft Excel files.

Select **Download Now** to save the **.zip** file containing the CSV files.
