A MITEL
PRODUCT
GUIDE

Unify OpenScape Media Server

Unify OpenScape Media Server V9

Administrator Documentation

08/2024

A31003-S2490-M102-19-76A9

Mitel

Contents

1 History of Changes

Date	Changes	Reason
2015-12-29	OSMS Version 9- initiated	-
2016-02-08	UPDATED: How to Edit a Web Collaboration Connection Point	UCBE-2608
2016-02-08	UPDATED: - How to Configure the OpenScape Web Collaboration Provider	UCBE-2930
2016-06-16	UPDATED: - Real-Time Transport Protocol (RTP / RTCP) - How to Add an RTP Streaming Route	UCBE-6845
2016-10-24	Introduction of Video Codec H.265 UPDATED: - OpenScape Media Server Features under OpenScape UC Application - Performance Evaluation Specific to the Processor - Video Calculation Example – CINT2006 Rate at OpenScape UC Application - Basic Configuration of the OpenScape Media Server under OpenScape UC Application - How to Define Terminal-Specific Codec Settings - SDP - Editing a Codec - Editing an RTP Data Stream	CMS-549
2017-03-07	Adapting Java version in chapter 9.4.20 TLS Certificate of the OpenScape Media Serverand sub-chapters (instead of ibm-java-i386-60 the ibm-java-<version> will be written)	review
2017-10-04	Updated: - Chapter 14.2.10.1 Deploying an Application	UCBE-13395
2017-10-10	Updated: - Chapter: 2.2.1 OpenScape Media Server Features under OpenScape UC Application - Chapter 2.4.4 Performance Evaluation Specific to the Processor - Chapter 2.4.4.2 Video Calculation Example – CINT2006 Rate at OpenScape UC Application	UCBE-11731 DOCLOC-22

Date	Changes	Reason
2018-04-03	Updated: - Chapter 2.6 Requirements for the OpenScape Media Server in a virtualized Environment	UCBE-12303
2018-08-14	Updated - Chapter 14.2.7 OpenScape Web Collaboration Provider	CMS-2610
2019-03-27	Added: - Chapter 9.2.22 How to Configure parameter reuseLocalAddressEnabled for all cnf-Circuits Updated: - Chapter 9.2.12 How to Configure an Internet Radio Station for providing Music-on-Hold	CMS-3044 UCBE-19335 UCBE-19336
2019-05-22	Added: - Chapter 9.2.23 Adjusting the volume level of an Internet Radio Station Stream Updated: - Chapter 9.2.12 How to Configure an Internet Radio Station for providing Music-on-Hold	UCBE-19805

2 About this Document

This section informs you about the document on hand.

2.1 Who should read this Document?

This document addresses administrators who configure and manage the **OpenScape Media Server**.

Readers should have the following knowledge for making full use of the information provided in this document:

- Knowledge of the communications systems' general working methods.
- Knowledge of terms used in the communications systems' environment.
- Practical experience with configuring and managing communications systems.

2.2 Structure of this Document

This document describes the general structure and operation as well as the features of the OpenScape Media Servers. Furthermore, it includes all associated reference information.

This document is divided into the following chapters:

Chapter 1 – About this Document

This chapter contains general information about this document. From here you can navigate to the pages to follow, thus finding the desired information quickly.

Chapter 2 – OpenScape Media Server Overview

Here you find a short overview of the features and the general structure of the **OpenScape Media Server**.

Chapter 3 – OpenScape Media Server Architecture

This chapter describes the basic services of the **OpenScape Media Server**.

Chapter 4 – OpenScape Media Server Applications

This chapter describes the **OpenScape Media Server** applications, in particular the voice and conference portal.

Chapter 5 – OpenScape Media Server Standards

In this chapter we explain standard technologies that the **OpenScape Media Server** uses.

Chapter 6 – Technological Concepts of the OpenScape Media Server

In this chapter we deal with individual technological concepts that the **OpenScape Media Server** uses.

Chapter 7 – Installing, Upgrading and Uninstalling the OpenScape Media Server

This chapter contains information about setting up, upgrading and uninstalling the **OpenScape Media Server**.

Chapter 8 – OpenScape Media Server Basic Configuration

This chapter describes how to configure the **OpenScape Media Server** basically for various application scenarios. After this basic configuration the **OpenScape Media Server** is ready for operation in the respective application scenario.

Chapter 9 – OpenScape Media Server Administration

This chapter describes continuative, administrative tasks that may follow the basic configuration of the **OpenScape Media Server**. This enables customizing the **OpenScape Media Server**.

Chapter 10 – OpenScape Media Server Monitoring

Here we describe in detail which central operating parameters of the **OpenScape Media Server** can be monitored.

Chapter 11 – OpenScape Media Server Logging

This chapter contains detailed information about logging the **OpenScape Media Server**.

Chapter 12 – Raw Statistics Data of the OpenScape Media Server

This chapter contains information about the raw statistics interface of the **OpenScape Media Server**.

Chapter 13 – OpenScape Media Server Error Management

This chapter describes the error messages that the **OpenScape Media Server** issues when an error occurs in a Media Server component.

Chapter 14 – Reference to the OpenScape Media Server

This chapter contains all reference information about the **OpenScape Media Server**.

2.3 Icons used

In this document we use the following markings to draw your attention to selected contents.

IMPORTANT:

This indicates notes that carry information of high priority. You definitely need to act according to such information to rule out malfunctions, damage to devices or possible loss of data.

NOTICE:

This indicates notes that point to information worth knowing or recommendations.

2.4 Markups used

In this document we use the following markups to highlight selected text passages:

Element	Markup
GUI elements	Click on **Save** to …
Sequence of menu entries	**Users& Resources** > **Resources**
Command line output	`C:> unknown command`
System input	Enter `true` in field ...
Directory and file names	`/var/config.xml`
File contents	`conname=%CONNECTION_NAME%`
Names of keyboard keys	Press `ESC` to …
Specifications with variable content	<user name >

2.5 Acronyms used

In this document we use the following acronyms:

Acronym	Meaning
ANAT	Alternative Network Address Types
ASR	Automatic Speech Recognition
BHCA	Busy Hour Call Attempts
CAD	Calling Number
CALEA	Communications Assistance for Law Enforcement Act
CLI	Command Line Interface
CTI	Computer Telephony Integration
CMP	Common Management Platform
CSR	Certificate Sign Request
DNS	Domain Name System
DSCP	Differentiated Services Codepoints
DTMF	Dual Tone Multiple Frequency
GNF	Global Number Format
GUI	Graphical User Interface

Acronym	Meaning
HTML	Hypertext Markup Language
ICE	Interactive Connectivity Establishment
JDK	Java Development Kit
JMX	Java Management Extensions
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LI	Lawful Intercept
IVR	Interactive Voice Response
LAN	Local Area Network
MGCP	Media Gateway Control Protocol
MLPP	Multi-level Precedence and Preemption
MRCP	Media Resource Control Protocol
MS	Media Server
MWI	Message Waiting Indicator
MYKEY	Multimedia Internet Keying
NAT	Network Address Translation
NTP	Network Time Protocol
PID	Permission ID
PKI	Public Key Infrastructure
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RAM	Random Access Memory
RFC	Request for Comment
RPM	RPM Packet Manager
RTCP	Real Time Transport Control Protocol
RTP	Real Time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol

Acronym	Meaning
SIP SM	SIP service manager
SOA	Service Oriented Architecture
SPEC	Standard Performance Evaluation Corporation
SQL	Structured Query Language
SRTP	Secure Realtime Transport Protocol
SRTCP	Secure Real Time Transport Control Protocol
TCP	Transmission Control Protocol
TK	Telecommunication
TLS	Transport Layer Security Protocol
TTM	Trusted Transfer Mode
TTS	Text-to-Speech
TUI	Telephony User Interface
UA	User Agent
UDP	User Datagram Protocol
UMS	Unified Messaging System
URI	Uniform Resource Identifier
VLAN	Virtual Local Area Network
W3C	World Wide Web Consortium
WPAD	Web Proxy Autodiscovery Protocol
XML	Extensible Markup Language
XPR	OpenScape Xpressions

2.6 Continuative Documents

You find further information about OpenScape UCApplication in the following documentation:

- *OpenScape UCApplication, System Description*
- *OpenScape UCApplication, Planning Guide*
- *OpenScape UCApplication, Installation and Upgrade, Installation Manual*
- *OpenScape UCApplication, Configuration and Administration, Administrator Documentation*

You find further information about OpenScape Voice in the following document among other things:

- *OpenScape Voice, Administrator Documentation*

You find further information about Common Management Platform in the following document among other things:

- *Common Management Platform, Administrator Documentation*

You find further information about the Application Builder in the following Document:

- *OpenScape UCApplication Application Builder, Administrator Documentation*

You find further information about the Common Management Platform in the following Document:

- *OpenScape CMP, Configuration and Administration, Administrator Documentation*

3 OpenScape Media Server Overview

The OpenScape Media Server can be shortly described as Apache Tomcat web server for voice and video applications. It does not use special hardware and is based exclusively on software, of which the main interfaces use Java technology.

You can use the OpenScape Media Server in the following environments:

- As Media Server farm at OpenScape Voice
- As Media Server under OpenScape UCApplicationOpenScape UCApplication
- In parallel operation at OpenScape Voice and OpenScape UCApplication

3.1 OpenScape Media Server at OpenScape Voice

You can use the OpenScape Media Server as integrated Media Server at OpenScape Voice.

In this role it serves in particular the purpose of creating tones and announcements used by OpenScape Voice and playing them via the relevant terminal devices. To this, the OpenScape Media Server is controlled by OpenScape Voice via the Media Gateway Control Protocol (MGCP).

Possible scenarios for generating and playing tones and announcements are:

- Intercepting exceptional conditions by OpenScape Voice – e. g. when a dialed phone number does not exist.
- Acoustic user guidance for system commands to control OpenScape Voice – e. g. call forwarding activation for a terminal device.

You can use the OpenScape Media Server in all OpenScape Voice operating modes released for OpenScape Voice.

If the performance data of a single OpenScape Media Server do not comply with the desired performance or redundancy requirements, you can also connect a Media Server farm with several parallel OpenScape Media Servers to an OpenScape Voice system. In doing so you need to install the same Media Server components on all computer systems of the OpenScape Media Server.

The OpenScape Voice system distributes in this case the load among the various OpenScape Media Servers.

3.1.1 OpenScape Media Server Features at OpenScape Voice

If the OpenScape Media Server is used as integrated Media Server at OpenScape Voice, it provides correspondingly adjusted features.

Network Environment

- Scaling Media Server services by using several OpenScape Media Server in a Media Server farm
- Supporting IPv4 and IPv6 network addresses
- Simultaneously supporting IPv4 and IPv6 network addresses by:
  - Alternative Network Address Types (ANAT)
  - Interactive Connectivity Establishment (ICE, ICE-lite, ICE-microlite)

- Supporting VLAN environments
- Simultaneously connecting several OpenScape Voice systems

Media

- Audio playback and recording
- Audio formats for sending and receiving via RTP
  - G.711 µ-Law / A-Law (8 KHz / 8 Bit, mono)
  - G.722 (16 KHz, mono)
  - G.722.1(Siren 7 and Siren 14/G.722.1)[1]
  - G.722.1 Annex C[2]
  - G.729 (8 KHz, mono)
- Audio formats before internal RTP formating [3]

Container format	Audio data format
WAV	– PCM (16 Bit LE, 8…48 kHz, mono / stereo) – G.711 µ-Law / A-Law (8 Bit LE, 8…48 kHz, mono / stereo)
MKV	– PCM (16 Bit LE, 8…48 kHz, mono / stereo) – MP3 (8…48 kHz, mono / stereo)
<without container>	– MP3 (8…48 kHz, mono / stereo)

- Audio formats for recording of incoming RTP streams

Container format	Audio data format
WAV	– PCM (16 Bit LE, mono) – G.711 µ-Law / A-Law (8 Bit LE, mono)
MKV	– PCM (16 Bit LE, mono)

- Converting codecs (transcoding)
- Mixing media streams with automatic gain control
- Creating DTMF and connection tones as well as dynamic announcements
- Playing DTMF and connection tones as well as announcements
- Supporting internet radio stations for music on hold
- DTMF recognition (RTP-inband, RFC 2833, SIP-INFO)
- Managing audio conferences of OpenScape Voice controlled by terminal devices (large conferencing)

1 Royalty free offered by Polycom

2 Royalty free offered by Polycom

3 In these formats you can upload audio files to the OpenScape Media Server.

- Tones for the following countries and announcements in the corresponding national language:

– Argentina	– Norway
– Brazil	– Poland
– Bulgaria	– Portugal
– China	– Romania
– Denmark	– Russia
– Germany	– Sweden
– Estonia	– Serbia
– Finland	– Slovakia
– France	– Slovenia
– Greece	– Spain
– Great Britain	– Spain (Catalan)
– Italy	– Czech Republic
– Canada	– Turkey
– Croatia	– Hungary
– Latvia	– USA
– Mexico	– United Arab Emirates
– Netherlands	

- In addition, tones for the following countries:

– Australia	– Malaysia
– Belgium	– Morocco
– Bosnia and Herzegovina	– Austria
– Chile	– Peru
– Ecuador	– Philippines
– Hong Kong	– Singapore
– India	– South Africa
– Indonesia	– Taiwan
– Japan	– Thailand
– Colombia	– Venezuela
– Korea	– Vietnam
– Lithuania	

- Additional announcements for the Multi Level Precedence and Preemption (MLPP) service

Security

- Encrypted transmission of RTP data by SRTP
- Encrypted transmission of RTCP data by SRTCP
- Negotiating keys based on:
  - Session Description Protocol Security (SDES)
  - Multimedia Internet Keying (MIKEY)
- Supporting the Media Server redundancy concepts of OpenScape Voice

Quality of Service (QoS)

- Supporting RTP Quality of Services by Differentiated Services Codepoints (DSCP)
- Individually configuring RTP Quality of Service for every network connection

Management and Monitoring

- Managing and monitoring the OpenScape Media Server integrated in the Common Management Platform
- Managing OpenScape Voice announcements individually
- Consistency check of important configuration parameters
- Assigning operation-critical system resources to individual media applications
- Supporting the Simple Network Management Protocol (SNMP) v2c
- Checking the RTP communication by RTCP
- Monitoring telecommunication according to CALEA / LI
- JMX-based statistics for MGCP and streaming connections
- Providing raw statistics data for further processing as required

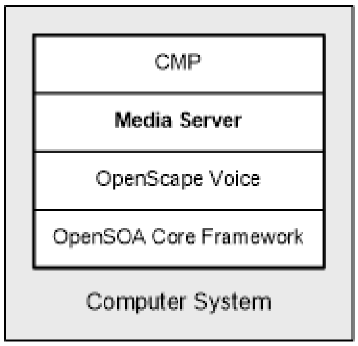
3.1.2 Operating Modes of the OpenScape Media Server at OpenScape Voice

If you use the OpenScape Media Server as integrated Media Server at OpenScape Voice, you can operate it in different ways.

- As internal OpenScape Media Server
- As external OpenScape Media Server

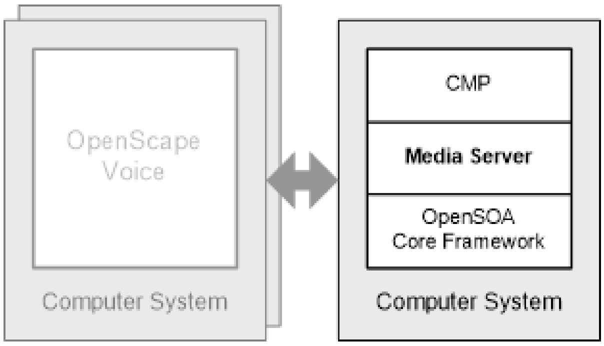
Internal OpenScape Media Server

In this operating mode the OpenScape Media Server is installed on the computer system that also hosts OpenScape Voice and the Common Management Platform.



External OpenScape Media Server

In this operating mode the OpenScape Media Server is not installed on the OpenScape Voice computer system. Instead, you find it on an individual computer platform together with the Common Management Platform.



3.1.3 License Management of the OpenScape Media Server at OpenScape Voice

You do not need any individual Media Server licenses for operating the OpenScape Media Server at OpenScape Voice.

3.1.4 The OpenScape Media Server Environment at OpenScape Voice

The OpenScape Media Server is based on the OpenSOA Core framework. This framework provides the OpenScape Media Server with basic structures of which the following interfaces are used. Furthermore, the OpenScape Media Server uses various default protocol interfaces for connecting external systems.

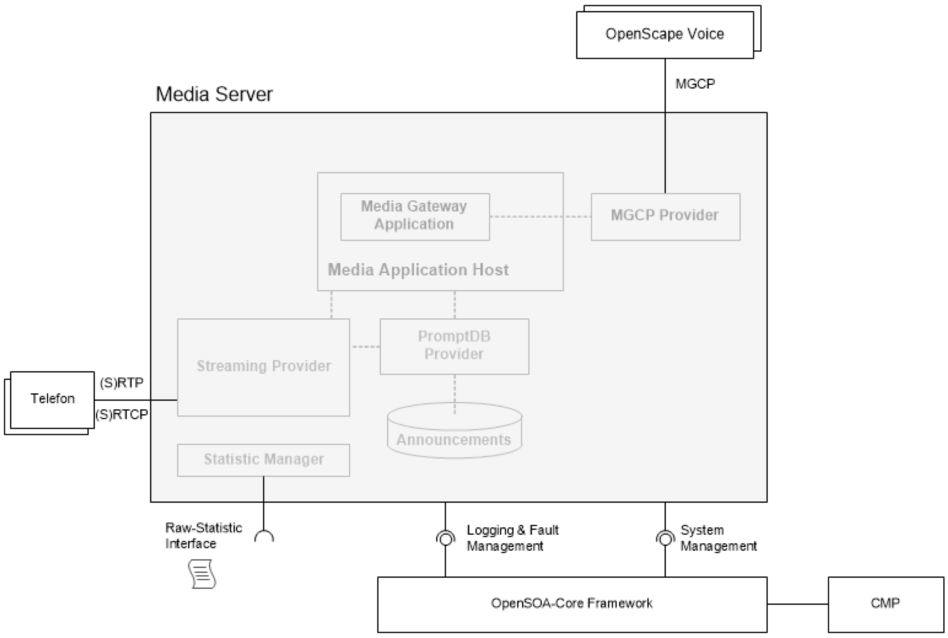
The OpenScape Media Server uses the following internal interfaces of the OpenSOA Core Framework:

- Logging and error management
- System Management

Beyond that, the OpenScape Media Server uses at OpenScape Voice the following default protocol interfaces for connecting external systems:

- MGCP
- RTP / SRTP
- RTCP / SRTCP

The raw statistics interface provides raw data, which you can further process using external statistics applications.



MGCP

Enables the communication between the OpenScape Media Server and OpenScape Voice.

Via this protocol OpenScape Voice controls the OpenScape Media Server features. The MGCP communication is interpreted by the OpenScape Media Server in the function of a media gateway.

RTP / SPRTP

Enables the communication between the OpenScape Media Server and RTP-compatible telephones.

The actual media and DTMF streams, sent and received by the OpenScape Media Server, are routed via this connection

If RTP information has to be transmitted encrypted, the OpenScape Media Server uses SRTP in connection with MIKEY or SDES.

RTCP / SRTCP

Enables optional checking tasks in the scope of an RTP communication. Such tasks include:

- continuously monitoring the service quality – e. g. in the form of lost data packages
- distributing information about subscribers involved in the communication.

SRTCP is offered by the terminal device and automatically activated in the OpenScape Media Server if required.

3.1.5 Ports used at OpenScape Voice

The OpenScape Media Server uses different protocol ports at OpenScape Voice. Such ports need to be released in a firewall possibly used.

NOTICE:

The following table describes the default settings of the OpenScape Media Server and of OpenScape Voice. Changing these default settings results in other requirements concerning port unblockings in a firewall possibly used.

Table 1: Ports used in the OpenScape Media Server (OpenScape Voice)

Protocol	Port number	Transport protocol	Communication direction	
			from	to
MGCP	2427 [4] (bidirectional)	UDP	OpenScape Voice	OpenScape Media Server
	2727 [5]	UDP	OpenScape Media Server	OpenScape Voice
RTP / RTCP	m to m + [2 × n – 1] [6] (bidirectional on Media Server side)	UDP	OpenScape Media Server	RTP terminal device
			RTP terminal device	OpenScape Media Server

3.2 OpenScape Media Server under OpenScape UCApplication

You can use the OpenScape Media Server as integrated Media Server for OpenScape UCApplication.

In this role it serves in particular the following purposes:

- Executing integrated media applications– e. g. the conference portal
- Processing complex media streams

You can use the OpenScape Media Server under OpenScape UCApplication in all UC Application deployment scenarios released for OpenScape UCApplication.

If the performance levels of a single OpenScape Media Server do not comply with the desired performance or redundancy requirements, you can connect a Media Server farm with several parallel OpenScape Media Servers under

4 Default setting in the OpenScape Media Server; is configurable in the OpenScape Media Server.

5 Default setting in the OpenScape Voice; is configurable in OpenScape Voice.

6 Individual for each RTP streaming route: m corresponds to the value for the streaming route setting **RTP / RTCP port range**. Default setting: 20 000. n corresponds to the value for the streaming route setting **Number of RTP ports**. Default setting: 2 500.

OpenScape UCApplication. In doing so you need to install the same Media Server components on all computer systems of the OpenScape Media Server.

The OpenScape Voice system distributes in this case the load among the various OpenScape Media Servers.

3.2.1 OpenScape Media Server Features under OpenScape UCApplication

If the OpenScape Media Server is used as integrated Media Server under OpenScape UCApplication, it provides correspondingly adjusted features.

Network Environment

- Scaling Media Server services by using several OpenScape Media Server in a Media Server farm
- Supporting IPv4 and IPv6 network addresses
- Simultaneously supporting IPv4 and IPv6 network addresses by:
  - Alternative Network Address Types (ANAT)
  - Interactive Connectivity Establishment (ICE-lite, ICE-microlite)
- Supporting VLAN environments
- Simultaneously connecting several SIP servers
- Configuring alternative SIP servers for every connected SIP server
- Supporting a supplied TTS / ASR system

> **NOTICE:**
>
> The OpenScape Media Server has only been released with the TTS / ASR engine by Nuance. It must always be present on the OpenScape Media Server computer system.

Media

- Audio playback and recording
- Video playback
- Audio formats for sending and receiving via RTP
  - G.711 µ-Law / A-Law (8 KHz / 8 Bit, mono)
  - G.722 (16 KHz, mono)
  - G.722.1(Siren 7 and Siren 14/G.722.1)[7]
  - G.722.1 Annex C[8]
  - G.729 (8 KHz, mono)
- Video formats for sending and receiving via RTP
  - H.264 (AVC / MPEG-4 - Part 10)
  - H.265 (AVC/MPEG-4 - Part 10)

7 Royalty free offered by Polycom

8 Royalty free offered by Polycom

- Audio formats before internal RTP formating [9]

Container format	Audio data format
WAV	– PCM (16 Bit LE, 8…48 kHz, mono / stereo) – G.711 µ-Law / A-Law (8 Bit LE, 8…48 kHz, mono / stereo)
MKV	– PCM (16 Bit LE, 8…48 kHz, mono / stereo) – AAC (8…48 kHz, mono / stereo) – MP3 (8…48 kHz, mono / stereo)
MP4	– AAC (8…48 kHz, mono / stereo)
<without container>	– AAC (8…48 kHz, mono / stereo) – MP3 (8…48 kHz, mono / stereo)

- Video formats before internal RTP formating [10]
  - H.264 (AVC / MPEG-4 – Part 10)
  - H.265 (AVC/MPEG-4 – Part 10)
- Audio formats for recording of incoming RTP streams

Container format	Audio data format
WAV	– PCM (16 Bit LE, mono) – G.711 µ-Law / A-Law (8 Bit LE, mono)
MKV	– PCM (16 Bit LE, mono)

- Prioritizing codecs per media type used
- Converting codecs (transcoding)
- Video solutions supported by default for outbound connections with a frame rate up to 30 images per second:
  - CIF (352 × 288 Pixel)
  - Full HD (1920 × 1080 Pixel)
  - HD720p (1280 × 720 Pixel)
  - HD1080p (1920 x 1080 Pixel)
  - QVGA (320 × 240 Pixel)
  - VGA (640 × 480 Pixel)
- Video solutions supported by default for inbound connections with any frame rate:
  - 4CIF (704 × 576 Pixel)
  - CIF (352 × 288 Pixel)
  - Full HD (1920 × 1080 Pixel)
  - HD720p (1280 × 720 Pixel)
  - HD1080p (1920 x 1080 Pixel)
  - QCIF (176 × 144 Pixel)
  - QVGA (320 × 240 Pixel)
  - VGA (640 × 480 Pixel)

9 In these formats you can upload audio files to the OpenScape Media Server.

10 In these formats you can upload video files to the OpenScape Media Server.

- Mixing media streams with automatic gain control
- DTMF recognition (RTP-inband, RFC 2833, SIP-INFO)

Security

- Encrypted transmission of RTP data by SRTP

> **NOTICE:**
>
> Encrypted connections involving OpenScape UCApplication are not displayed to users in their client / phone as secure connection.

- Encrypted transmission of RTCP data by SRTCP
- Encrypted transmission of SIP signaling by TLS
- Negotiating keys based on:
  - Session Description Protocol Security (SDES)
  - Multimedia Internet Keying (MIKEY)
- Supporting the Media Server redundancy concepts of OpenScape UCApplication

Quality of Service (QoS)

- Supporting RTP Quality of Services by Differentiated Services Codepoints (DSCP)
- Individually configuring RTP Quality of Service for every network connection
- Individually configuring RTP Quality of Service for every media type

Application support

- Integrated runtime environment for java-based media applications
- Executing the conference portal application of OpenScape UCApplication
- Executing the voice portal applications of OpenScape UCApplication
- Executing customer-specific Application Builder applications
- Executing the integrated VoiceXML browser

Management and Monitoring

- Managing and monitoring the OpenScape Media Server integrated in the Common Management Platform
- Managing the media applications integrated in the OpenScape Media Server management
- Managing announcements for the media applications of the OpenScape Media Server individually
- Consistency check of important configuration parameters
- Assigning operation-critical system resources to individual media applications
- Replicating selected system resources automatically
- Supporting the Simple Network Management Protocol (SNMP) v2c
- Checking the RTP communication by RTCP
- Option for controlling the mailbox LED on telephones (MWI) for OpenScape Voice
- JMX-based statistics for SIP and streaming connections
- Providing raw statistics data for further processing as required

3.2.2 Operating Modes of the OpenScape Media Server under OpenScape UCApplication

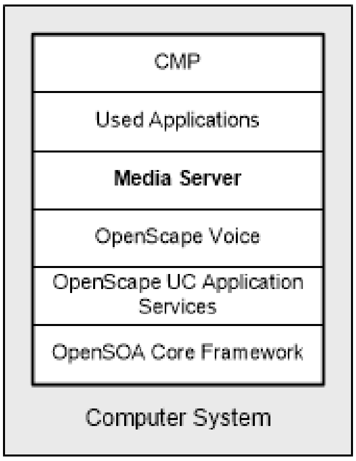
If you use the OpenScape Media Server as integrated Media Server under OpenScape UCApplication, you can operate it in different ways.

- In the operating mode Integrated Deployment of OpenScape UCApplication
- In the operating mode Integrated Deployment of OpenScape UCApplication with External Media Server for Video Conferences
- In the operating mode Small Deployment of OpenScape UCApplication
- In the operating modes Large / Very Large Deployment of OpenScape UCApplication

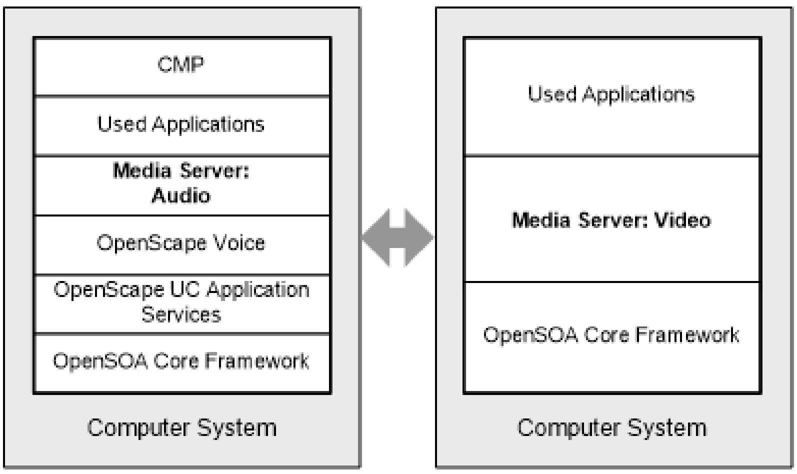
Integrated Deployment

Integrated Deployment with External Media Server

In this operating mode the OpenScape Media Server is installed on a computer system that also hosts OpenScape Voice and the other components of OpenScape UCApplication.

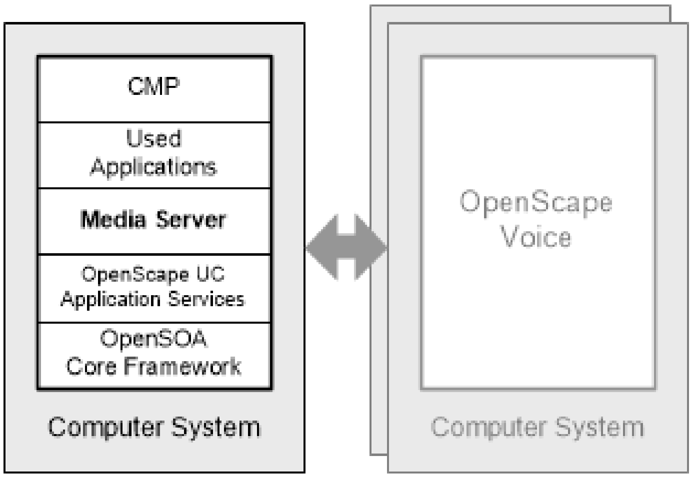


In this operating mode the OpenScape Media Server is installed on a computer system that also hosts OpenScape Voice and the other components of OpenScape UCApplication. Video streaming for video conferences is supported by an external media server.



Small Deployment

In this operating mode the OpenScape Media Server is not installed on the OpenScape Voice computer system. Instead, you find it on an individual computer platform in combination with the other UC Application components and its used applications.



Large / Very Large Deployment

In these operating modes the OpenScape Media Server is found on an individual computer platform, independent from the other UC Application components and from OpenScape Voice.

3.2.3 License Management of the OpenScape Media Server under OpenScape UCApplication

You do not need any individual Media Server licenses for the general OpenScape Media Server operation under OpenScape UCApplication. However, if you wish to use the TTS or ASR features of the OpenScape Media Server, you need to have a corresponding number of port-based TTS or ASR licenses. You find details about this in the planning guide for OpenScape UCApplication.

Using individual OpenScape UCApplication features may require further individual UC Application licenses – this concerns e. g. video conferences. You find detailed license information about this in the OpenScape UCApplication planning guide also.

3.2.4 The OpenScape Media Server Environment at OpenScape UCApplication

The OpenScape Media Server is based on the OpenSOA Core framework. This framework provides the OpenScape Media Server with basic structures of which the following interfaces are used. Furthermore, the OpenScape Media Server uses various default protocol interfaces for connecting external systems.

The OpenScape Media Server uses the following internal interfaces of the OpenSOA Core Framework:

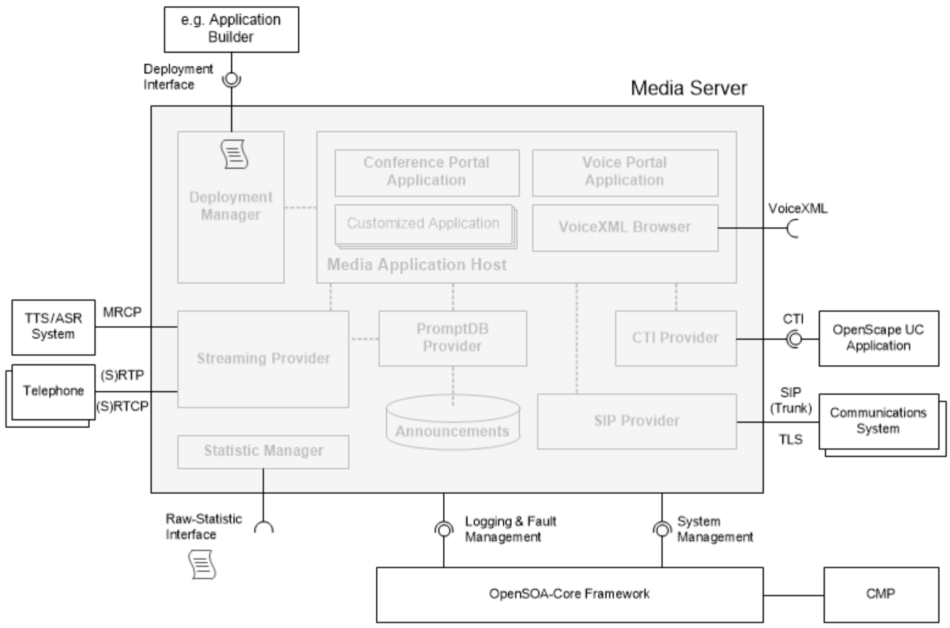
- Logging and error management
- System Management

Beyond that, the OpenScape Media Server uses under OpenScape UCApplication the following default protocol interfaces for connecting external systems:

- CTI
- RTP / SRTP
- RTCP
- SIP
- MRCP
- VoiceXML

The additional deployment interface enables adding applications or updating existing ones in the OpenScape Media Server at runtime.

The raw statistics interface provides raw data, which you can further process using external statistics applications.



CTI

Using CTI commands, external systems can monitor and control OpenScape Media Server system resources via the CTI interface.

External systems can thus execute the following tasks, for example:

- Controlling the setup up and closing of phone connections in the OpenScape Media Server.
- Monitoring existing phone connections of the OpenScape Media Server.

MRCP

Enables the OpenScape Media Server communication with the TTS / ASR system used by the conference and voice portal and that must be installed on the OpenScape Media Server computer system.

RTP / SRTP

Enables the communication between the OpenScape Media Server and RTP-compatible telephones.

The actual media and DTMF streams, sent and received by the OpenScape Media Server, are routed via this connection

If RTP information has to be transmitted encrypted, the OpenScape Media Server uses SRTP in connection with MIKEY or SDES.

RTCP / SRTCP

Enables optional checking tasks in the scope of an RTP communication. Such tasks include:

- continuously monitoring the service quality – e. g. in the form of lost data packages
- distributing information about subscribers involved in the communication.

SRTCP is offered by the terminal device and automatically activated in the OpenScape Media Server if required.

SIP

Enables the SIP-based OpenScape Media Server communication with the communications system used – e. g. with OpenScape Voice. An SIP trunk must always be used for the SIP communication between the OpenScape Media Server and the communications system.

If SIP information has to be transmitted encrypted, the OpenScape Media Server uses TLS.

VoiceXML

The VoiceXML lets the OpenScape Media Server exchange voice data in the standardized VoiceXML format with external systems.

3.2.5 Ports used under OpenScape UCApplication

The OpenScape Media Server uses different protocol ports under OpenScape UCApplication. Which ports are concerned is described in the manual

OpenScape UCApplication, Installation and Upgrade. Such ports need to be released in a firewall possibly used.

3.3 OpenScape Media Server in Parallel Operation

You can use the OpenScape Media Server also simultaneously as Media Server at OpenScape Voice and under OpenScape UCApplication.

3.4 Hardware Recommendations for the OpenScape Media Server

You can use the OpenScape Media Server basically with any hardware that uses intel-compatible x64 CPUs. All other hardware requirements depend on the desired performance and the system environment in which you use the OpenScape Media Server.

In the following we specify the recommended minimum performance value according to the Standard Performance Evaluation Corporation (SPEC) [11] – more precisely in CINT2006 rate or CINT2006 speed – for the external environment of the OpenScape Media Server and Small, Large and Very Large Deployment.

CINT2006 rate / speed according to the Standard Performance Evaluation Corporation

The CINT2006 rate and CINT2006 speed enable a relatively objective performance comparison between different computer processors. From this value you may approximate the individual BHCA and channel performance of the OpenScape Media Server if you use a computer processor that deviates from the recommended CINT2006 specification.

Example calculation with freely assumed values: A computer system performs up to 30 000 BHCA and 500 G.711 channels if it has a CINT2006 rate of 80. If, in contrast, you use a computer system with a CINT2006 rate of 120, the BHCA performance and number of channels increases proportionately to 45 000 respectively 750.

Difference between CINT2006 rate and CINT2006 speed

CINT2006 speed considers the performance of a processor on the basis of a single thread.

CINT2006 rate considers the performance of a processor on the basis of any number of threads. The various kernels of a processor can execute these threads in parallel, with the value for CINT2006 rate always being larger than the one for CINT2006 speed.

[11] http://www.spec.org/cpu2006/results/

3.4.1 How to Determine the CINT2006 Rate of a Computer System

You can determine the CINT2006 rate of a computer system via the internet page of the Standard Performance Evaluation Corporation.

Step by Step

1) Enter the following address in your web browser:

   `http://www.spec.org/cgi-bin/osgresults?conf=cpu2006`

   You see the search page for the CPU2006 results.
2) Select the entry **Processor** in the combo box under **Simple Request**.
3) Specify under **Matches** the name of the computer processor mounted in the relevant computer system.

   Example: `x5650`
4) Select **Execute Simple Fetch** to start the search.
5) Scroll towards the bottom of the hit list until you see section **CINT2006 Rate** and look there for the relevant producer and his computer system.

3.4.2 Hardware Recommendations for the OpenScape Media Server at OpenScape Voice

The hardware requirements on the OpenScape Media Server at OpenScape Voice depend on the desired performance requirements and the operating mode in which you use the OpenScape Media Server.

Depending on the operating mode used and the desired performance requirements, there are hardware recommendations for the OpenScape Media Server at OpenScape Voice for the following applications:

- Internal OpenScape Media Server
- External OpenScape Media Server – basic system
- External OpenScape Media Server – default system
- External OpenScape Media Server – high performance system

Internal OpenScape Media Server

(OpenScape Media Server, and OpenScape Voice share a computer system.)

The hardware is determined by OpenScape Voice.

Underlying MGCP-BHCA:	5 000 (every MGCP scenario uses the following MGCP messages: 1 × CRCX, 3 × MDCX, 2 × RQNT, 1 × DLCX)
Maximum permissible number of channels for announcements and conference participants:	
• G.711:	Max. 150 RTP or RTCP channels or
• G.729 / G.732.1:	Max. 50 RTP or RTCP channels or
• G.722:	Max. 75 RTP or RTCP channels or
• a combination of shares	

External OpenScape Media Server (basic system)

(OpenScape Media Server on an individual computer system.)

Hardware
• One 4-core CPU Intel Xeon E5620 or W3550 (CINT2006 rate[12] >= 110)
• 4 GB RAM DDR3 / 1066
• Two 73 GB [13] SAS harddisks in Raid-1 configuration with single partition
• One Gigabit LAN interface

Underlying MGCP-BHCA:	20 000 (every MGCP scenario uses the following MGCP messages: 1 × CRCX, 3 × MDCX, 2 × RQNT, 1 × DLCX)
Maximum permissible number of channels for announcements and conference participants:	
• G.711:	Max. 650 RTP or RTCP channels or
• G.729:	Max. 270 RTP or RTCP channels or
• G.722:	Max. 330 RTP or RTCP channels or
• a combination of shares	

NOTICE:

Assumption for the specified number of channels: The OpenScape Media Server can use up to 40 % of the processor performance on the computer system.

External OpenScape Media Server (default system)

(OpenScape Media Server on an individual computer system.)

Hardware
• Two 4-core CPUs Intel Xeon E5620 (CINT2006 rate[14] >= 220)
• 8 GB RAM DDR3 / 1066
• Two 73 GB [15] SAS harddisks in Raid-1 configuration with single partition
• One Gigabit LAN interface

12 performance evaluation according to the Standard Performance Evaluation Corporation (SPEC) – http://www.spec.org/cpu2006/results/

13 If the feature syncUC is to be used, we recommend two 300 GB SAS harddisks in Raid-1 configuration.

14 performance evaluation according to the Standard Performance Evaluation Corporation (SPEC) – http://www.spec.org/cpu2006/results/

15 If the feature syncUC is to be used, we recommend two 300 GB SAS harddisks in Raid-1 configuration.

Underlying MGCP-BHCA:	40 000 (every MGCP scenario uses the following MGCP messages: 1 × CRCX, 3 × MDCX, 2 × RQNT, 1 × DLCX)
Maximum permissible number of channels for announcements and conference participants:	
• G.711:	Max. 1 290 RTP or RTCP channels or
• G.729:	Max. 540 RTP or RTCP channels or
• G.722:	Max. 650 RTP or RTCP channels or
• a combination of shares	

NOTICE:

Assumption for the specified number of channels: The OpenScape Media Server can use up to 40 % of the processor performance on the computer system.

External OpenScape Media Server (high performance system)

(OpenScape Media Server on an individual computer system.)

Hardware

- Two 6-core CPUs Intel Xeon E5650 (CINT2006 rate[16] >= 340)
- 8 GB RAM DDR3 / 1066
- Two 73 GB [17] SAS harddisks in Raid-1 configuration with single partition
- One Gigabit LAN interface

Underlying MGCP-BHCA:	60 000 (every MGCP scenario uses the following MGCP messages: 1 × CRCX, 3 × MDCX, 2 × RQNT, 1 × DLCX)
Maximum permissible number of channels for announcements and conference participants:	
• G.711:	Max. 2 000 RTP or RTCP channels or
• G.729:	Max. 830 RTP or RTCP channels or
• G.722:	Max. 1 000 RTP or RTCP channels or
• a combination of shares	

NOTICE:

16 performance evaluation according to the Standard Performance Evaluation Corporation (SPEC) – http://www.spec.org/cpu2006/results/

17 If the feature syncUC is to be used, we recommend two 300 GB SAS harddisks in Raid-1 configuration.

Assumption for the specified number of channels: The OpenScape Media Server can use up to 40 % of the processor performance on the computer system.

3.4.3 Hardware Recommendations for the OpenScape Media Server under OpenScape UCApplication

Information about the minimal hardware requirements and the corresponding performance of the OpenScape Media Server under OpenScape UCApplication is described in the manual OpenScape UCApplication, Planning Guide.

3.4.4 Performance Evaluation Specific to the Processor

You can approximate the number of channels and busy-hour call attempts the OpenScape Media Server supports with a computer processor of individual CINT2006 rate. In doing so please consider the scenario in which the OpenScape Media Server is used and whether its communication is encrypted.

Formula for approximating the maximum number of channels

$$\mathrm{Channel} = \frac{(\mathrm{CPU} \times \mathrm{CINT}) - (\mathrm{kBHCA}_{\mathrm{SIP}} \times 50) - (\mathrm{kBHCA}_{\mathrm{MGCP}} \times 20{,}5)}{\mathrm{Encryption} \times \mathrm{Codec}}$$

Formula for approximating the minimum CINT2006 rate

$$\mathrm{CINT} = \frac{\mathrm{Channel} \times \mathrm{Encryption} \times \mathrm{Codec} + (\mathrm{kBHCA}_{\mathrm{SIP}} \times 50) + (\mathrm{kBHCA}_{\mathrm{MGCP}} \times 20{,}5)}{\mathrm{CPU}}$$

The formulas for approximating the performance use the following parameters.

• Channel	Number of simultaneously possible media channels.
• CINT	CINT2006 rate of the computer processor used.
• Codec	Factor the value of which depends on the codec used by the OpenScape Media Server. Possible values are: • Codec = 1 for G.711 • Codec = 2 for G.722 • Codec = 2,4 for G.729 • Codec = 180 for 720p video conferences (incl. H.264 / H.265 transcoding) • Codec = 350 for 1080p video conference (for H.264) • Codec = 700 for 1080p video conference (for H.265)

• CPU	Maximum processor load the OpenScape Media Server may create. This value is specified in percent. If the OpenScape Media Server is installed on an individual computer system, the estimated value must not exceed 40; if the OpenScape Media Server shares a computer system with other components alien to the Media Server, the value must not exceed 20.
• Encryption	Factor the value of which depends on whether or not the OpenScape Media Server communication is encrypted. Possible values are: • Encryption = 6,2 for unencrypted communication • Encryption = 7,7 for encrypted communication
• $kBHCA_{SIP}$	Number of simultaneously possible SIP busy-hour call attempts multiplied with factor 1000. In this context, every SIP connection signaling is assumed to consist of 7 – 10 SIP messages. Exchanging more or fewer SIP messages (e. g. additional SIP-REINVITES) may falsify the calculated performance value. This value is required when the OpenScape Media Server is used as Media Server under OpenScape UCApplication.
• $kBHCA_{MGCP}$	Number of simultaneously possible MGCP busy-hour call attempts multiplied with factor 1000. In this context we assume that each MGCP connection signaling consists of 5 MGCP messages (1 × CRCX, 1 × DLCX, 1 × MDCX + 2 × RQNT). Exchanging more or fewer MGCP messages may falsify the calculated performance value. This value is required when the OpenScape Media Server is used as Media Server under OpenScape Voice.

Use in a virtualized environment

You can use and install the OpenScape Media Server in a virtualized environment also. In this case there is no negative influence on the OpenScape Media Server performance in general.

However, when configuring the virtual machines, care must be taken that the OpenScape Media Server is assigned as many and efficient CPU and RAM resources as are described in the hardware recommendations of this documentation. For example, if only a smaller number of CPUs is assigned to the OpenScape Media Server, the OpenScape Media Server performance decreases accordingly.

3.4.4.1 Audio Calculation Example– Number of Channels at OpenScape UCApplication

How to calculate e. g. the number of channels of an OpenScape Media Server that exclusively operates under OpenScape UCApplication and communicates unencrypted.

Calculation demands:

- The CINT2006 rate for the processor of the available computer system is 350– CINT = 350
- The computer system shall exclusively be used for the OpenScape Media Server – CPU = 40
- The OpenScape Media Server shall use the G.722 codec– Codec = 2
- The OpenScape Media Server shall be used as Media Server under OpenScape UCApplication. This includes a planned maximum rate of 10 000 SIP calls per hour– $kBHCA_{SIP}$ = 10
- The OpenScape Media Server shall not be simultaneously used as Media Server at OpenScape Voice– $kBHCA_{MGCP}$ = 0
- The OpenScape Media Server shall communicate unencrypted– Encryption = 6,2

Step by Step

1) Equation for calculating the number of channels:

$$\mathrm{Channel} = \frac{(\mathrm{CPU} \times \mathrm{CINT}) - (\mathrm{kBHCA}_{\mathrm{SIP}} \times 50) - (\mathrm{kBHCA}_{\mathrm{MGCP}} \times 20{,}5)}{\mathrm{Encryption} \times \mathrm{Codec}}$$

2) Inserting the default values and calculation:

$$\mathrm{Channel} = \frac{(40 \times 350) - (10 \times 50) - (0 \times 20{,}5)}{6{,}2 \times 2} \sim 1088$$

An OpenScape Media Server that complies with the calculation demands supports approximately 1088 simultaneous channels.

3.4.4.2 Video Calculation Example– CINT2006 Rate at OpenScape UCApplication

How to calculate e. g. the CINT2006 rate for the processor of an OpenScape Media Server that exclusively operates under OpenScape UCApplication and communicates encrypted.

Calculation demands:

- The computer system shall exclusively be used for the OpenScape Media Server – CPU = 40
- The OpenScape Media Server shall support at least 25 simultaneous channels– Channel = 25
- The OpenScape Media Server shall use 720p video conferences (incl. H.264 /H.265 -transcoding)– Codec = 180
- The OpenScape Media Server shall use 1080p video conferences (incl. H.264-transcoding)– Codec = 350
- The OpenScape Media Server shall use 1080p video conferences (incl. H.265-transcoding)– Codec = 700
- The OpenScape Media Server shall be used as Media Server under OpenScape UCApplication. This includes a planned maximum rate of 1 000 SIP calls per hour– $kBHCA_{SIP}$ = 1
- The OpenScape Media Server shall not be simultaneously used as Media Server at OpenScape Voice– $kBHCA_{MGCP}$ = 0

- The OpenScape Media Server shall communicate encrypted– Encryption = 7,7

Step by Step

1) Equation for calculating the CINT2006 rate:

$$\text{CINT} = \frac{\text{Channel} \times \text{Encryption} \times \text{Codec} + (\text{kBHCA}_{\text{SIP}} \times 50) + (\text{kBHCA}_{\text{MGCP}} \times 20{,}5)}{\text{CPU}}$$

2) Inserting the default values and calculation:

$$\text{CINT} = \frac{25 \times 7{,}7 \times 180 + (1 \times 50) + (0 \times 20{,}5)}{40} \sim 867$$

An OpenScape Media Server that complies with the calculation demands must have a minimum CINT2006 rate of approximately 867.

3.4.4.3 Audio Calculation Example– CINT2006 Rate at OpenScape UCApplication and OpenScape Voice

How to calculate e. g. the CINT2006 rate for the processor of an OpenScape Media Server that operates simultaneously under OpenScape UCApplication and OpenScape Voice and communicates unencrypted.

Calculation demands:

- The computer system shall exclusively be used for the OpenScape Media Server – CPU = 40
- The OpenScape Media Server shall support at least 1 000 simultaneous channels– Channel = 1 000
- The OpenScape Media Server shall use the G.722 codec– Codec = 2
- The OpenScape Media Server shall be used as Media Server under OpenScape UCApplication. This includes a planned maximum rate of 7 000 SIP calls per hour– $\text{kBHCA}_{\text{SIP}}$ = 7
- The OpenScape Media Server shall be used as Media Server under OpenScape Voice. This includes a planned maximum rate of 5 000 MGCP requests per hour– $\text{kBHCA}_{\text{MGCP}}$ = 5
- The OpenScape Media Server shall communicate unencrypted– Encryption = 6,2

Step by Step

1) Equation for calculating the CINT2006 rate:

$$\text{CINT} = \frac{\text{Channel} \times \text{Encryption} \times \text{Codec} + (\text{kBHCA}_{\text{SIP}} \times 50) + (\text{kBHCA}_{\text{MGCP}} \times 20{,}5)}{\text{CPU}}$$

2) Inserting the default values and calculation:

$$\text{CINT} = \frac{1000 \times 6{,}2 \times 2 + (7 \times 50) + (5 \times 20{,}5)}{40} \sim 321$$

An OpenScape Media Server that complies with the calculation demands must have a minimum CINT2006 rate of approximately 321.

3.5 Operating System Requirements for the OpenScape Media Server

The OpenScape Media Server must exclusively be installed and operated on computer systems with selected operating system.

This is:

- SUSE Linux Enterprise Server 11 SP4 (64-bit version)
- SUSE Linux Enterprise Server 12 SP1 (64-bit version)
- SUSE Linux Enterprise Server 12 SP2 (64-bit version)

3.6 Requirements for the OpenScape Media Server in a virtualized Environment

You can use and install the OpenScape Media Server in a virtualized environment also. In this case there is no negative influence on the OpenScape Media Server performance in general. However, when configuring the virtual machines, care must be taken that the OpenScape Media Server is assigned as many and efficient CPU and RAM resources as are described in the hardware recommendations of this documentation. For example, if only a smaller number of CPUs is assigned to the OpenScape Media Server, the OpenScape Media Server performance decreases accordingly.

The following virtualization platforms have been released for the OpenScape Media Server:

- VMware ESXi V4.0 / V4.1

  (synonym: VMware vSphere Hypervisor V4.0 / V4.1)
- VMware ESXi V5 / V5.1

  (synonym: VMware vSphere Hypervisor V5 / V5.1)

Furthermore, the following requirements and restrictions apply for using a released virtualization platform:

- Use the following settings for the virtual machine of the OpenScape Media Server:
  - Option **Normal** for the **CPU shares** setting.
  - Option **Unlimited** for the **CPU reservation limit** setting.
  - Option **Normal** for the **RAM shares** setting.
  - Option **No** for the **Using manual MAC address** setting.
  - Option **Yes** for the **Support of the VMware Data Recovery** setting.
- Install the VMware tools.
- We generally recommend using the virtual network board type VMXNET3 of VMware ESXi. However, a bug in version 5 of VMware ESXi causes the loss of UDP packages. You can use the network board type E1000 as alternative, but this type has a poor data throughput. You find information about the current status of the abovementioned bug under the following link: http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&externalId=2019944&sliceId=1&docTypeID=DT_KB_1_

- The load of the virtualization platform CPUs must not exceed 75 %.
- When operating in test and demonstration systems you can save considerable amounts of hard disk space by enabling the **Allocate and commit space on demand (Thin provisioning)** option. This means that the virtual hard disk grows with the actually required hard disk space. This option is supported by a virtualized OpenScape Media Server, but we do not recommend it for productive systems, because it affects the system's performance negatively.
- In productive systems you may use snapshots only in the scope of system updates and upgrades.
- Use a single snapshot at the most for system updates and upgrades.
- Synchronize the OpenScape Media Server exclusively by means of an external NTP source.

IMPORTANT:

The VMware tools pre-settings effect a synchronization between host and virtualization platform. To avoid an instable double synchronization, the VMware tools synchronization must be disabled.

- No video conferences in full-HD format are supported.
- If OpenScape Media Server is used under OpenScape UCApplication, additional restrictions may exist. You find details about this in the manual *OpenScape UCApplication, Planning Guide*.

4 OpenScape Media Server Architecture

The OpenScape Media Server can be shortly described as Apache Tomcat web server for voice and video applications. In the OpenScape Media Server the direct equivalent to the Apache Tomcat web server is the Media Application Host. The OpenScape Media Server uses different media applets (applications) and a VoiceXML browser, which corresponds in an Apache Tomcat web server to the Servlets and the JSP engine.

The Media Application Host is the central OpenScape Media Server element. It forms the runtime environment for the applications and the logical components of the OpenScape Media Server.

4.1 Overview of the Logical Components of the OpenScape Media Server

The OpenScape Media Server services are based on different logical components. The Media Application Host forms the runtime environment for such components.

The essential logical components of the OpenScape Media Server at OpenScape Voice are:

- MGCP Application
- MGCP Provider
- PromtDB Provider
- Streaming Provider
- Statistics Manager

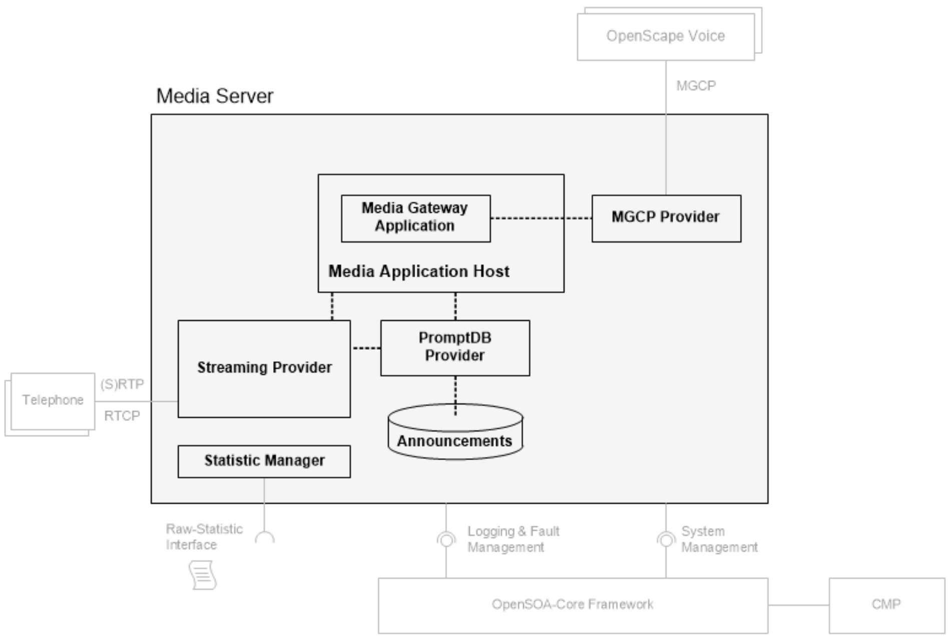


Figure 1: Essential logical Media Server components at OpenScape Voice

The essential logical components of the OpenScape Media Server under OpenScape UCApplication are:

- CTI Provider
- PromptDB Provider

- SIP Provider
- Streaming Provider
- Web Collaboration Provider
- VoiceXML Browser
- Deployment Manager
- Statistics Manager
- Applications

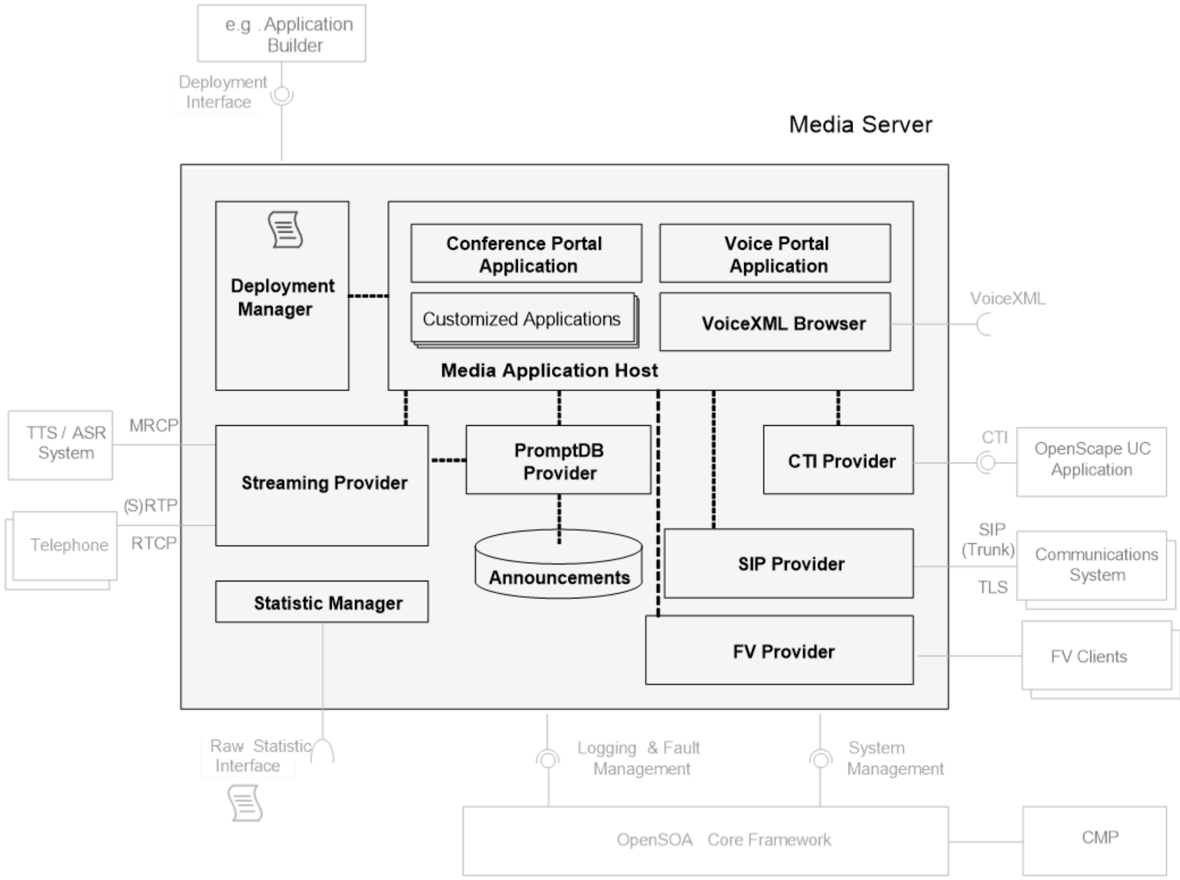


Figure 2: Essential logical Media Server components under OpenScape UCApplication

4.2 PromptDB Provider

The PromptDB provider is in charge of handling OpenScape Media Server announcements. To do this it realizes a management interface among other things, which can be accessed in the OpenScape Media Server configuration dialog.

The PromptDB provider serves in particular the following purposes:

- Managing announcements stored in the OpenScape Media Server. This includes the structured storage of available announcements.
- Enabling read and write access to filed announcements.
- Creating variable announcements – e. g. for playing the current time.

4.3 Streaming Provider

The Streaming provider manages and processes the payload of existing real-time connections processed by the OpenScape Media Server.

Within this scope it particularly enables:

- RTP communication with terminal devices for sound file playback.
- Recognition of DTMF tones sent to the OpenScape Media Server by terminal devices via RTP.
- Provision of codecs for encoding, decoding and codec-conversion of payload.
- The combination of different media streams.
- Encryption of RTP data if required (SRTP).

The Streaming provider uses the native auxiliary process nativeRTPunit for the RTP streaming. This maximizes the number and quality of the media streams processed by the OpenScape Media Server in real-time.

4.4 MGCP Provider

The MGCP provider provides an MGCP interface for the OpenScape Media Server. This interface corresponds to the standard RFC 2705 and is used by the OpenScape Voice for controlling the OpenScape Media Server.

The MGCP provider interprets the commands sent to the OpenScape Media Server via the MGCP interface and hands them over to the Media Gateway application for further processing.

4.5 CTI Provider

External systems can access the CTI provider for monitoring and controlling system resources of the OpenScape Media Server by CTI commands.

External systems can thus execute the following tasks, for example:

- Controlling the setup up and closing of phone connections in the OpenScape Media Server.
- Monitoring existing phone connections of the OpenScape Media Server.

If the OpenScape Media Server is used under OpenScape UCApplication, the BCom service of OpenScape UCApplication uses the CTI provider like the BCom service uses e. g. the CTI link of OpenScape Voice.

4.6 SIP Provider

The OpenScape Media Server uses the SIP provider for controlling SIP-based communications connections.

4.7 OpenScape Web Collaboration Provider

The OpenScape Web Collaboration provider provides services that users can deploy to display the screen contents of their computer to other participants and release these contents for editing.

In Web Collaboration conferences you can thus do the following:

- Performing presentations using a computer.
- Editing documents on the computer of a conference participant with other users.
- Using additional Web Collaboration tools – e. g. a whiteboard for creating simple scetches or the chat feature.

NOTICE:

You cannot use the OpenScape Web Collaboration provider of the OpenScape Media Server in the scope of OpenScape UCApplication V7 as replacement for the external web conferencing system OpenScape Web Collaboration.

4.8 Internet Radio Streaming Provider

Instead of audio files used for OpenScape Voice by default you can also deploy music from Internet radio stations to serve as music-on-hold. The Internet Radio Streaming Provider automatically establishes the connection to desired Internet radio stations and makes the relevant Internet radio streams available to the MGCP provider for playback.

Various internal data buffers of the OpenScape Media Server see to the Internet radio streams being played without disruptions in normal practice. This buffer concept also prevents the Internet radio streams from being played on different devices synchronously.

Generally, Internet radio stations will interrupt existing connections regularly at individual times. In this case, the Internet Radio Streaming Provider reboots the connections concerned automatically at night.

If music from an Internet radio station not started has to be played to a user, the Internet Radio Streaming Provider boots the relevant connection at the time of the playback start. In this case, no music-on-hold will be audible in the first seconds.

Providing every configured Internet radio station allocates approximately 100 kbit/s of bandwidth on the recipient side of the OpenScape Media Server. This value is independent from the number of subscribers to whom music from an Internet radio station is played.

The Internet Radio Streaming Provider supports Internet radio stations with the following specifications:

- MP3-coded
- PLS and M3U playback lists
- Content type(s) HTTP, audio/mpeg, audio/x-mpegurl
- The Internet radio stream is broadcasted on port 80

IMPORTANT:

Playing back music is generally subject to copyrights. Make sure that you are authorized to play the selected music using the Internet Radio Streaming Provider.

NOTICE:

Owing to individual, technical restrictions, playing back music from Internet radio stations may fail even if they comply with the listed specifications.

As a test, you can open a station's URL for example in the VLC Media Player. If the VLC Media Player does not play the Internet radio station, it cannot be used as an Internet radio station in the OpenScape Media Server either.

4.9 VoiceXML-Browser

The VoiceXML-Browser is a user interface of the OpenScape Media Server that can be used by customer-specific applications.

After a user has started a connection to the VoiceXML-Browser, the browser loads and interprets an application-specific VoiceXML document. This VoiceXML document is the starting point of a voice application. In the course of such a voice application the VoiceXML-Browser may load further VoiceXML documents.

Central element of the VoiceXML-Browser is the VoiceXML-Interpreter. It interprets the content of VoiceXML documents loaded into the VoiceXML-Browser.

4.10 Deployment Manager

When importing an application to the OpenScape Media Server, the respective deployment file of the application is copied to the deployment directory of the OpenScape Media Server. This deployment file may have been created using the Application Builder, for example. The deployment manager of the OpenScape Media Server monitors the deployment directory and unpacks each newly imported deployment file into the working directory of the OpenScape Media Server. This way, the Deployment Manager assigns an individual version number to the data in order to avoid conflicts with other existing versions.

If an imported application uses individual announcements, for example, the Deployment Manager loads them together with the application code into the OpenScape Media Server. This happens while the OpenScape Media Server is active and does not require a restart of the Media Server.

4.11 Statistics Manager

The statistics manager of the OpenScape Media Server collects statistics information of the single Media Server components and puts it out in the form of raw statistics via the raw statistics interface.

Statistics applications can access it there to prepare it for customers.

4.12 Applications

The OpenScape Media Server can execute applications to provide users with extended media services. These applications are executed in the Media Application Host of the OpenScape Media Server and configured via the OpenScape Media Server settings if required.

The following default applications can be installed with the OpenScape Media Server:

- At OpenScape Voice:
  – Media gateway
- Under OpenScape UCApplication:
  – Conference portal
  – Voice portal (DTMF-controlled)
  – Voice portal "Speech" (voice-controlled)
  – AutoAttendant

If you use the OpenScape Media Server under OpenScape UCApplication, you can import further individual applications in the OpenScape Media Server - for example applications created with the Application Builder of OpenScape UCApplication.

5 Applications

The OpenScape Media Server can execute applications to provide users with extended media services. These applications are executed in the Media Application Host of the OpenScape Media Server and configured via the OpenScape Media Server settings if required.

The following default applications can be installed with the OpenScape Media Server:

- At OpenScape Voice:
  - Media gateway
- Under OpenScape UCApplication:
  - Conference portal
  - Voice portal (DTMF-controlled)
  - Voice portal "Speech" (voice-controlled)
  - AutoAttendant

If you use the OpenScape Media Server under OpenScape UCApplication, you can import further individual applications in the OpenScape Media Server - for example applications created with the Application Builder of OpenScape UCApplication.

5.1 Media Gateway Application

If you use the OpenScape Media Server at OpenScape Voice, the Media Gateway application is automatically installed with the OpenScape Media Server setup.

This application processes commands sent by OpenScape Voice to the OpenScape Media Server via the MGCP interface. The Media Gateway application uses the following internal services for this purpose:

- Station-controlled conferencing (cnf)

  Processes commands that effect the participant-controlled conferences of OpenScape Voice.
- Announcements (ann)

  Processes commands that effect the playback of OpenScape Voice announcements.
- CALEA / LI (es)

  Processes commands that effect monitoring OpenScape Voice connections.

5.2 Conference Portal Application

If you use the OpenScape Media Server under OpenScape UCApplication, the conference portal is automatically installed with the OpenScape Media Server setup. With the conference portal the OpenScape Media Server provides conference rooms in which users can gather and hold audio conferences. Users may deploy any telephone or softphone as terminal device.

The conferences can be scheduled and controlled via a telephone user interface (TUI) of the OpenScape Media Server or via an associated conference client application.

The conference portal of the OpenScape Media Server supports the following conference types:

- Ad-hoc
- Meet Me
- MeetNow!

Both conference types comprise audio and video conferences.

5.2.1 Meet Me Conference

A Meet Me conference is scheduled and configured in advance. Before the conference begins, an OpenScape user creates an access ID and PIN that he/she distributes among the desired conference participants. When the conference participants enter this ID and PIN after logging on to the conference portal, they are routed to the relevant conference room. There they hear music or an announcement or see a video until the moderator activates the conference.

Conference participants can also be dialed via the conference portal and thus directly enter the conference room.

5.2.2 Ad-hoc Conference

An Ad-hoc conference is initiated by a user spontaneously. To this, he/she selects the desired conference participants and immediately initiates a conference. The conference portal calls the desired conference participants to join this conference.

If the desired conference participants cannot be reached when the conference begins, they can later log on to the conference portal by themselves and enter the conference room via an access ID and PIN.

5.2.3 MeetNow! Conference

To join a MeetNow! conference, participants dial into the conference portal spontaneously. All conference participants share an access PIN they have previously agreed on to book into the conference room.

NOTICE:

The nature of this conference type does not allow the conference portal to manage the assignment of access PINs for MeetNow! conferences. This may lead to participants using the same access PIN for different conferences. In this case, the participants who wish to join different conferences are connected to each other in the same conference room. To manage access PIN assignment for MeetNow! conferences, each user can be assigned a personal access PIN. He/she then needs to use this PIN when inviting other participants to a MeetNow! conference. Such a private access PIN may be derived from a company's extensions, for example.

5.2.4 Video Standards and Hardware Supported for the Conference Portal Application

The conference portal support of video standards and video hardware is defined by the video standards and video hardware that the OpenScape Media Server supports. They are described in detail in the scope of the OpenScape Media Server features.

5.3 Voice Portal Applications

If you use the OpenScape Media Server under OpenScape UCApplication, the voice portal is automatically installed with the OpenScape Media Server setup. The voice portal provides a telephone user interface (TUI) via which users can access the comprehensive Unified Communications services of OpenScape UCApplication.

There are two applications for the voice portal, each of which providing different telephone user interfaces:

- The application Voice Portal

  This application provides telephone user interfaces that a user operates with the keypad of his/her telephone.
- The application Voice Portal "Speech"

  This application provides telephone user interfaces that a user operates by voice commands.

The voice portal applications Voice Portal and Voice Portal "Speech" both provide two access types of telephone user interfaces for accessing the respective voice portal application:

- User access (control mode)

  This type of access lets OpenScape users e. g. configure their UC Application settings or access the Unified Communications services of OpenScape UCApplication.
- Guest access (answering machine mode)

  This type of access allows guests to leave messages for OpenScape users.

Voice Portal Application Profiles

You can perform the settings of the voice portal applications Voice Portal and Voice Portal "Speech" individually for each Media Server in the voice portal plug-in of the Common Management Platform. This configuration is based on the voice portal application profiles. You can bind each of these application profiles to access phone numbers via a terminal, thus enabling voice portal access with individual settings.

5.4 AutoAttendant Application

If you use the OpenScape Media Server under OpenScape UCApplication, the AutoAttendant application is automatically installed along with the OpenScape Media Server. This application is an automated central postmaster account for OpenScape UCApplication that can be customized.

With its help you can construct static and interactive workflows from pre-defined elements in a simple way. Such workflows can route incoming calls specific to time and caller without an employee having to interfere in the routing process.

AutoAttendant details are contained in the manual *OpenScape UCApplication AutoAttendant, Administrator Documentation*.

5.5 Customized Applications

Using the Application Builder you can create customer-specific IVR-based applications for the OpenScape Media Server. For this purpose, you create on the graphic user interface of the Application Builder the flowchart of a passive or interactive voice dialog application.

This flowchart consists of blocks and connections between these blocks. The flowchart blocks are controls that, for example, play a sound file, perform a database query or establish a phone connection to a subscriber. The connections between the controls in the flowchart indicate from which control a transition to another control is possible.

The Application Builder puts out a created application as Java file, which the OpenScape Media Server can then import and execute as deployment file.

The manual OpenScape UCApplication Application Builder, Administrator Documentation provides details of the Application Builder and describes how to create customized applications with it.

6 OpenScape Media Server Standards

The OpenScape Media Server supports different standards. But which of these the OpenScape Media Server uses in live operation depends on whether you deploy the OpenScape Media Server at OpenScape Voice or under OpenScape UCApplication.

The following list itemizes the most important standards that the OpenScape Media Server supports in the single application environments.

At OpenScape Voice:

- Media Gateway Control Protocol (MGCP)
- Real-Time Transport Protocol (RTP / RTCP)
- Secure Real Time Transport Protocol (SRTP)
- Session Description Protocol (SDP)
- Multimedia Internet Keying (MIKEY)
- SDP Security Descriptions for Media Streams (SDES)

Under OpenScape UCApplication:

- Media Resource Control Protocol (MRCP)
- Real-Time Transport Protocol (RTP / RTCP)
- Secure Real Time Transport Protocol (SRTP)
- Session Description Protocol (SDP)
- Alternative Network Address Types (ANAT)
- Interactive Connectivity Establishment (ICE)
- Session Initiation Protocol (SIP)
- Transport Layer Security Protocol (TLS)
- Voice Extensible Markup Language (VXML)
- Multimedia Internet Keying (MIKEY)
- SDP Security Descriptions for Media Streams (SDES)
- Binary Floor Control Protocol (BFCP)

6.1 Media Gateway Control Protocol (MGCP)

The introduction of Voice over IP (VoIP) requires IP-based networks being able to communicate with classic PBX networks. For this purpose, so-called media gateways were developed to bridge the networks. In this environment, MGCP originally served for centrally controlling these gateways by a so-called call agent.

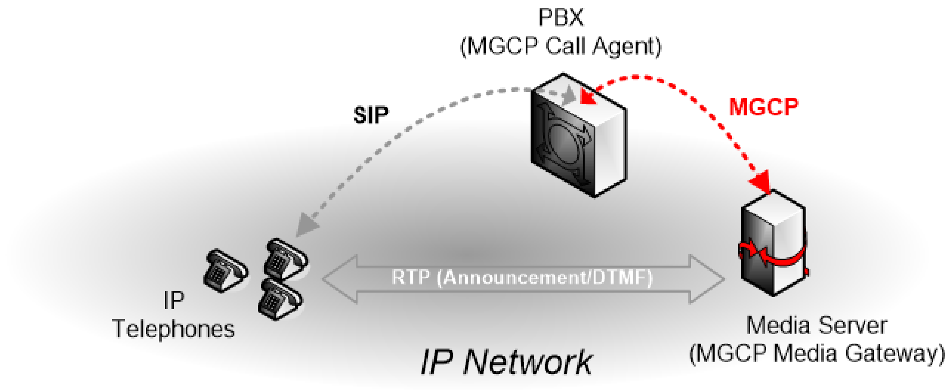
In the mean time, PBXs use MGCP in particular to control connected Media Servers.

6.1.1 MGCP in the OpenScape Media Server

NOTICE:

MGCP is used in the OpenScape Media Server at OpenScape Voice only.

The following figure shows how MGCP is used in the OpenScape Media Server.



The PBX uses MGCP:

- For controlling announcement playback by the OpenScape Media Server. To this, the PBX informs the OpenScape Media Server which announcement it should send to which terminal device. Only after this instruction phase the announcement thus defined can be directly transmitted by the OpenScape Media Server to the telephone terminal device via RTP.
- For controlling the conferencing features for participant-controlled conferences of OpenScape Voice in the OpenScape Media Server.
- For monitoring the telecommunication according to CALEA / LI.

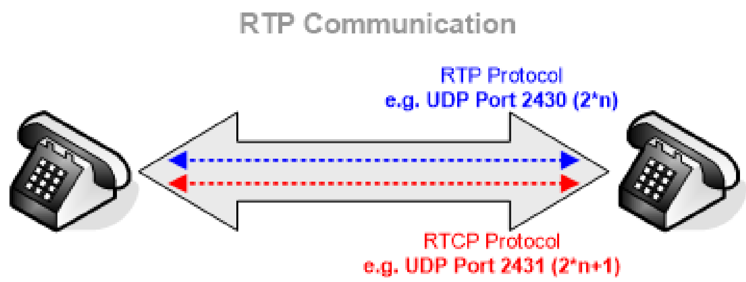
In case of MGCP, the OpenScape Media Server assumes the role of the MGCP media gateway, while the PBX executes the MGCP call agent function.

6.2 Real-Time Transport Protocol (RTP / RTCP)

RTP provides an IP-based transmission service for real-time communication between terminal devices. In combination with UDP it is used especially for transmitting audio and video information.

RTP itself does not provide a mechanism to secure the transmission quality. Such requirements must – if necessary – be met by underlying network layers. RTP is able to ensure real-time communication even without such mechanisms. It uses consecutive numbering of the sent data packets for this purpose. Based on this numbering the recipient can rearrange information that arrived in the wrong order. Numbering also serves here to determine the correct position of a data fragment within a data stream. This is particularly important for audio and video transmissions, from which information is continuously lost owing to poor transmission quality.

Data transmission via RTP may be based on a total of two protocols.



- RTP

  Enables the transmission of the actual media stream of an RTP communication.
- RTCP

  Enables optional checking tasks in the scope of an RTP communication. This includes among other things:

  – continuously monitoring the service quality – e. g. in the form of lost data packages
  – the distribution of information about communication participants

Both, RTP and RTCP use an individual transmission channel to communicate. With using UDP this corresponds to one UDP port each. On a subscriber system, two often consecutive UDP ports are accordingly allocated for each communication relation. An even port number is then used as port for RTP, and the next higher odd port number as port for the associated RTCP communication.

You find detailed information on RTP and RTCP operation is available in the relevant RFC specifications of the IETF standardization board.

6.2.1 RTP in the OpenScape Media Server

RTP serves for the actual audio information transmission between OpenScape Media Server and terminal device.

The following figures show how RTP is used in the OpenScape Media Server; depending on whether the OpenScape Media Server is used at OpenScape Voice or under OpenScape UCApplication.

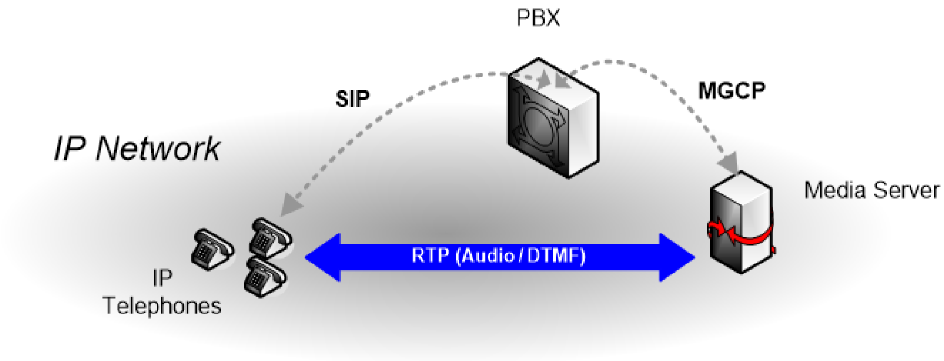


Figure 3: Using RTP at OpenScape Voice

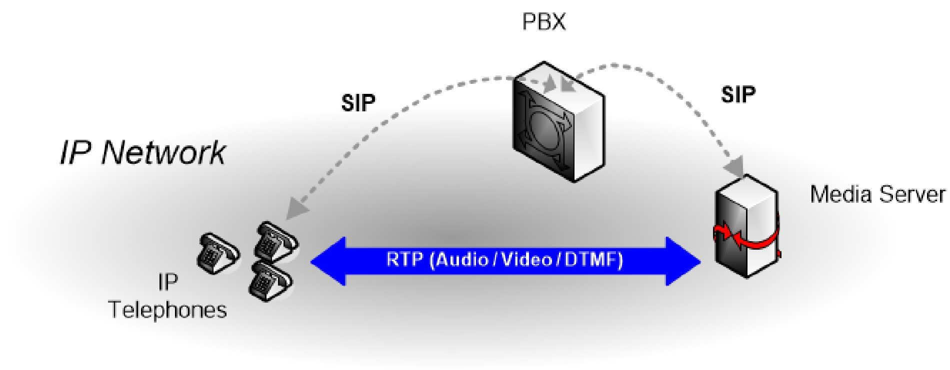


Figure 4: Using RTP under OpenScape UCApplication

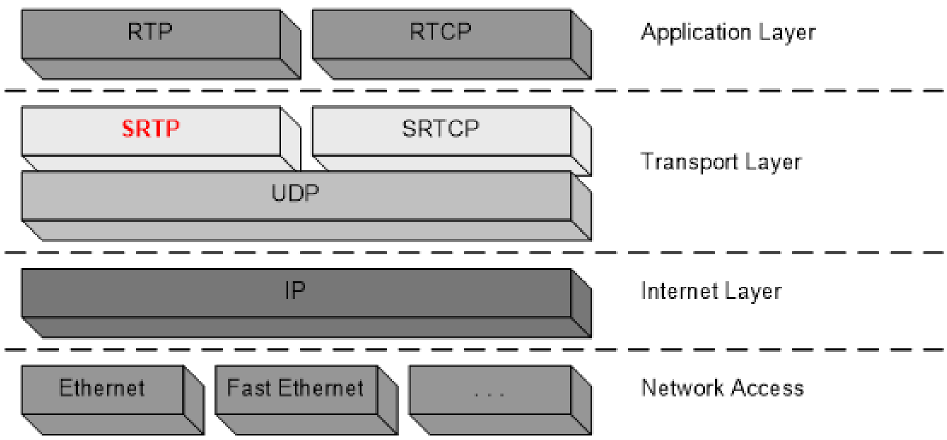
6.2.2 RTCP in the OpenScape Media Server

If the option **RTCP Reporting** is active for an RTP streaming route of the OpenScape Media Server, the OpenScape Media Server sends RTCP originator reports via the relevant RTP streaming route in specific intervals. Furthermore, it can receive RTCP originator / receiver reports via the relevant RTP streaming route.

6.3 Secure Real Time Transport Protocol (SRTP)

SRTP is used for encrypted RTP data transmission.

The following figure shows the position of SRTP in the TCP / IP layer model.



Using SRTP serves mainly the following purposes:

- ensuring the authenticity of a communication partner.

  For this purpose, communication partners usually exchange individual keys for each connection, with which message transmission is encrypted. Consequently, intruding parties cannot send messages the originator of which is apparently a different person.
- securing the confidentiality of RTP payload.

  RTP data is encrypted before its transmission for this purpose. This makes it difficult for intruding parties to read along sent messages.

- guaranteeing the integrity of RTP payload and header.

  This disables an intruding party to alter a message unnoticed.

You find continuative information about SRTP e. g. under:
`ftp://ftp.rfc-editor.org/in-notes/rfc3711.txt`.

6.3.1 SRTP in the OpenScape Media Server

The OpenScape Media Server uses SRTP to secure the RTP payload from unauthorized access.

IMPORTANT:

Using SRTP with MIKEY requires the system time of all systems involved in the SRTP communication to be synchronized – OpenScape Media Server, RTP-based devices (e. g. phone), VoIP gateway etc. The Network Time Protocol (NTP) may be used for this purpose.

The following figures show how SRTP is used in the OpenScape Media Server; depending on whether the OpenScape Media Server is used at OpenScape Voice or under OpenScape UCApplication.

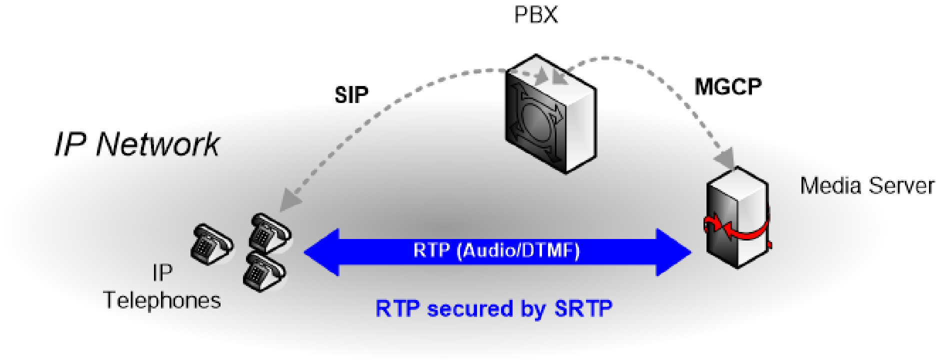


Figure 5: Using SRTP at OpenScape Voice

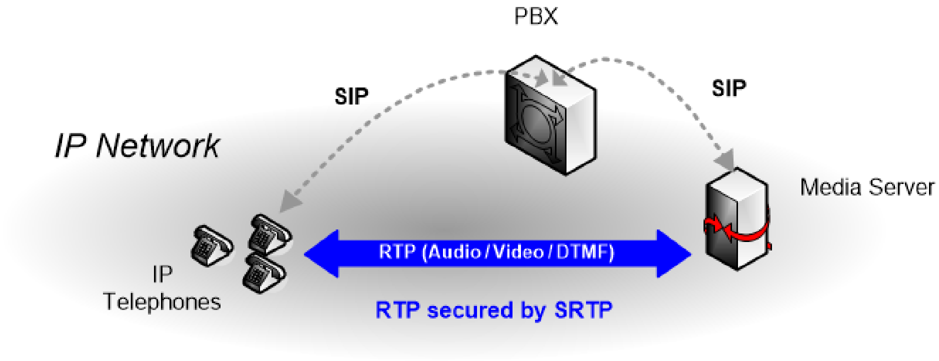


Figure 6: Using SRTP under OpenScape UCApplication

In the depicted example, SRTP secures the RTP-based audio data that is exchanged between the OpenScape Media Server and IP-telephones.

If the OpenScape Media Server is used at OpenScape Voice, IPSec should also be used to secure the MGCP communication between the OpenScape Media Server and OpenScape Voice from unauthorized access.

If the OpenScape Media Server is used under OpenScape UCApplication, TLS must also be used to secure the SIP signaling between the OpenScape Media Server and OpenScape UCApplication from unauthorized access.

6.4 Session Description Protocol (SDP)

Communication partners use SDP for negotiating a data exchange for the connection parameters.

If terminal devices are to communicate with each other via a data network, they first need to agree on the type of data they want to exchange and on the data format. They define various connection parameters before the actual data exchange for this purpose.

Such connection parameters comprise in particular:

- Information about the media used (audio, video)
- Information about the codec used
- Encryption information
- Simple connection metadata

SDP provides merely a standardized format for negotiating such connection parameters. Because SDP does not define a proprietary transfer protocol, it needs to rely on an existing one – e. g. MGCP or SIP.

You find continuative information about SDP e. g. under:

`ftp://ftp.rfc-editor.org/in-notes/rfc4566.txt`

6.4.1 SDP in the OpenScape Media Server

The OpenScape Media Server uses SDP to exchange connection information with the involved telephones – in particular also the keys for encrypting the SRTP communication.

In this process SDP only specifies the transmission format for the connection information. As actual transmission protocol the OpenScape Media Server uses MGCP at OpenScape Voice respectively SIP under OpenScape UCApplication.

6.5 Alternative Network Address Types (ANAT)

Using ANAT, communication partners can negotiate during a connection setup which IP address each of them uses for the connection to be set up. It is thus an extension of SDP.

In case of setting up a communication connection the communication partners involved can negotiate via standard SDP various parameters they want to use for the relevant connection. Such parameters comprise e. g. the codec to be used or the IP address. While the communication partners can well exchange a list of alternative codecs in this way, this is not possible in case of the IP address. Consequently, each communication partner can always only specify one IP address when the communication connection is set up.

This standard SDP restriction causes problems especially if IP v4 as well as IP V6 addresses are used in a network. In such a case a communication partner is not to know whether his/her counterpart may address exclusively IP v4 or IP V6 addresses. If an IP address is specified that the counterpart cannot address, the communication partners may in this case not be able to set up a connection between them.

In such a network environment you can use ANAT as extension of standard SDP for offering an alternative IP address for a communication connection to a communication partner – namely e. g. an IP v4 and an alternative IP V6 address.

The ANAT function thus resembles the function of the ICE protocol. Please note though that ICE extends the SDP functions conformable to SDP but ANAT does not. Consequently, a terminal device using ANAT may not be able to communicate with terminal devices that solely use standard SDP. However, a terminal device using ICE may well be able to communicate with terminal devices using standard SDP.

You find continuative information about ANAT under:

`http://rfc-editor.org/in-notes/rfc4091.txt`

6.5.1 ANAT in the OpenScape Media Server

In the OpenScape Media Server you can use ANAT for offering two alternative streaming routes per data stream during the SDP negotiation of SIP / MGCP connections. The two alternative streaming routes must always be based on different IP address versions – thus one on IPv4 and one on IPv6.

Consequently, IP v4 and IP v6 addresses can be simultaneously used in a network environment.

Alternatively to ANAT the OpenScape Media Server can also use the ICE protocol, which provides a comparable function.

NOTICE:

The ANAT and ICE protocols cannot be used simultaneously.

6.6 Interactive Connectivity Establishment (ICE)

Using ICE, communication partners can define during a connection setup which IP address and which transport layer address each of them uses for the connection to be set up. ICE uses an active algorithm for identifying combinations of IP address and transport layer address via which the communication partners can communicate.

The ICE function thus resembles the function of the ANAT protocol. Please note though that ICE extends the SDP functions conformable to SDP but ANAT does not. Consequently, a terminal device using ANAT may not be able to communicate with terminal devices that solely use standard SDP. However, a terminal device using ICE may well be able to communicate with terminal devices using standard SDP.

You find continuative information about ICE under:

`http://rfc-editor.org/in-notes/rfc5245.txt`

ICE-lite

ICE-lite is a partial implementation of ICE and, compared to the full ICE implementation, subject to the following restrictions:

- It can offer only one IPv4 and one IPv6 candidate per media stream.
- It does not use an active algorithm for identifying combinations of IP address and transport layer address via which the communication partners can communicate. It can, however, respond correctly to the associated availability inquiries of a fully adequate ICE remote station.

ICE-microlite

ICE-microlite is a partial implementation of ICE and, compared to the full ICE implementation, subject to the following restrictions:

- It does not support NAT.
- It does not use an active algorithm for identifying combinations of IP address and transport layer address via which the communication partners can communicate. What's more, it does not react to the associated availability inquiries of a fully adequate ICE remote station.

6.6.1 ICE in the OpenScape Media Server

In the OpenScape Media Server you can use only ICE-lite and ICE-microlite for offering two alternative streaming routes per data stream during the SDP negotiation of SIP / MGCP connections. The two alternative streaming routes must always be based on different IP address versions – thus one on IPv4 and one on IPv6.

Consequently, IP v4 and IP v6 addresses can be simultaneously used in a network environment.

Alternatively to the ICE protocols the OpenScape Media Server can also use the ANAT protocol, which provides a comparable function.

NOTICE:

The ANAT and ICE-lite protocols cannot be used simultaneously.

6.7 Media Resource Control Protocol (MRCP)

MRCP is a client / server-based protocol and serves in voice dialog systems in particular for controlling system resources.

Detailed information on the operation mode of MRCP and its components is available in the associated RFC specifications of the IETF.

6.7.1 MRCP in the OpenScape Media Server

MRCP is used in the OpenScape Media Server to control the ASR and TTS system used in OpenScape UCApplication by the conference and voice portal.

For this the OpenScape Media Server works as MRCP client.

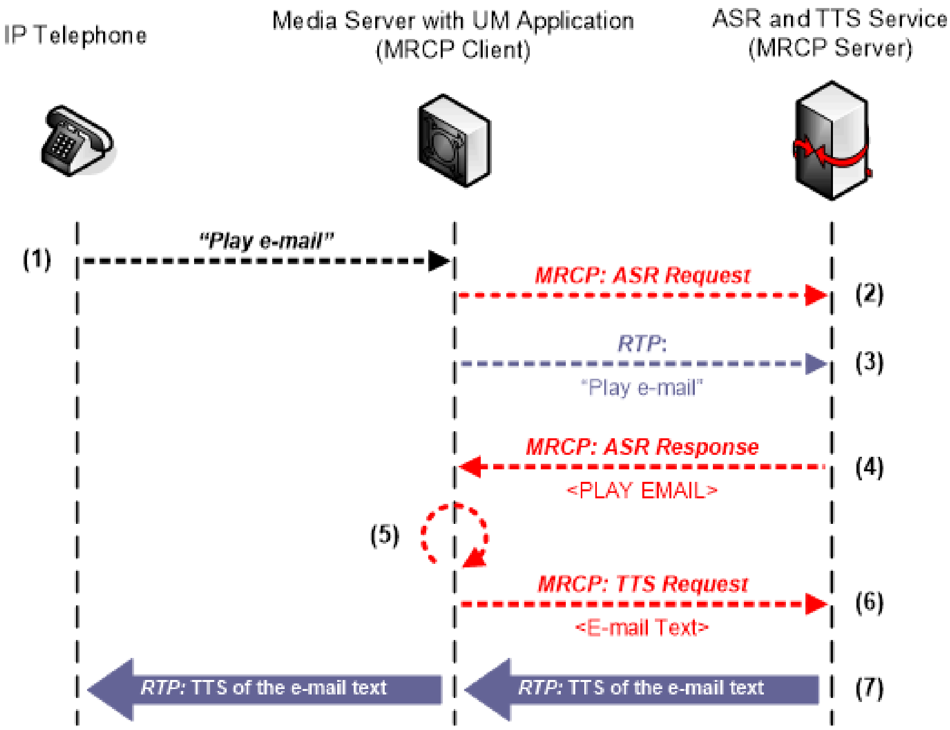
NOTICE:

MRCP is in the OpenScape Media Server only used under OpenScape UCApplication.

NOTICE:

The ASR and TTS system must have been installed on the OpenScape Media Server computer system.

The following figure exemplifies the MRCP communication of the OpenScape Media Server. It shows the voice-operated retrieval of an e-mail, which is put out by text-to-speech.



1) The user enters the voice command "Play e-mail" in his/her device to play an e-mail via the Unified Messaging (UM) application of the OpenScape Media Server.

2) This voice command must be evaluated by the voice-controlled Unified Messaging application. For this purpose, the OpenScape Media Server sends an ASR request to the MRCP server, thus asking for the associated ASR service.

3) The OpenScape Media Server sends the recorded voice command as RTP sound data to the ASR service.

4) The ASR service evaluates the RTP sound data and recognizes the command “PLAY EMAIL”. The MRCP server returns this result as ASR response to the OpenScape Media Server.
5) The Unified Messaging application of the OpenScape Media Server executes the “PLAY EMAIL” command by internally accessing the requested e-mail data to prepare their playback.
6) So that the e-mail text can be output at the user's telephone, it must be converted into speech. For this purpose, the OpenScape Media Server sends a TTS request to the MRCP server, thus asking for the associated TTS service. With the TTS request the OpenScape Media Server also sends the e-mail text to be converted into speech.
7) The TTS service converts the e-mail text into speech and sends the thus created sound data to the OpenScape Media Server via RTP. The server then forwards the sound data to the user's terminal device.

6.8 Session Initiation Protocol (SIP)

SIP was developed by the IETF. It originally realized the signaling of IP-based voice transmission, but has in the meantime been expanded for applications in the areas video and instant messaging. Since SIP only realizes signaling of connections within this scope, it uses various other protocols for the actual payload transmission. This includes e. g. RTP, used for transmitting real-time data.

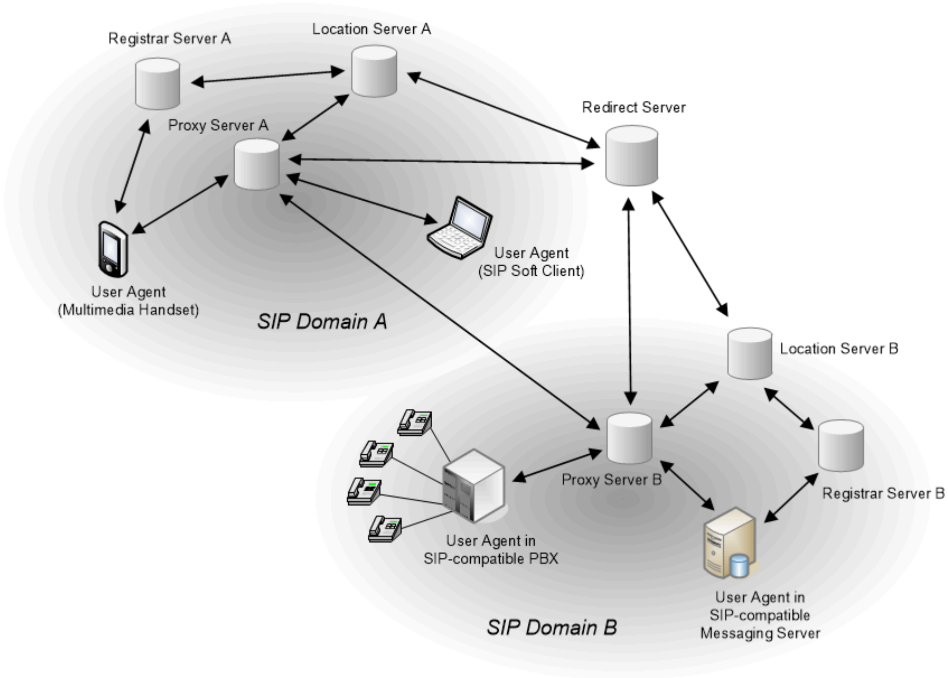
In the voice area, SIP enables all basic call functions such as connection set-up and shutdown and call notification. Beyond that, further features are already implemented in SIP. Among these are the features call transfer or conference switch. Considering the supported features, SIP can by now be compared with H.323.

Contrary to H.323, the SIP communication model realizes a big part of the functions in the terminal device. This significantly differentiates it from the traditional communication concepts in which the actual intelligence lies in the network nodes.

You find further information on SIP in the appropriate literature or in the relevant RFC standards of the IETF (`www.ietf.org`).

6.8.1 SIP Network Components

An SIP network consists of different SIP-specific logic components. These intercommunicate in a defined way.



The logic components of an SIP network are:

- User Agent (UA)

  The user agent represents the terminal device in an SIP network. It signals and manages SIP connections that it initiates with other user agents or proxy servers. Upon logging in at an SIP network a user agent registers with the registrar server in charge.

  The user agent is logically divided into the user agent client and the user agent server. The user agent client is in charge of initiating SIP connections. The user agent server replies to connection requests.

  User agents are e.g. SIP telephones or an SIP client software.
- Registrar Server

  Registrar servers are responsible for registering user agents. The information collected during logging on single user agents are transferred to the location server that stores this information for future requests.

  Registrar servers often operate on the same platform as the associated location server (see below).
- Location Server

  Each SIP domain has a location server. This server administers among other things information about bindings of logical and physical SIP addresses.

  Location servers often operate on the same platform as the associated registrar server (see above).
- Proxy Server

  Each SIP domain has a proxy server. This server receives the connection requests by user agents or other proxy servers. The proxy server is logically divided into a client and a server component, which perform individual connection requests on behalf of user agents.

With handling a connection request, two cases must be differentiated:

– The communication participants are in the same SIP domain

  In this case only the proxy server of the domain concerned is involved in the connection establishment.

– The communication participant is in different SIP domains

  In this case the two proxy servers of the domains concerned are involved in the connection establishment.

For the resolution of SIP addresses the proxy server communicates with the associating location and redirect server.

- Redirect Server

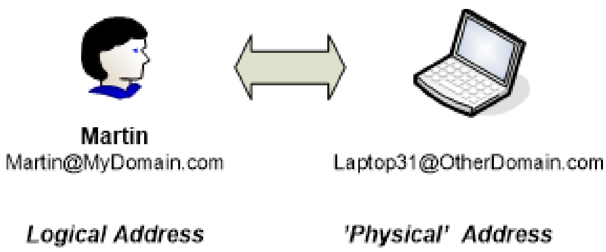
  A redirect server processes proxy server requests as regards configured call reroutings for user agents. It operates domain-spanning.

  For the resolution of SIP addresses the redirect server communicates with the associated location server.

6.8.2 Addressing an SIP Subscriber

SIP addressing is based on a logical and a physical SIP address. The logical address is assigned to the person "user", the physical address is allocated for the device, with which the user registers with the registrar server. The actual routing within an SIP network occurs based on the physical address.

Example:



User Martin has in our example the logical address *Martin@MyDomain.com*. Under this address he is to be addressed in the entire SIP network. His physical[18] address, according to which messages are routed for him in the network, depends on the terminal device with which he registers in the SIP network. In our example Martin registers with a laptop. This laptop has the physical address *Laptop31@OtherDomain.com*.

If another SIP subscriber wants to establish a communication relation to Martin, he/she addresses the connection setup with the logical destination address *Martin@MyDomain.com*. This makes sense since the SIP users do not know via which terminal device a subscriber registers. In the course of the connection setup this logical address is resolved by the location server into the current physical address.

18 The physical SIP address is not to be confused with an address of the physical OSI layer.

6.8.3 Interaction between Logical SIP Components

The interactions between the logical SIP components are based on various transactions.

Such interactions consist in each case of:

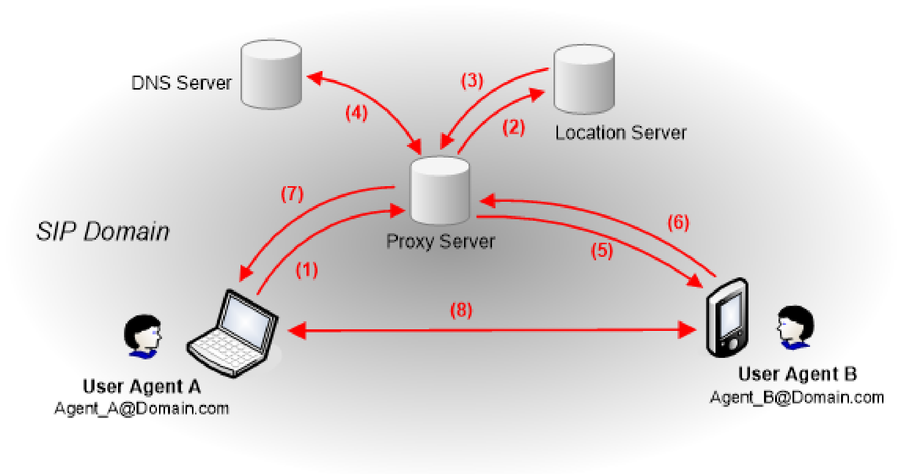
- a request sent by an SIP client to an SIP server
- an associated reply sent by an SIP server to an SIP client

Let's take a look at two simple examples to describe the general interactions between the SIP components to establish a connection between two user agents. For reasons of simplification we discount the registrar and redirect server function.

The first example describes the connection establishment between two agents who are in the same SIP domain. In the second case the user agents involved are in different SIP domains.

Connection between two Subscribers in one SIP Domain

Let us see how an SIP connection is established between two SIP clients that are in the same SIP domain.



1) User-agent A initiates a connection to user-agent B. For this purpose, he/she sends a corresponding connection request to the proxy server of the domain. The connection request contains the logical SIP address of the destination party– Agent_B@Domain.com.

2) The proxy server requests the registered address information of the destination subscriber from the location server.

3) The location server replies to the proxy server with the physical SIP address of the destination subscriber.

4) Subsequently, the proxy server resolves the received SIP address into an IP address via the DNS server in charge.

5) The proxy server sends an individual connection request to the IP address of user-agent B.

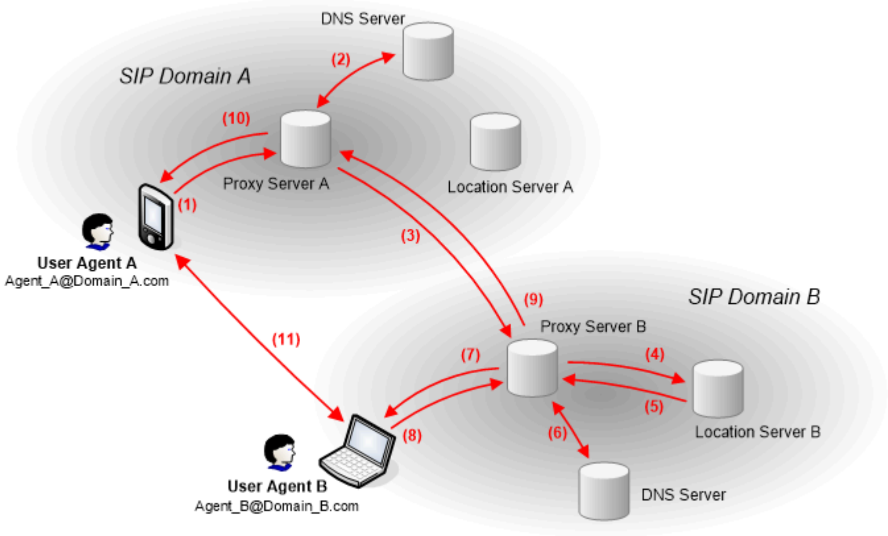
6) User-agent B replies to this request and informs the proxy server that he/she accepts the requested connection.

7) The proxy server correspondingly accepts the original connection request of user-agent A (see 1).

8) User-agent A then establishes a direct RTP connection to user-agent B.

Connection between two Subscribers in different SIP Domains

The following example shows the general structure of an SIP connection between two subscribers in different domains.



1) User-agent A initiates a connection to user-agent B. For this purpose he/she sends a corresponding connection request to proxy server A of his/her own domain. The connection requests contains the logical SIP address of the destination party– Agent_B@Domain_B.com .

2) By the domain name of the destination address Domain_B.com , proxy server A recognizes that user agent B does not belong to the own domain A. Subsequently, it queries the IP address of the proxy server responsible for domain B at the DNS server in charge. Thus the IP address of proxy server B.

3) Proxy server A then sends its own connection request to proxy server B[19].

4) Proxy server B then requests the SIP address under which the destination subscriber is registered in the SIP network from the location server in charge.

5) The location server replies with the physical address of the destination subscriber.

6) Subsequently, the proxy server resolves the received address into an IP address via the DNS server in charge.

7) Proxy server B now sends an individual connection request to user-agent B.

8) User-agent B replies to this request and informs proxy server B that he/she accepts the requested connection.

9) Proxy server B accepts the connection request by proxy server A (see 4).

10) Afterwards, proxy server A accepts the connection request by user-agent A (see 1).

11) User-agent A then establishes a direct RTP connection to user-agent B.

19 Proxy server A thus becomes the outbound proxy server, proxy server B the inbound proxy server.

6.8.4 SIP Subscriber Line and SIP Trunk

SIP components can be connected to each other via different connection types:

- SIP subscriber connection (SIP subscriber line)
- SIP server connection (SIP trunk)

SIP trunk and SIP subscriber line differ mainly in the fact that the SIP trunk is configured statically, whereas the SIP subscriber line has a dynamic connection character. In contrast to components connected via an SIP trunk, components connected via an SIP subscriber line must therefore register with the SIP network.

Accordingly, SIP proxys are connected to each other via SIP trunks, for example. Subscriber lines, on the other hand, are used to connect SIP terminal devices.

If you connect an SIP-based PBX to other SIP components via an SIP trunk, you have the advantage that you can use additional features for connections via this trunk. Such features are in particular:

- Outgoing-call billing
- Several addresses or address ranges for incoming calls
- Several originator addresses

6.8.5 SIP in the OpenScape Media Server

The OpenScape Media Server provides the user access for parts of OpenScape UCApplication – e. g. the user access to the conference portal. In order to accept incoming connection requests and to establish outgoing connection requests, the OpenScape Media Server operates as SIP user agent.

NOTICE:

SIP is in the OpenScape Media Server only used under OpenScape UCApplication.

You need to connect the OpenScape Media Server to OpenScape Voice or to another SIP-compatible communications system via an SIP trunk. In doing so you configure the communications system used in a way that it conveys all SIP connections to the OpenScape Media Server the destination addresses of which begin with a defined prefix.

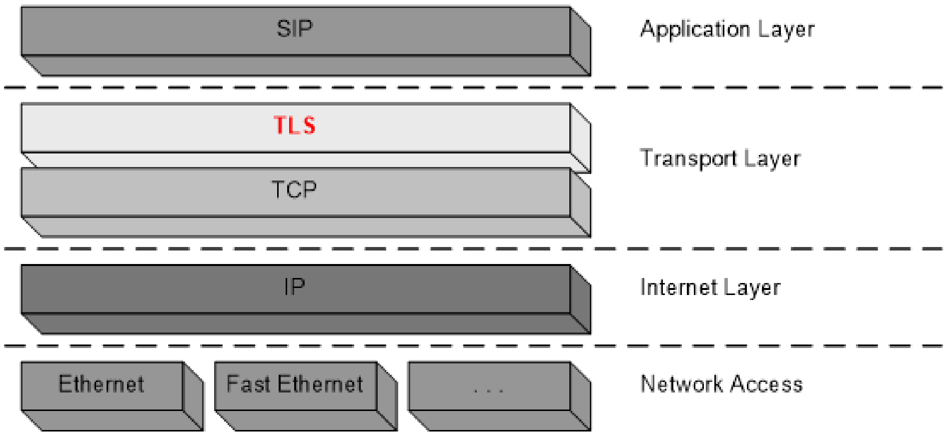
IMPORTANT:

The OpenScape Media Server always requires an SIP trunk for communicating with a communications system. If no SIP trunk is used, communication between OpenScape Media Server and the communications system fails.

6.9 Transport Layer Security Protocol (TLS)

TLS is an IETF recommendation and successor to the Secure Socket Layer (SSL) protocol, which was developed by Netscape to encrypt Internet communication.

The following figure shows the position of TLS in the TCP / IP layer model.



TLS is positioned directly above the transport protocol TCP. All information of the application layer lying on top, which includes SIP, is thus encrypted.

Using TLS serves mainly the following purposes:

- ensuring the authenticity of a communication partner.

  To this, TLS uses security certificates and asymmetric encryption. Consequently, intruding parties cannot send messages the originator of which is apparently a different person.
- assuring the confidentiality of a connection

  Data is encrypted before its transmission. This makes it difficult for intruding parties to read along sent messages.
- guaranteeing message integrity

  This disables an intruding party to alter a message unnoticed.

You find continuative information about TLS e. g. under: `http://www.ietf.org/rfc/rfc2246.txt.`

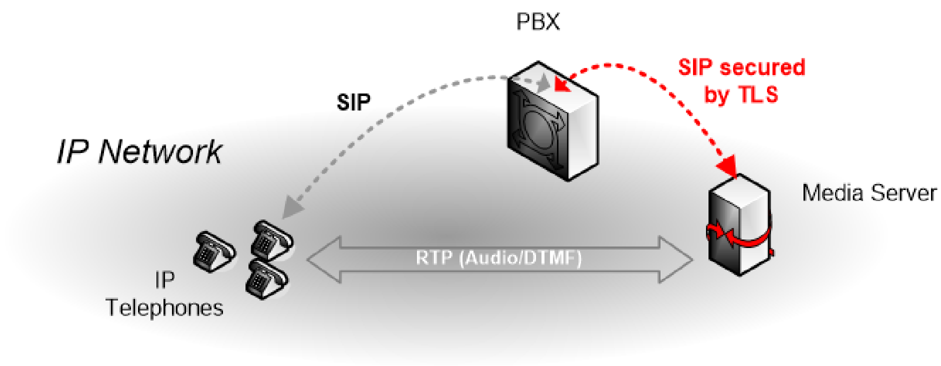
6.9.1 TLS in the OpenScape Media Server

The OpenScape Media Server uses TLS to secure the SIP signaling from unauthorized access.

NOTICE:

TLS is in the OpenScape Media Server only used under OpenScape UCApplication.

The following figure shows a OpenScape Media Server connection to a PBX.



TLS secures here the control information exchanged between the OpenScape Media Server and the PBX.

Consider here that TLS is a store-and-forward-based protocol. To ensure that the SIP communication is encrypted on the entire transmission network from the OpenScape Media Server server to the SIP terminal device, TLS must also be implemented between PBX and telephone.

The audio data of the communication connection must be separately protected from unauthorized access – e. g. using SRTP.

6.10 Voice Extensible Markup Language (VXML)

VoiceXML is a markup language that describes the flow of voice dialogs in voice dialog systems.

In many sectors of their daily life people have come across voice dialog systems such as online banking, time table information or automatic routing assistants for a long time. Such systems offer the option of being served by voice operation.

In the past, producers would program the dialog structure as integral part of the respective voice dialog system. This results in the following:

- The dialog structure could in most cases not be separated from the respective voice dialog system
- Modifications to the dialog structure used to require an adjustment of the entire voice dialog system.

To avoid such disadvantages, many producers started to develop their dialog structures independently from the respective voice dialog system. This required the development of new means and methods though, which each producer developed and maintained individually.

To reduce such development and maintenance efforts, the World Wide Web Consortiums (W3C) eventually developed the markup language VoiceXML. It is based on the meta language XML and serves for the universal description of dialog structures in a voice dialog system. In this function, VoiceXML can be compared with other markup languages – for example with HTML, used for marking up internet texts.

Since VoiceXML marks up voice information and thus audio data, common HTML web browsers cannot be used for this data output. The output software required instead is a VoiceXML browser. This browser interprets the VoiceXML code of a VoiceXML document and plays the actual voice information according to its marking up.

The working method of a VoiceXML environment can be demonstrated by the similar working method of an HTML environment.

Working method in an HTML environment

1) The web browser of the web client requests an HTML document from the web server.
2) The web server loads the static content of the requested document or creates the relevant document dynamically.
3) The web server then sends this document to the web client, which displays it in its web browser.

Working method in a VoiceXML environment

In a VoiceXML environment this process is in principle the same. But the central element is no HTTP document but a VoiceXML document.

Another difference is: in an HTML environment the web browser is usually directly available on the user device, e.g. the PC. In a VoiceXML environment the VoiceXML browser is not found on the user device – e. g. the telephone. Instead, it exists, for example, on a Media Server. In this case the user connects his/her device with the Media Server, which is controlled by its VoiceXML browser in a way that it emits all required outputs via the user device.

You find continuative information about the markup language VoiceXML e. g. under:
`http://www.w3.org/`

6.10.1 VoiceXML in the OpenScape Media Server

The OpenScape Media Server provides a VoiceXML interface that customer-specific applications can use. In this scope the OpenScape Media Server reproduces the content of the VoiceXML documents that it receives from an application.

NOTICE:

VoiceXML is in the OpenScape Media Server only used under OpenScape UCApplication.

To interpret and put out the relevant VoiceXML documents, a VoiceXML browser is integrated in the OpenScape Media Server.

6.11 Multimedia Internet Keying (MIKEY)

MIKEY is a key management security model and thus used where keys must be managed for message encryption. It is an IETF recommendation and was developed especially for real-time applications. Because of this orientation, MIKEY is today especially used in the SRTP environment.

MIKEY's tasks are to:

- generate keys for RTP-information encryption
- distribute the generated keys to the involved communication partners

You find continuative information about MIKEY under:
`http://www.ietf.org/rfc/rfc3830.txt.`

6.11.1 MIKEY in the OpenScape Media Server

In the OpenScape Media Server, MIKEY is used for the management of keys used to encrypt SRTP connections.

In this function it has the following tasks:

- Creating a new key for each SRTP connection
- Initiate to distribute the created keys among the involved communication partners.

The keys are distributed via the signaling channel while the connection parameters for the communication are negotiated with the connection partners. For the actual key transmission MIKEY uses SDP (Session Description Protocol).

If the OpenScape Media Server is used at OpenScape Voice, the SDP information is transmitted within MGCP. IPSec should be used in this process to secure the key information from unauthorized access.

If the OpenScape Media Server is used under OpenScape UCApplication, the SDP information is transmitted within SIP. TLS must be used in this process to secure the key information from unauthorized access.

6.12 SDP Security Descriptions for Media Streams (SDES)

SDES is a key management security model and thus used where keys must be managed for encrypting messages. It is an IETF recommendation and was developed especially for real-time applications. Because of this orientation, SDES is today especially used in the SRTP environment.

SDES's tasks are to:

- generate keys for RTP-information encryption
- distribute the generated keys to the involved communication partners.

You find continuative information about SDES e. g. under:
`http://www.ietf.org/rfc/rfc4568.txt.`

6.12.1 SDES in the OpenScape Media Server

In the OpenScape Media Server, SDES is used for managing keys used to encrypt SRTP connections.

In this function it has the following tasks:

- Creating a new key for each SRTP connection
- Distributing the created keys among the relevant terminal devices.

The keys are distributed via the signaling channel while the connection parameters for the communication are negotiated with the connection partners. For the actual key transmission SDES uses SDP (Session Description Protocol).

If the OpenScape Media Server is used at OpenScape Voice, the SDP information is transmitted within MGCP. IPSec should be used in this process to secure the key information from unauthorized access.

If the OpenScape Media Server is used under OpenScape UCApplication, the SDP information is transmitted within SIP. TLS must be used in this process to secure the key information from unauthorized access.

6.13 Binary-Floor-Control-Protocol (BCFP)

The Binary Floor Control Protocol is used for the support of dual video. The steering of presentations is accomplished via the BFCP protocol. The BFCP protocol establishes a separate TCP channel on an independent port. It allows establishing presentation "floors". A floor is associated with a video stream and is used to indicate that a presentation is active. Presentations are only active in one direction at anyone time. It is thus needed to release a floor before the other side can establish its floor, in order to start a presentation in the opposite direction.

You find continuative information about BCFP under:
`http://tools.ietf.org/html/rfc4582`

`http://tools.ietf.org/html/rfc4583`

The BFCP protocol is signaled via SDP by enabling a separate application m-line, as in the following example:

- m=application 40296 TCP/BFCP *
- a=floorctrl:s-only
- a=confid:1

- a=userid:2
- a=floorid:1 m-stream:3
- a=setup:passive
- a=connection:new

7 Technological Concepts of the OpenScape Media Server

The OpenScape Media Server supports various technological concepts. But which of these the OpenScape Media Server uses in live operation depends on whether you deploy the OpenScape Media Server at OpenScape Voice or under OpenScape UCApplication.

The following list itemizes the most important technological concepts that the OpenScape Media Server uses in the single application environments.

At OpenScape Voice:

- Configuration elements of the OpenScape Media Server
- Application partitioning
- Consistency check
- RTP monitoring
- Media Server farm at OpenScape Voice
- Tones and system announcements of OpenScape Voice
- Participant-controlled conferences (large conference)
- Communications Assistance for Law Enforcement Act (CALEA / LI)

Under OpenScape UCApplication:

- Configuration elements of the OpenScape Media Server
- Application partitioning
- Consistency check
- RTP monitoring
- Connecting several SIP servers
- Connecting alternative SIP servers
- Transfer conference
- Importing customer-specific applications
- Media Server farm under OpenScape UCApplication
- Announcement replication in a Media Server farm
- Trusted Transfer Mode (TTM)

7.1 Configuration Elements of the OpenScape Media Server

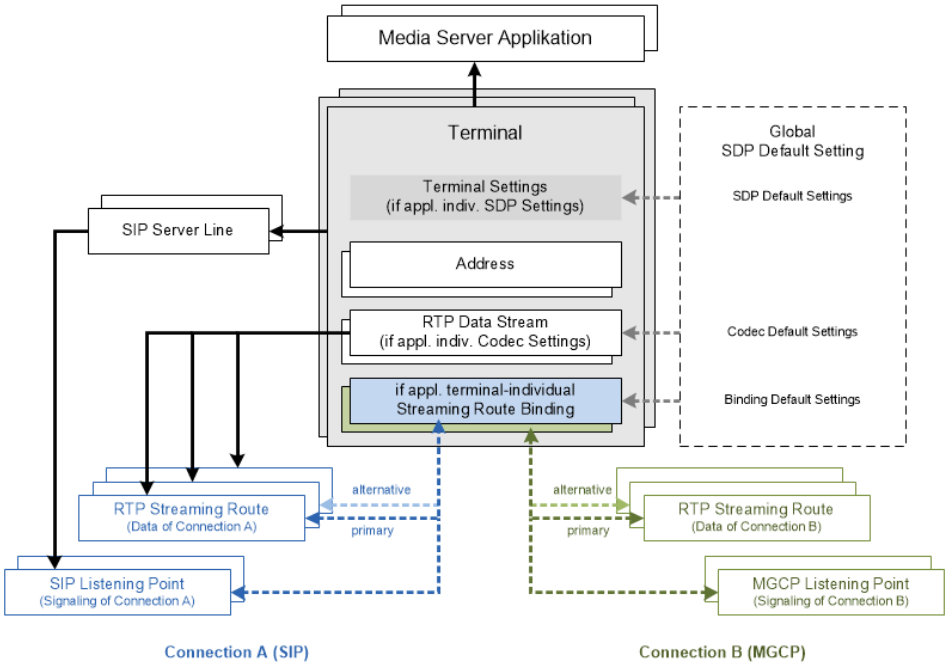
The OpenScape Media Server uses different configuration elements that control its communication behavior.

These are:

- Application
- Terminal
- Address
- RTP data stream
- RTP streaming route
- SIP server line [20]
- SIP / MGCP listening point
- Streaming route binding

20 SIP server lines are used only if the OpenScape Media Server is deployed under OpenScape UCApplication.

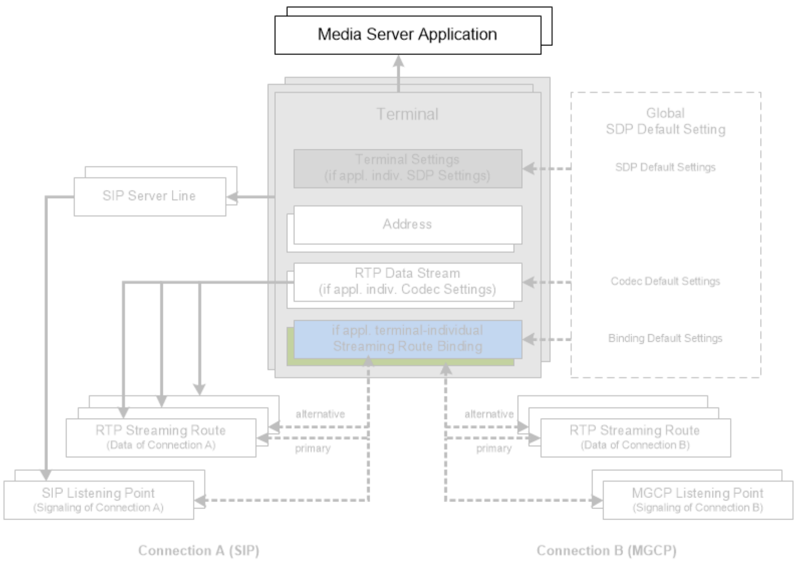
The following figure shows the structural dependencies that exist between these configuration elements. The represented dependencies and features of the single configuration elements are clarified in the following sections.



7.1.1 Application

The OpenScape Media Server executes various internal applications to provide media services to other systems or users under defined addresses. Such applications include under OpenScape UCApplication e.g. the voice portal or, at OpenScape Voice, e. g. the media gateway application for MGCP.

Applications are the origin or the destination of communication connections that the OpenScape Media Server sets up or receives.

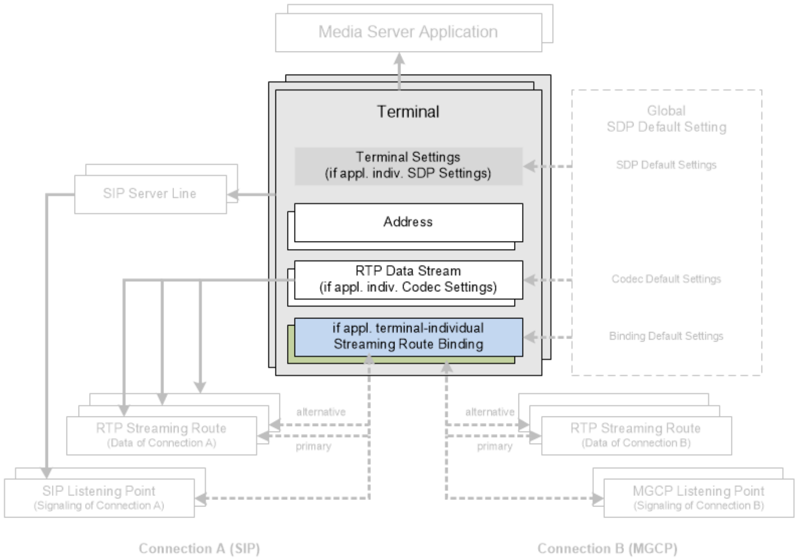


7.1.2 Terminal

A terminal defines in the OpenScape Media Server a communication endpoint for data and signaling streams. In this process, individual communication attributes are assigned to it.

NOTICE:

A terminal can be best compared with the logical configuration for the terminal device of a communications system, which is also assigned specific attributes – e. g. phone numbers.



The following configuration elements are assigned to a terminal of the OpenScape Media Server:

- An application for which the terminal forms the communication endpoint.
- Any number of addresses under which the terminal can be reached as communication endpoint.

NOTICE:

If the relevant application and thus the terminal need not be available from outside via SIP, no address has to be specified.

- Not more than one RTP data stream for each media type used. The terminal sends and receives RTP communication via the RTP data stream's RTP streaming routes.

- One SIP server line via which the terminal routes SIP communication for outbound communication connections. [21]

NOTICE:

If the relevant application need not set up outbound connections via the terminal, no SIP server line has to be specified.

- Optional, terminal-specific streaming route bindings that define via which RTP streaming route the OpenScape Media Server transmits connection payload when the associated connection signaling is handled via a specific listening point.

NOTICE:

Terminal-specific streaming route bindings have a higher priority than those valid across the system that you may have configured in the Streaming-IVR provider.

- General terminal settings – such as a billing address for charging terminal-related connection costs.
- Optional, generic properties transferred to the relevant application when being invoked. These properties influence only the behavior of the application and do not serve any other purpose in the OpenScape Media Server.

NOTICE:

The expert parameters of the conference portal can be used as generic properties, for example.

You find information about the expert parameters of the conference portal in the manual *OpenScape UCApplication, Configuration and Administration*.

Furthermore, you can perform the following special settings specific to a terminal:

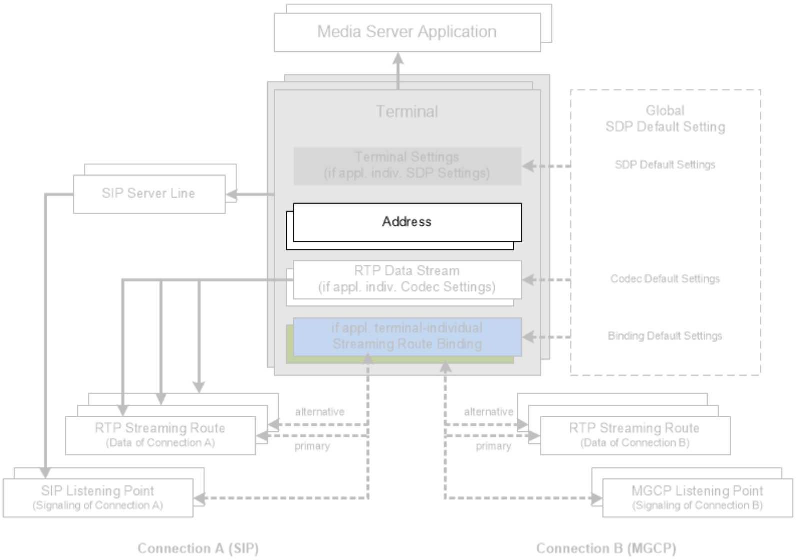
- Defining how the globally set security protocol SDES or MIKEY is used.
- Selecting and prioritizing the audio and video codecs to be used.

Such terminal-specific settings have a higher priority than the corresponding settings valid across the system that you may have configured in the Streaming-IVR provider.

21 SIP server lines are used only if the OpenScape Media Server is used under OpenScape UCApplication.

7.1.3 Address

An address defines how an application of the OpenScape Media Server can be reached for a user. The address may be a simple phone number or a number range.



In case of an inbound SIP connection the OpenScape Media Server checks whether a terminal exists for the dialed SIP address to which this phone number is assigned as address.

- If the OpenScape Media Server can uniquely associate the dialed phone number to a terminal, the OpenScape Media Server starts the assigned application. Furthermore, it determines the communication parameter to be used for the connection via the terminal.
- If the OpenScape Media Server cannot uniquely associate the dialed phone number to a terminal, the inbound SIP connection is rejected.

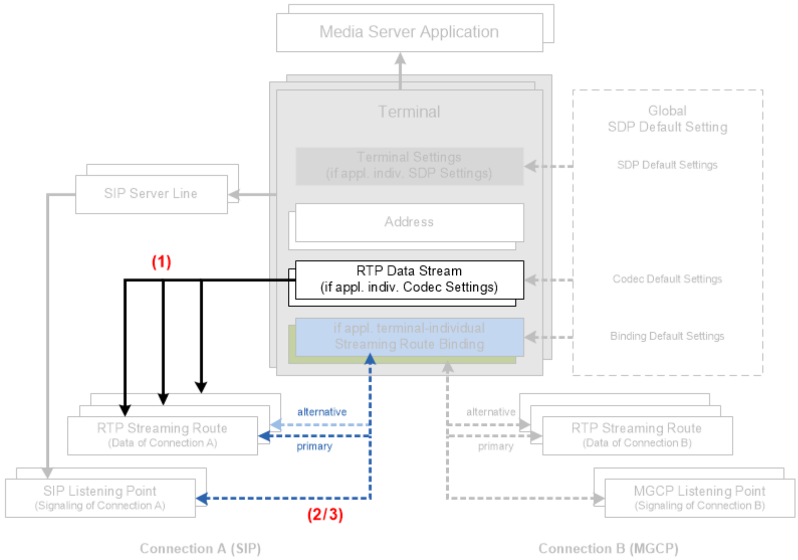
Before the OpenScape Media Server processes a dialed phone number, it normalizes this number via its normalization algorithm. Therefore, phone numbers always need to be specified in the terminal in the normalized phone number format.

Examples of normalized phone number formats:

- Single number
  - +492404901100
  - SIP : +492404901100@company.com
- Number range
  - +492404901 – +492404909
- Regular expression
  - +4924049011..
  - SIP : +492404901100@company.*

7.1.4 RTP Data Stream

An RTP data stream defines for a terminal a logical channel for transmitting RTP data. The data stream settings specify basic transmission parameters.



Such transmission parameters include:

- The media type (audio, video)
- The usable codecs inclusive their prioritization

NOTICE:

If you do not define terminal-specific codec settings, the global codec settings of the Streaming-IVR provider apply.

The streaming route to be used by a data stream for transmitting data must always be determined. This is done using the following options - also combined. Their prioritization declines from 1) to 3).

1) Assigning statistic streaming routes to the respective data stream.

NOTICE:

Even if several streaming routes are assigned to a data stream, it always uses only one of these streaming routes for transferring data of a specific RTP connection.

---

2) Assigning individual streaming route bindings to the terminal. Such streaming route bindings define the streaming route to be used dynamically, depending on the listening point respectively used.

3) Configuring globally valid streaming route bindings.

In a terminal, precisely one data stream must always be created for each media stream that the relevant application supports.

Example:

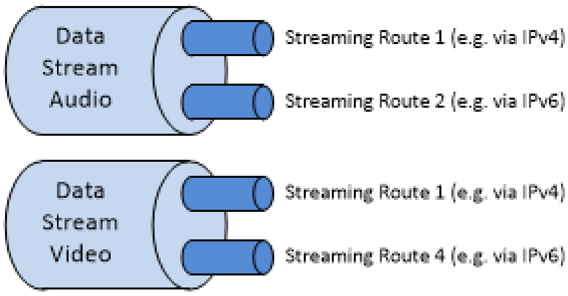
- Terminal for an audio application (e. g. the voice portal)

  In this case you need to create a data stream for media type audio in the relevant terminal.

  Individual streaming routes may have been assigned to this data stream.
- Terminal for a video application (e. g. the conference portal)

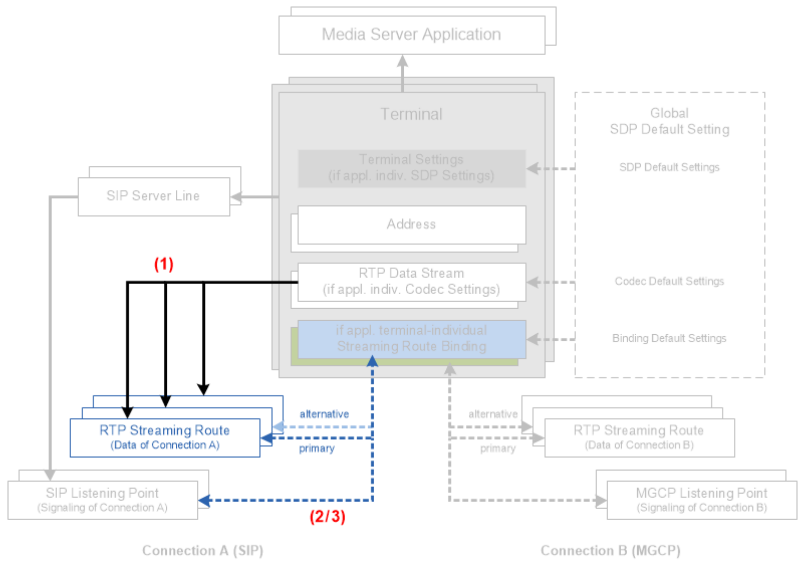
  In this case you need to create two data streams for the relevant terminal: One for media type audio and one for media type video.

  Individual streaming routes can be assigned to each of these data streams, but also such streaming routes used jointly by other data streams or terminals.



7.1.5 RTP Streaming Routes

An RTP streaming route defines a local network address with associated RTP / RTCP port range via which the data streams of the OpenScape Media Server send and receive RTP and RTCP data. This network address can be IPv4- or IPv6-based. VPNs are also supported.



Any number of RTP streaming routes can be configured for the OpenScape Media Server.

In the configuration always specify which streaming route a data stream is to use for transmitting data. To this, the following options exist. Prioritization decreases from 1) to 3).

1) By directly assigning individual streaming routes to a data stream.

NOTICE:

Even if several streaming routes are assigned to a data stream, it always uses only one of these streaming routes for transferring data of a specific RTP connection.

2) By assigning individual streaming route bindings to the terminal. Such streaming route bindings define the streaming route to be used depending on the listening point used.
3) By configuring global streaming route bindings.

7.1.6 Listening Points

A listening point defines a local network address with an associated port and transport protocol. This network address can be IPv4- or IPv6-based. VPNs are also supported. The OpenScape Media Server continuously monitors a network address defined in this way for incoming MGCP or SIP communication, through which other systems request media services of the OpenScape Media Server. Accordingly, a difference is made between MGCP and SIP listening points.

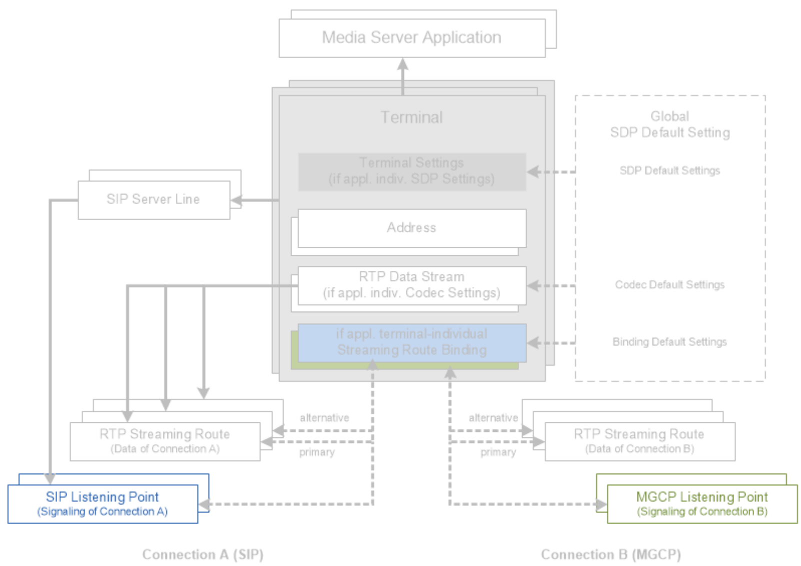
Any number of listening points can be configured for the OpenScape Media Server.

NOTICE:

The SIP listening points are not used if the OpenScape Media Server is deployed at OpenScape Voice. In this case the OpenScape Media Server uses MGCP listening points only.

NOTICE:

SIP listening points are also used for defining the network route in SIP server lines for outbound SIP signaling.



7.1.7 SIP Server Lines

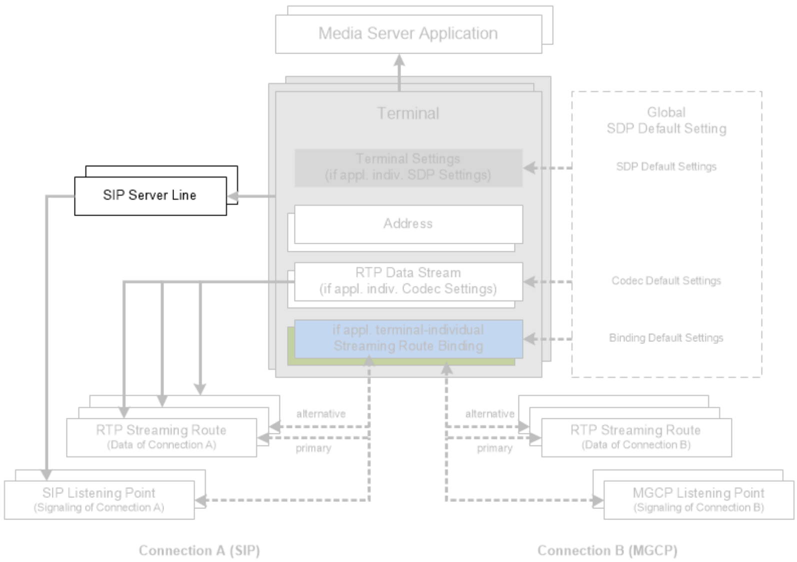
An SIP server line defines the connection settings under which an individual SIP server (e. g. an SIP communications system) can be reached for outbound SIP connection requests.

So that the OpenScape Media Server can still communicate via an SIP server line when the assigned SIP server has failed, you can configure additional alternative SIP servers in every SIP server line.

Any number of SIP server lines can be configured for the OpenScape Media Server. This enables you to connect the OpenScape Media Server to different SIP servers for outbound SIP connections at the same time.

NOTICE:

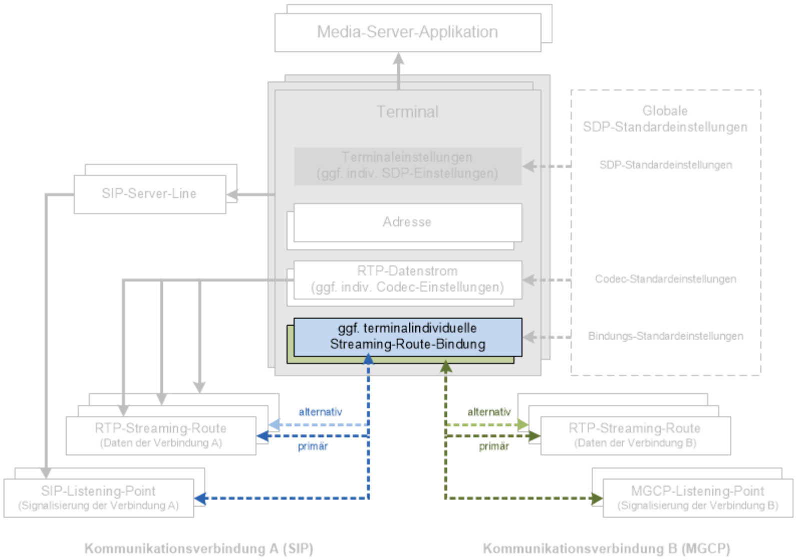
SIP server lines are only used if the OpenScape Media Server is deployed under OpenScape UCApplication.



7.1.8 Streaming Route Binding

A streaming route binding specifies which streaming route the OpenScape Media Server uses to transmit RTP data when the associated connection signaling is handled via a specific listening point.

Using streaming route bindings you can thus control dependently from the listening point which streaming route an RTP data stream uses for transmitting RTP data.



Every streaming route binding combines:

- An SIP or MGCP listening point

> **NOTICE:**
>
> The SIP listening points are not used if the OpenScape Media Server is deployed at OpenScape Voice. In this case the OpenScape Media Server uses MGCP listening points only.

- A primary RTP streaming route
- Optionally an additional alternative RTP streaming route that needs to use an IP address format (IPv4, IPv6) different from the one the primary RTP streaming route uses.

Specifying a primary and an alternative RTP streaming route effects the associated network routes to be offered as possible alternative communication paths to a communication partner. This requires either ICE or ANAT to be active for the OpenScape Media Server.

> **NOTICE:**
>
> You need to specify an alternative streaming route if an RTP data stream is to simultaneously use IPv4- and IPv6-based networks. Thus, if either ICE or ANAT are active.

Terminal-specific streaming route bindings have a higher priority than those valid across the system that you may have configured in the Streaming-IVR provider.

7.1.9 Controlling the Communication Behavior by Configuration Elements

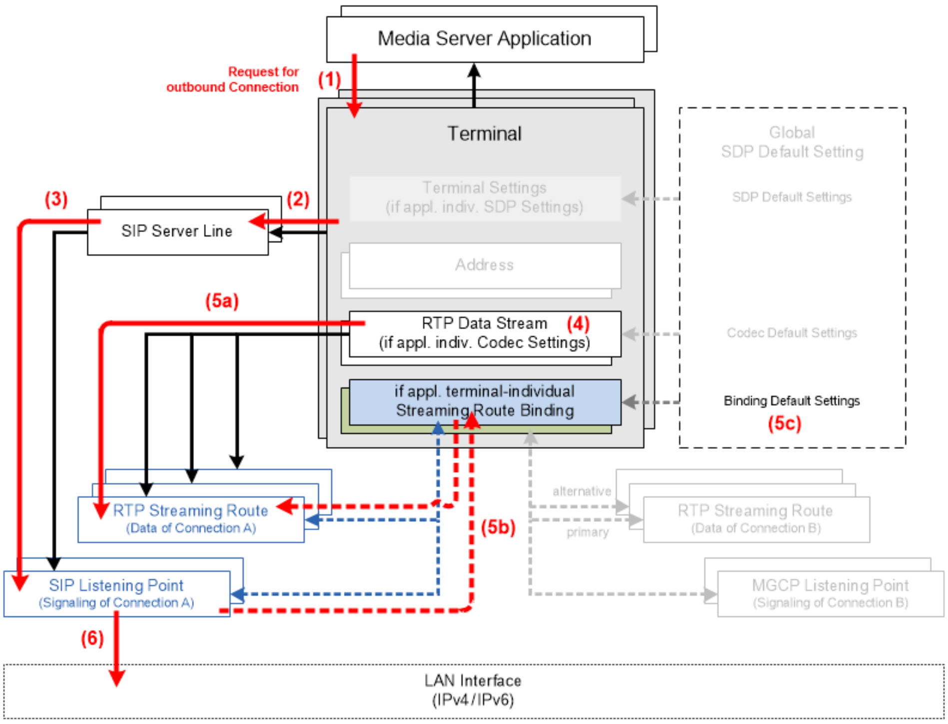
The configuration elements control the OpenScape Media Server communication behavior.

The following two examples show how the OpenScape Media Server sets up out- and inbound communication connections and, in this process, uses the settings of the configuration elements.

Example of an outbound communication connection

The OpenScape Media Server sets up outbound communication connections when a Media Server application attempts to establish a connection to a user phone, for example.

The following figure shows how the OpenScape Media Server sets up such an outbound communication connection.



1) The OpenScape Media Server receives e.g. a request for an outbound SIP-based connection from one of its applications. The application transfers the connection target and the ID of the terminal to be used by the OpenScape Media Server for processing the connection request.
2) The OpenScape Media Server determines from the relevant terminal the SIP server line via which the OpenScape Media Server is to signal the connection request.
3) The OpenScape Media Server determines from the SIP server line the associated listening point and the connection data of the SIP server that is available via the SIP server line.
4) The OpenScape Media Server determines the applicable RTP data streams from the terminal and the demanded media types.

5) The OpenScape Media Server determines the RTP streaming route to be used.

   You can specify the streaming route for transferring RTP data in the following ways. Prioritization decreases from a) to c).

   a) By directly assigning individual streaming routes to a data stream.

      NOTICE:

      Even if several streaming routes are assigned to a data stream, it always uses only one of these streaming routes for transferring data of a specific RTP connection.

   b) By assigning individual streaming route bindings to the terminal. Such streaming route bindings define the streaming route to be used depending on the listening point used.
   c) By configuring global streaming route bindings.

   From the port settings of the RTP streaming route used the OpenScape Media Server determines a valid free port for the RTP communication of the requested connection and reserves it.
6) The OpenScape Media Server determines from the listening point the local IP address and the transport protocol via which the OpenScape Media Server signals the connection request to the defined SIP server.

   Subsequently, the OpenScape Media Server negotiates the connection parameters with the defined SIP server. In doing so, it transfers the already reserved RTP port of the streaming route used. The OpenScape Media Server localizes phone numbers before transmission with the address translation context configured for the SIP server line used.

After the SIP server has confirmed the connection, the OpenScape Media Server signals the connection setup to the Media Server application. In this process, it also transfers the reserved RTP port for the RTP communication of the connection.

The outbound connection is thus set up and the Media Server application can exchange data with the connection target.

Example of an inbound communication connection

The OpenScape Media Server receives inbound connection requests, if e. g. a subscriber attempts to log on to a Media Server application using his/her telephone.

The following figure shows how the OpenScape Media Server sets up such an inbound communication connection.

1) The OpenScape Media Server receives e.g. a request for an inbound SIP connection from an external communications system. This request reaches the OpenScape Media Server via one of its LAN interfaces the inbound communication of which is selectively monitored by SIP listening points.

2) The OpenScape Media Server determines the associated SIP server line from the relevant listening point and the address data of the communications system. Subsequently, the OpenScape Media Server normalizes the phone numbers of the inbound connection request with the address translation context configured for the relevant SIP server line.

3) The OpenScape Media Server evaluates the normalized destination phone number of the SIP connection request and looks for the terminal the address of which corresponds to the destination phone number.

4) The OpenScape Media Server determines the applicable RTP data streams from the terminal and the media types used.

5) The OpenScape Media Server determines the RTP streaming route to be used.

You can specify the streaming route for transferring RTP data in the following ways. Prioritization decreases from a) to c).

a) By directly assigning individual streaming routes to a data stream.

NOTICE:

Even if several streaming routes are assigned to a data stream, it always uses only one of these streaming routes for transferring data of a specific RTP connection.

b) By assigning individual streaming route bindings to the terminal. Such streaming route bindings define the streaming route to be used depending on the listening point used.

c) By configuring global streaming route bindings.

From the port settings of the RTP streaming route used the OpenScape Media Server determines a valid free port for the RTP communication of the requested connection and reserves it.

Based on the reserved port the OpenScape Media Server negotiates the connection parameters.

6) The OpenScape Media Server determines the associated application from the terminal and starts it. In this process the OpenScape Media Server transfers the reserved RTP port for the RTP communication of the connection.

The outbound connection is thus set up and the Media Server application can exchange data with the connection target.

The OpenScape Media Server processes an MGCP connection request in the same way. However, the request would then not be received via an SIP listening point but via an MGCP listening point.

7.2 Application Partitioning

The OpenScape Media Server manages internally various operation-critical system resources that can be proportionally assigned to individual applications.

The operation-critical system resources comprise:

- Conference mixing unit

  The OpenScape Media Server uses a conference mixing unit to interconnect conference participants. For each conference a conference mixing unit is required in the OpenScape Media Server.

- RTP channel

  The OpenScape Media Server uses RTP channels for in and outbound voice and video data. Each RTP channel resource specifies a bidirectional transmission channel.

- Session

  As a rule, OpenScape Media Server manages several sessions for each application. For the speech respectively conference portal this means:

  – One voice portal session for each user logged in at the voice portal.
  – One conference portal session for each user just logging on to the conference portal.
  – One conference portal session for each active conference room.
- Video composer

  The OpenScape Media Server uses a video composer to merge video streams of different video conference participants to a common video image with individual participant screens. A video composer is required in the OpenScape Media Server for every video conference.

You can use the application partitioning of the OpenScape Media Server to proportionately assign these operation-critical system resources to individual applications – e. g. to the user access of the conference portal. In this way it is possible to split up the operation-critical system resources according to their application and to guarantee each application a specific number of operation-critical system resources.

To proportionately assign a system resource to an individual application, you first need to determine how many resources of the relevant type are altogether available. Since the OpenScape Media Server operates software-based, this number of resources is defaulted by the performance of the computer system used. Only the maximum number of configurable RTP channels is automatically restricted by the number of ports of all configured RTP streaming routes.

After the maximum number of a resource type has been determined, the relevant resources can be divided application-individually.

The following resource type names are assigned to the listed system resources in the OpenScape Media Server application partitioning:

- Conference mixing unit – resource type **ConferenceMixingUnit**
- RTP channel – resource type **RTPChannel**
- Session – resource type **Session**
- Video composer – resource type **VideoComposer**

7.3 Consistency Check

The consistency check tests important configuration parameters of the OpenScape Media Server and the resulting functionality of the Media Server components. You can for example determine whether the OpenScape Media Server configuration is consistent or configuration errors restrict the server's system performance.

The consistency check is based on individual test scripts that determine the components and configurations to be checked. The OpenScape Media Server uses test scripts for the following areas:

IP telephony (SIP)

Checks for SIP-based connections of the OpenScape Media Server to communications systems:

- Whether the connected communications systems can be reached via SIP.

- Whether the configured SIP listening points are ready for use.

Streaming (RTP)

Checks for the OpenScape Media Server streaming:

- Whether the streaming server of the OpenScape Media Server has been started and is ready for use.
- Whether the configured streaming routes are ready for use.

Streaming IVR (TTS, ASR, SDP)

Checks for the connection of the OpenScape Media Server to the TTS engine:

- Whether the connected TTS engine can be reached.

Media gateway (MGCP)

Checks for the connection of the OpenScape Media Server to communications systems:

- Whether the connected communications systems can be reached via MGCP.

Node replication

Checks the configuration of the node replication in a Media Server farm.

Internet radio

Checks whether the OpenScape Media Server can connect to the configured Internet radio stations and the current status of each of those connections.

7.4 RTP Monitoring

The OpenScape Media Server uses different mechanisms for monitoring the RTP communication.

Such mechanisms are in particular:

- RTP port monitoring
- ICMP monitoring

RTP Port Monitoring

The OpenScape Media Server uses an RTP port scanner to detect and fend off Denial-of-Service attacks. Using this scanner the OpenScape Media Server searches all officially free RTP ports for suspicious communication in a round-robin process. The suspicious communication may be caused by a client with unusual communication behavior or a Denial-of-Service attacker.

If the RTP port scanner could not detect any suspicious communication on a checked RTP channel, it marks this port as safe and the OpenScape Media Server can use it for its communication. If the RTP port scanner detects suspicious communication on a checked RTP channel, this port is integrated in a black list and not be used by the OpenScape Media Server for a specific period.

The RTP port monitoring is configured by the following expert parameters:

- **rtpBlacklistedTime**
- **rtpScanDuration**

- **rtpScanWindowSize**

These expert parameters apply globally for all RTP streaming routes.

ICMP Monitoring

Network components use the Internet Control Message Protocol (ICMP) to exchange diagnostics data via the internet protocol. A router may return e.g. ICMP messages to a data source if it needs to dismiss packets of this data source.

When the ICMP monitoring of the OpenScape Media Server is active, the OpenScape Media Server reacts to ICMP messages that it receives from the network. If the number of received ICMP messages exceeds a threshold, the Media Server sends appropriate messages to its applications. The applications can react to this by temporarily stopping the send activities or reducing the sent data.

The ICMP monitoring is configured by the following expert parameters:

- **icmpMonitoringEnabled**
- **icmpUnreachableCount**
- **icmpRecoveryTime**

These expert parameters apply individually for each RTP streaming route.

NOTICE:

If the OpenScape Media Server is to use its ICMP monitoring, the components of the network infrastructure must not block ICMP messages.

7.5 Connecting Several SIP Servers

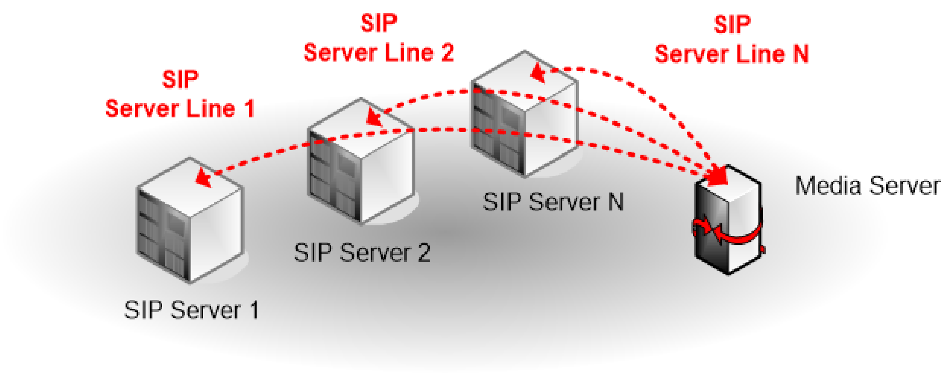
If an OpenScape Media Server is to set up outbound SIP connections, it must be connected to an SIP server (e. g. a communications system) via an SIP server line. You can also use several SIP server lines to connect the OpenScape Media Server to several different SIP servers. The OpenScape Media Server can then use different SIP servers for various communication connections. The terminal via which the communication connection is set up determines which of these servers is concerned in the single case.

NOTICE:

The OpenScape Media Server can only be connected with SIP servers if the OpenScape Media Server is used under OpenScape UCApplication.

IMPORTANT:

The OpenScape Media Server always requires an SIP trunk for communicating with a communications system. If no SIP trunk is used, communication between OpenScape Media Server and the communications system fails.



7.6 Connecting alternative SIP Servers

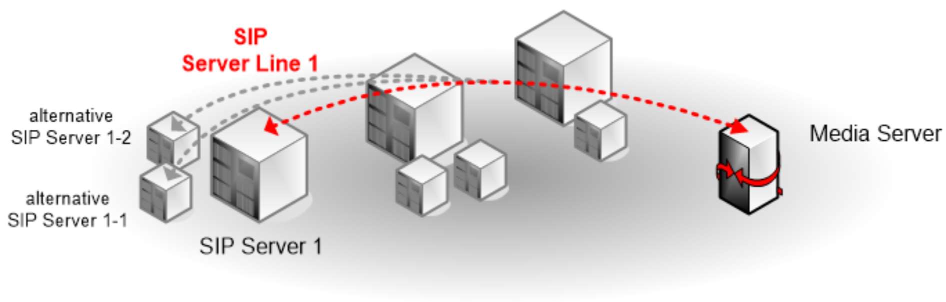
If an OpenScape Media Server is to set up outbound SIP connections, it must be connected to an SIP server (e. g. a communications system) via at least one SIP server line. You can use such an SIP server line to additionally connect the OpenScape Media Server to different alternative SIP servers.

NOTICE:

The OpenScape Media Server can only be connected with SIP servers if the OpenScape Media Server is used under OpenScape UCApplication.

IMPORTANT:

The OpenScape Media Server always requires an SIP trunk for communicating with a communications system. If no SIP trunk is used, communication between OpenScape Media Server and the communications system fails.



In this case the OpenScape Media Server differentiates the SIP connections of an SIP server line as follows:

- Master connection

  Describes the connection to the preferred SIP server of an SIP server line
- Alternative connections

  Describes the connections to every further, alternative SIP server of an SIP server line.

The OpenScape Media Server uses the master connection by default for communicating via an SIP server line. If, however, the preferred SIP server or the connection to this server fails, the OpenScape Media Server communicates via the next alternative connection that is operable for the relevant SIP server line. To determine the availability of all preferred SIP servers, the OpenScape Media Server uses a keep-alive mechanism.

If the preferred SIP server can be reached again later, the OpenScape Media Server can switch back to the master connection. This switch-back can be controlled by two mechanisms:

- Keep-alive mechanism

  The OpenScape Media Server sends by default and in regular intervals a keep-alive request to the preferred SIP server of each SIP server line. Via this mechanism the OpenScape Media Server can determine whether the preferred SIP servers can be reached.

  You can individually configure the send interval for keep-alive requests for each SIP server line via the expert setting **keepAliveRequestInterval** of the SIP provider.
- Timer mechanism

  You can specify a period after which the OpenScape Media Server switches back to the master connection. If, however, the preferred SIP server is not yet available at this time, the OpenScape Media Server communicates via the next alternative connection that is operable for the relevant SIP server line.

  You can configure the period for the switch-back to the master connection via the expert setting **fallbackToMasterSipServerTime** of the SIP provider. This setting applies globally for all SIP server lines. The timer mechanism is deactivated by default.

You need to individually configure the connection settings for alternative SIP servers for each SIP server line.

NOTICE:

You must not configure any alternative SIP servers for the SIP connection to a co-located OpenScape Voice system.
For a geo-separated system, you may configure only a single alternative SIP server. In this case, the master connection to the SIP service manager (SIPSM) must lead from node 1 and the alternative connection to the SIP service manager (SIPSM) from node 2.

7.7 Transfer Conference

Using the transfer conference the OpenScape Media Server can set up a conference from an active call with two subscribers. More participants can be added to this conference (Merge Calls feature of OpenScape UCApplication). For this type of conference the OpenScape Media Server does not use the terminal-device-controlled conference feature of OpenScape Voice but the conference portal of OpenScape UCApplication.

NOTICE:

In the OpenScape Media Server the transfer conference is only available if the OpenScape Media Server is used under OpenScape UCApplication. OpenScape UCApplication must use OpenScape Voice as communications system.

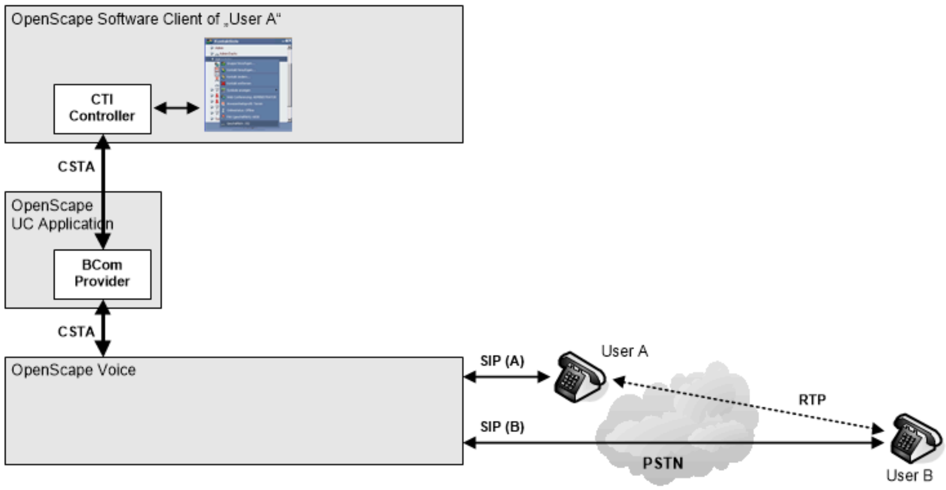
NOTICE:

The LocalParkSlot application must have been installed in the OpenScape Media Server for the transfer conference. This application is currently automatically installed with the RPM packet BCOM .

NOTICE:

So that a user can deploy this conference feature of the OpenScape Media Server, the **second call** feature must have been configured for the user terminal device.

The following figures show how such a transfer conference operates.

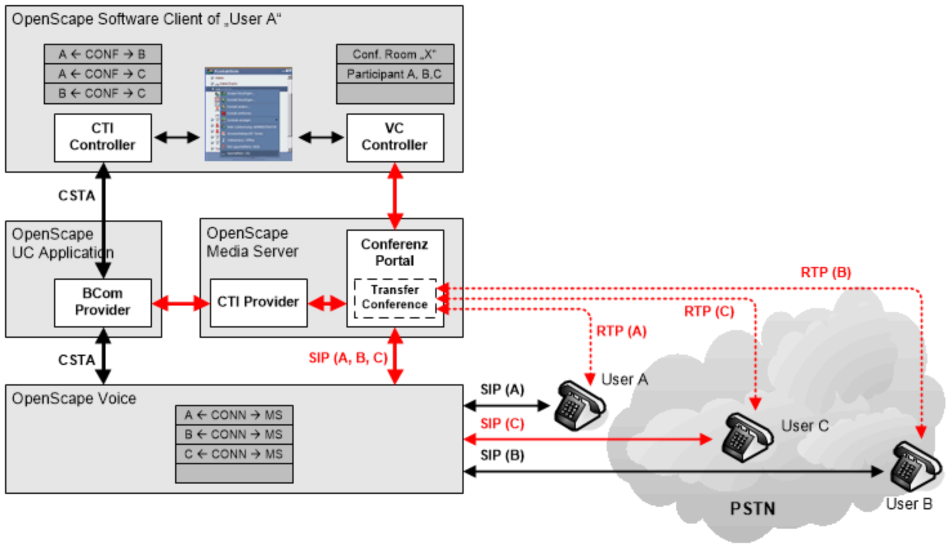


The transfer conference mechanism starts with a simple telephone connection and two subscribers who are connected via OpenScape Voice. In this scenario the SIP signaling of the phone connection leads via OpenScape Voice. The RTP-based payload is directly exchanged between the telephones.

In the depicted example, one of the two subscribers is an OpenScape user A who can control his/her telephone via a software client. To this, the software client communicates via its CTI controller and the CSTA protocol with the BCom provider of the OpenScape UCApplication. The BCom provider also communicates via CSTA with OpenScape Voice and controls in particular the telephone of user A.

The second subscriber to the phone connection is e.g. an external subscriber.

Based on the existing phone connection and via the GUI of his/her software client user A can initiate an ad-hoc conference to integrate a new subscriber in the existing connection. The following happens:



1) The BCom provider of the OpenScape server cuts the connection between the subscribers A and B in OpenScape Voice and connects the two resulting connection fragments to a new transfer conference in the conference portal. To this, the BCom provider controls OpenScape Voice via appropriate CTI commands.

2) At the same time, the BCom provider transfers all information about the rerouted connections and their subscribers to the CTI provider of the OpenScape Media Server. This provider then forwards this information to the conference portal. In this way the conference portal can determine which of the newly arriving calls are to be routed into a common transfer conference. Furthermore, the conference portal is thus enabled to suppress default announcements of the portal for the relevant users.

3) Besides the subscribers A and B, also the new conference participant is added to the transfer conference.

Eventually, all users are in a common transfer conference of the conference portal. In this scenario the SIP signaling of the phone connection leads via OpenScape Voice to the conference portal. The RTP-based payload is processed by a conference mixer of the OpenScape Media Server.

After the users have been connected in the transfer conference of the conference portal, this conference can be controlled via the Conferencing Interface of the software client.

The available information about the state of the different connections differ in the system components involved.

- In OpenScape Voice the participating connections are registered as CONNECTED. OpenScape Voice does not know that such connections are conference connections.
- In the CTI controller of the software client the connections are registered as CONFERENCED. The CTI controller receives the additional information about the conference state from the BCom provider, which has received it from the CTI provider of the OpenScape Media Server.
- In the Conferencing Interface of the software client all users are registered as subscribers to a common conference. The Conferencing Interface receives this comprehensive information directly from the OpenScape Media Server conference portal.

7.8 Media Server Farm

If required, you can operate several OpenScape Media Servers in a Media Server farm.

7.8.1 Media Server Farm at OpenScape Voice

If the performance levels of a single OpenScape Media Server do not comply with the desired performance or redundancy requirements, you can operate several OpenScape Media Servers in the form of a Media Server farm at OpenScape Voice.

OpenScape Voice distributes in this case the load among the various OpenScape Media Servers.

In a Media Server farm the same Media Server components must be installed on all computer systems of the OpenScape Media Server.

7.8.2 Media Server Farm under OpenScape UCApplication

If the performance levels of a single OpenScape Media Server do not comply with the desired performance or redundancy requirements, you can operate up to four OpenScape Media Servers in the form of a Media Server farm under OpenScape UCApplication.

OpenScape Voice distributes in this case the load among the various OpenScape Media Servers.

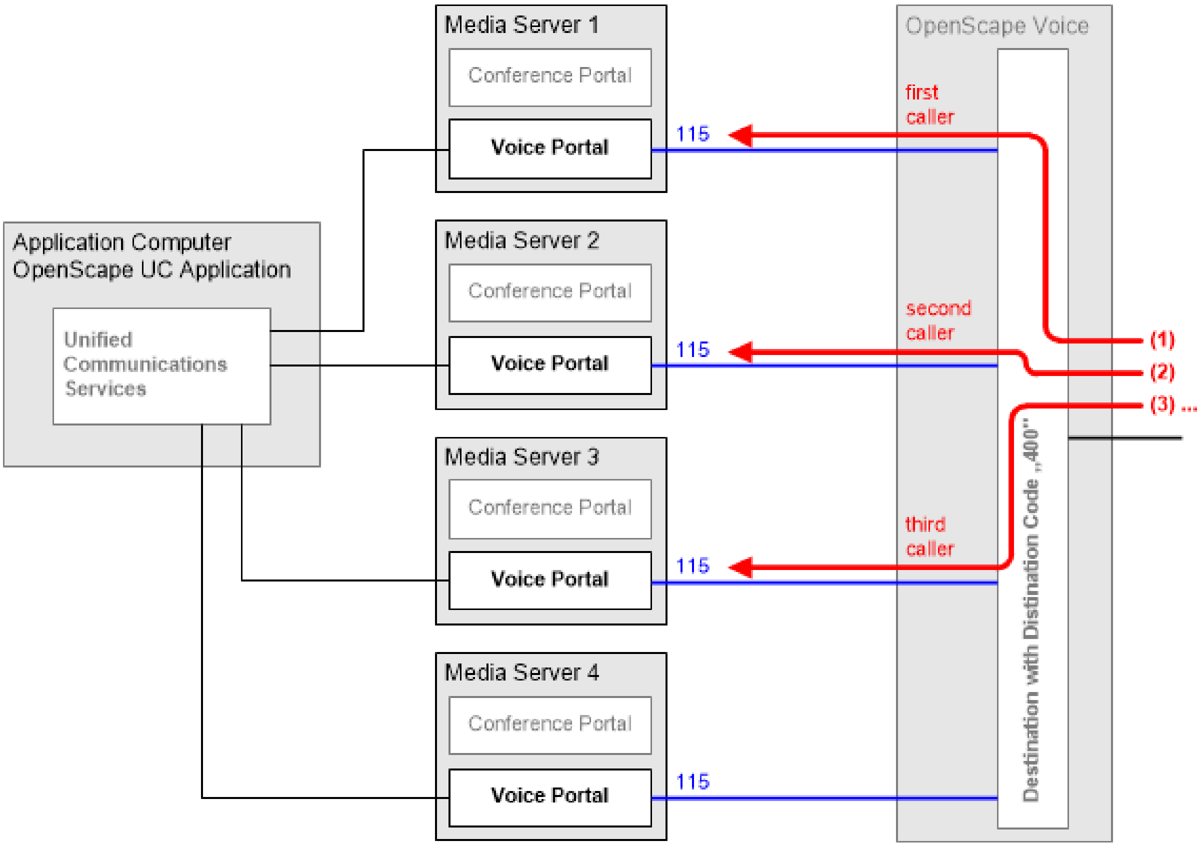
In a Media Server farm the same Media Server components must be installed on all computer systems of the OpenScape Media Server.

7.8.2.1 Voice Portal in a Media Server Farm

NOTICE:

If you use a Media Server farm you should configure all other OpenScape Media Servers on each OpenScape Media Server of the Media Server farm for announcement replication.

The following figure provides an overview of the voice portal working in a Media Server farm. To improve clarity we now take a look at an access mode– e. g. the guest access.



In OpenScape Voice you need to configure a destination that contains in total as many routes as OpenScape Media Servers exist. Each of these routes must have an individual OpenScape Media Server as endpoint.

A network code must be configured for the destination– e. g. 400. All calls arriving with this network code are distributed among the different OpenScape Media Servers by the destination and its routes.

A common access number – e. g. 115 – must be configured for the guest accesses of the different OpenScape Media Server.

Via such accesses the voice portal then provides the caller with a TUI via which the Unified Communications services of the connected OpenScape server are to be controlled in the guest mode.

A call is processed by the voice portal to which it was routed by the OpenScape Voice destination.

You can use the already configured OpenScape Voice destination for the user access. In the various OpenScape Media Servers you only need to configure an additional common access number– e. g. 116.

7.8.2.2 Conference Portal in a Media Server Farm

In OpenScape Voice you need to configure a destination that contains in total as many routes as OpenScape Media Servers exist. Each of these routes must have an individual OpenScape Media Server as endpoint.

A network code must be configured for the destination– e. g. 400. All calls arriving with this network code are distributed among the different OpenScape Media Servers by the destination and its routes.

Furthermore, an additional destination must be configured for each OpenScape Media Server, via which only the individual OpenScape Media Server can be reached.

The following access numbers must be configured for the conference portal of the different OpenScape Media Servers:

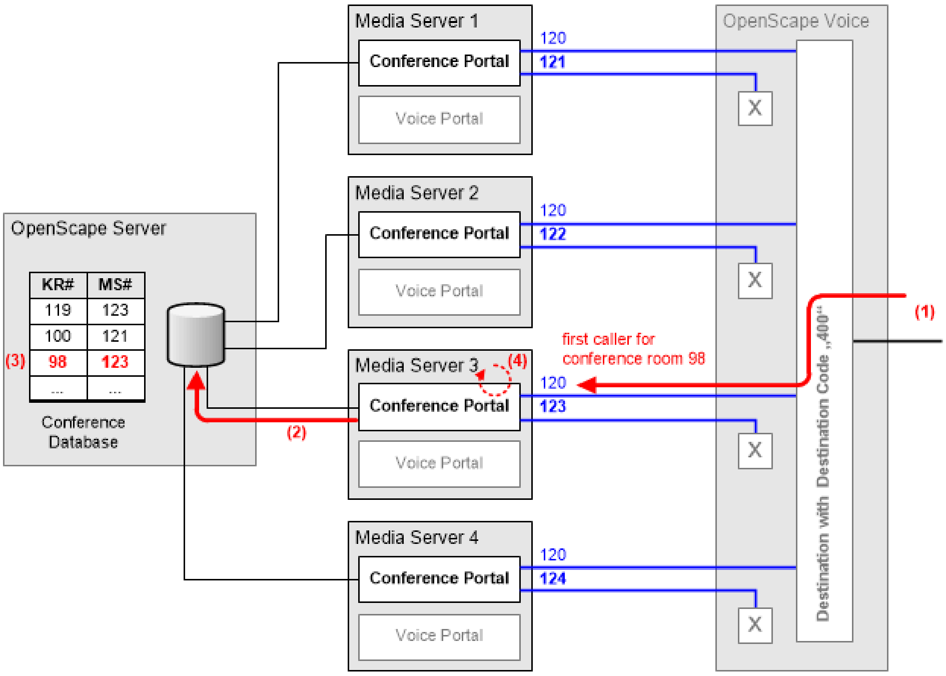
- One access number that is the same for all OpenScape Media Server– e. g. 120
- One access number that is individual for each OpenScape Media Server– e. g. 121 to 124.

After a call was routed to an OpenScape Media Server, the behavior of the conference portal application differs in the following two cases:

- First caller for a conference room
- Further callers for a conference room

First caller for a conference room

The following figure provides an overview of how the conference portal operates in a Media Server farm when the first call for a conference room comes in.



1) The call that comes in for the conference portal is routed by the destination in OpenScape Voice to one of the available OpenScape Media Servers.

The conference portal of the relevant OpenScape Media Server accepts the call and asks the caller for the conference room number to which he/she wants to be connected.

2) If the desired conference room in the conference portal of the relevant OpenScape Media Server has not been started yet, the conference portal determines via a centrally administered conference database whether the desired conference room has already been started in another conference portal of the Media Server farm.

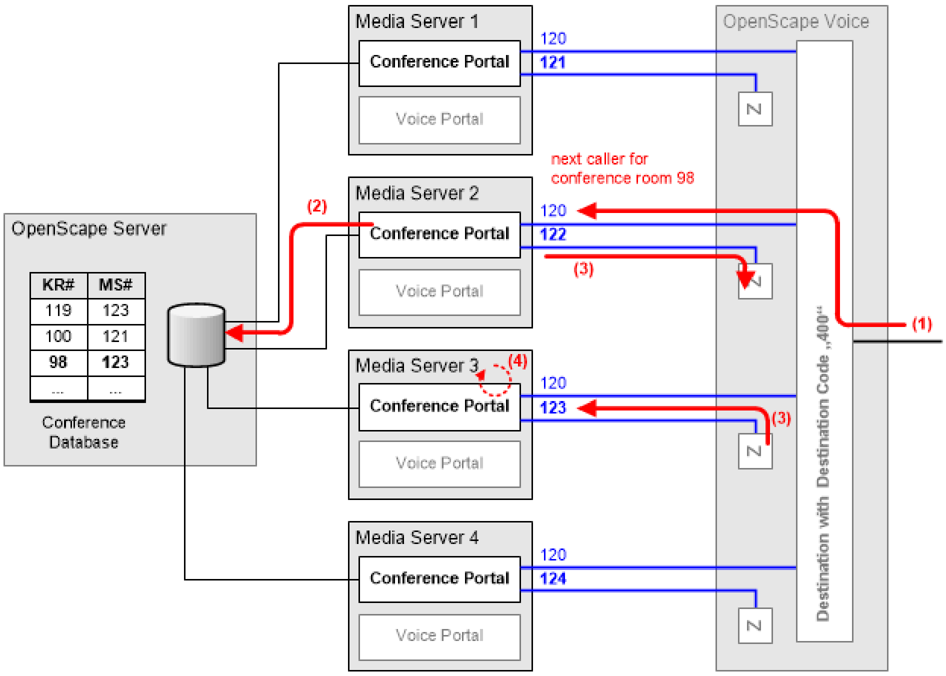
But since the call is made by the first caller for conference room 98, this is not the case.

3) The conference portal adds a new entry to the conference database for conference room 98, which references the individual phone number for Media Server 3.

4) The conference portal of the relevant OpenScape Media Server starts the new conference room and connects it to the inbound caller.

Further callers for a conference room

The following figure provides an overview of how the conference portal operates in a Media Server farm when further calls for a conference room come in.



1) The call that comes in for the conference portal is routed by the destination in OpenScape Voice to one of the available OpenScape Media Servers.

The conference portal of the relevant OpenScape Media Server accepts the call and asks the caller for the conference room number to which he/she wants to be connected.

2) If the desired conference room in the conference portal of the relevant OpenScape Media Server has been started, the conference portal connects it to the inbound caller.

Otherwise, the conference portal will investigate via a centrally administered conference database whether the desired conference room has already been started in another conference portal of the Media Server farm.

In our example, conference room 98 has been started on the OpenScape Media Server with phone number 123.

3) The conference portal of Media Server 2 reroutes the incoming call to phone number 123, thus to the conference portal of Media Server3.

> **NOTICE:**
>
> Media Server 2 transfers various information with the call to Media Server 3 – among other things the number of the requested conference room. It uses the Call Attached Data (CAD) feature, which can be used to transfer data via a phone connection.
>
> So that OpenScape Voice lets this information pass, the **Allow Sending of Insecure Referred-By Header** option must be activated in OpenScape Voice for all Media Server endpoints.

4) The conference portal of Media Server 3 picks up the incoming call and connects the inbound caller with conference room 98 without asking the caller for his/her desired conference room.

7.8.2.3 Conference Portal in an Integrated Deployment with External Media Server

In OpenScape Voice you need to configure a destination that contains in total as many routes as the number of OpenScape Media Servers. Each of these routes must have an individual OpenScape Media Server as endpoint.

A network code must be configured for the destination– e. g. 400. All calls arriving with this network code are distributed among the different OpenScape Media Servers by the destination and its routes.

Furthermore, an additional destination must be configured for each OpenScape Media Server, via which only the individual OpenScape Media Server can be reached.

The following access numbers must be configured for the conference portal of the different OpenScape Media Servers:

- One access number that is the same for all OpenScape Media Servermedia servers– e. g. 120
- One access number that is individual for each media server – e. g. 121 for the Integrated Media Server (handling the audio streaming) and 122 for the External Media Server (handling the video streaming).

The call distribution depends on whether the conference is audio or video:

1) The call comes in via the common bridge number:
   - The user joins an audio only conference: The call is handled by the Integrated Media Server.
   - The user joins a video conference: The call is handled by the External Media Server.
2) The call comes in via the individual Integrated Media Server number:
   - The user joins an audio only conference: The call is handled by the the Internal Media Server.
   - The user joins user joins a video conference: The call is rerouted to the Integrated Media Server.
3) The call comes in via the individual External Media Server number:

1) • The user joins an audio only conference: The call is rerouted to the Internal Media Server.
   • The user joins user joins a video conference: The call is handled by the Integrated Media Server.
2) A UC video conference is started. The video conference is handled by the External Media Server.
3) A UC audio conference is started. The audio conference is handled by the Integrated Media Server.

7.8.2.4 Node Replication in a Media Server Farm

Using a replication mechanism you can make customized welcome and name announcements of the voice portal automatically available on every OpenScape Media Server of a Media Server farm.

OpenScape users may configure an individual welcome and name announcement for the voice portal. In doing so they customize these announcements always only on the OpenScape Media Server the voice portal of which they are currently logged in to. If you use OpenScape UCApplication with a Media Server farm, all other OpenScape Media Servers of the farm use the original version of the announcements.

The node replication of the OpenScape Media Server replicates modified voice portal announcements automatically to all other OpenScape Media Servers of a Media Server farm. All OpenScape Media Servers of the Media Server farm use automatically the customized announcements then.

NOTICE:

If you use a Media Server farm you should configure all other OpenScape Media Servers on each OpenScape Media Server of the Media Server farm for node replication.

7.9 Importing Customized Applications

The deployment interface of the OpenScape Media Server enables adding applications or updating existing ones in the OpenScape Media Server at runtime. This refers in particular to applications that were created using the Application Builder, but also customized announcements can be imported in the OpenScape Media Server in this way.

A so-called deployment file of an application is required for adding this application or updating it in the OpenScape Media Server. This deployment file is a zip-file with the extension `.mdp.zip`. It contains all required data of the relevant application.

If you import a deployment file into the OpenScape Media Server, the relevant file is unpacked in the following deployment directory of the OpenScape Media Server:

<MS#Install [22]>`/mediaserver/application_host/deployment-custom`

22 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

The deployment manager of the OpenScape Media Server monitors the deployment directory and copies all newly imported files into the following working directory of the OpenScape Media Server.

<MS#Install >`/mediaserver/application_host/work`

In doing so, the deployment manager assigns the data an individual version number to avoid conflicts with other available versions. That way the OpenScape Media Server also ensures that the entities of an older application version are shut down duly before the OpenScape Media Server deletes the old application files and activates the new ones.

The OpenScape Media Server executes the relevant application from the working directory.

If a deployment file is removed from the `deployment-custom` directory again after its import, the OpenScape Media Server deletes it thereafter automatically from the working directory `work` also.

7.10 Tones and System Announcements for OpenScape Voice

The task of the OpenScape Media Server is to generate the tones and announcements used by OpenScape Voice and to transfer them to the corresponding terminals. The OpenScape Media Server can provide tones and announcements for every country released for the OpenScape Voice.

7.10.1 Tones for OpenScape Voice

An essential function of the OpenScape Media Server is to provide tones the OpenScape Voice system has to play at its terminals. Tones are country-specific. In every country, individual requirements on tone frequency, tone duration and pause intervals between single tone fractions apply for tones.

Each tone is realized by an audio file. Several tone frequencies of different playback length with specific pause intervals can be combined in such a file.

Which tones the OpenScape Media Server can play may depend on the relevant entities. In this case the entities signal the OpenScape Media Server to play specific tones only if required – for example:

- Subscriber endpoints

  The OpenScape Media Server plays simple telephone tones only if the signaling indicates that the endpoint cannot do this by itself. Examples of such tones are ringback tone, dial tone, busy tone or call-waiting tone.
- Remote gateways

  The OpenScape Media Server plays network tones only if the signaling indicates that the remote gateway cannot do this by itself. An example of this is the network busy tone indicating that calls via network are currently not possible.

For another, the OpenScape Media Server is always in charge of playing specific tones – for example:

- When an error occurs, like a subscriber dialing an invalid phone number, and the terminal device sounds a specific tone to indicate this.

- When a person joins or leaves a conference and this is indicated to the other participants by a signal tone.

7.10.2 System Announcements for OpenScape Voice

An essential function of the OpenScape Media Server is to provide system announcements that the OpenScape Voice system has to play at its terminals.

NOTICE:

The system announcements described here are independent from those that the OpenScape Media Server manages for the voice and conference portal of OpenScape UCApplication.

An OpenScape Voice system announcement consists of at least one audio segment played to a subscriber. Besides audio segments you can perform additional system announcement settings in OpenScape Voice – e. g. how often an audio segment shall be played to a subscriber or the playback pause between audio segments.

OpenScape Voice requests the OpenScape Media Server to play system announcements appropriate for selected events or conditions. These requests comprise information about the files of the audio segments to be played and the relevant target subscriber.

The OpenScape Media Server is shipped with the default system announcements of OpenScape Voice already. They can be administered in the OpenScape Media Server if required. Furthermore, the system administrator can create and administer system announcements specific to customers.

The OpenScape Media Server provides a so-called Basic Announcement Unit set (BAU set) for every supported language. If required, these BAU sets are used for system announcement playback and contain the following as a rule:

- Cardinals
- Ordinals
- Date and time specifications
- Names for weekdays and months
- Currency names
- Commonly used words – e. g. and, the

You can divide the system announcements of a Media Server in the following main categories:

- Intercept announcements
- Interactive announcements

Intercept Announcements

Using intercept announcements, OpenScape Voice reacts in particular to dropped calls. This enables OpenScape Voice to create error or other messages played to a subscriber when he/she dials a specific phone number.

Intercept announcements can be grouped as follows:

- System announcements with fixed content – e. g. *The subscriber you have dialed is currently unavailable. Please hang up and try again later.*

- System announcements with variable content contain at least one individual parameter – e. g. *The phone number 321-9876 you have dialed has changed. The new phone number is 321-6789.*

An intercept announcement of OpenScape Voice can consist of up to three tones, system announcements or a combination of these, which are all controlled by OpenScape Voice. After OpenScape Voice has requested the OpenScape Media Server to play the system announcement, the Media Server performs all necessary activities independently.

NOTICE:

The restriction on three tones, system announcements or a combination of these is determined by the OpenScape Voice system.

Interactive Announcements

Interactive announcements assume caller action – e. g. operating telephone keys to generate DTMF tones or speaking voice commands (IVR). Example: *The phone number 321-9876 you have dialed has changed. The new phone number is 321-6789. If you wish to be connected to the new phone number, please press 1.*

How OpenScape Voice then handles the call depends on the caller's reaction to the system announcement.

7.10.3 Internal Management of Tones and System Announcements of OpenScape Voice

The task of the OpenScape Media Server is to generate the tones and announcements used by OpenScape Voice and to transfer them to the corresponding terminals. The OpenScape Media Server can provide tones and announcements for every country released for the OpenScape Voice.

NOTICE:

The languages listed here do not describe the language support of the applications executed by the OpenScape Media Server under OpenScape UCApplication.

So that the OpenScape Media Server can play tones and system announcements of a specific country, the associated language package must be installed on the OpenScape Media Server. Such a language package contains the following:

- All country-specific tones of the relevant country
- The country-specific system announcements as far as they are available for the corresponding country.

If a language package does not contain all country-specific announcements, the language package of another country must be installed to supplement the missing announcements.

The following table shows which language packages must at least be installed to use the OpenScape Media Server for a specific country.

Table 2: Language packages in the OpenScape Media Server

Country	Codes of the language packages to be installed	
Argentina	es_ar	
Australia	en_au	en
Belgium	nl_be	
Bosnia and Herzegovina	bs	sr
Brazil	pt_br	
Bulgaria	bg	
Chile	es_cl	es_mx
China	zh	
Denmark	da	
Germany	de	
Ecuador	es_ec	es_mx
Estonia	et	
Finland	fi	
France	fr	
Greece	el	
Great Britain / Ireland	en	
Hong Kong	zh_hk	en_us
India	en_in	en
Indonesia	ID	en_us
Ireland	en_ie	en
Italy	it	
Japan	japanese – do not modify!!!	en_us
Canada	fr_ca	
Colombia	es_co	es_mx
Korea	ko	en_us
Croatia	hr	
Latvia	lv	
Lithuania	lt	en
Malaysia	MS	en_us
Morocco	fr_ma	fr
Mexico	es_mx	
Netherlands	nl	
Norway	no	

Country	Codes of the language packages to be installed	
Austria	de_at	de
Peru	es_pe	es_mx
Philippines	en_ph	en_us
Poland	pl	
Portugal	pt	
Romania	ro	
Russia	ru	
Sweden	sv for Sweden – do not modify!!!	
Serbia	sr	
Singapore	zh_sg	en_us
Slovakia	sk	
Slovenia	sl	
South Africa	en_za	en
Spain	es	
Spain (Catalan)	ca	
Taiwan	zh_tw	en_us
Thailand	th	en_us
Czech Republic	cs	
Turkey	tr	
Hungary	hu	
USA	en_us	
United Arab Emirates	ar	
Venezuela	es_ve	es_mx
Vietnam	vi	en_us

To enable the OpenScape Media Server playing a system announcement or tone, the OpenScape Voice must transfer to it the ID of the language for which the system announcement or tone is to be played. OpenScape Voice supports currently no locale IDs, but only language IDs. Therefore, OpenScape Voice cannot prompt the OpenScape Media Server to play an announcement in a sublanguage– e. g. in Brazilian, which is sublanguage of the basic language Portuguese.

To support sublanguages just the same, the OpenScape Media Server enables their playback internally. Within this scope the following mechanisms are important:

- Preferring a language package
- Fallback to an alternative language package

You can install the language packages for different OpenScape Voice language IDs to enable the OpenScape Media Server to play the tones and announcements of different countries simultaneously. In doing so, you can use always only the basic language or one of the associated sublanguages for each OpenScape Voice language ID, though.

Consequently, you can use the OpenScape Media Server for the languages German (Germany) and Spanish (Spain) simultaneously. In contrast, it can not be used for the languages Spanish (Mexico) and Spanish (Argentina) at the same time.

Preferring a language package

If several language packages are installed for one OpenScape Voice language ID in the OpenScape Media Server, the OpenScape Media Server determines internally which of these language packages to use for this OpenScape Voice language ID.

If required, you can manually control the preference of a language package for an OpenScape Voice language ID. The expert setting **preferredLanguages** is used for this purpose.

How the OpenScape Media Server prefers language packages by default:

- If only one language package is installed of an OpenScape Voice language ID, the OpenScape Media Server uses this language package.
- If language packages of the basic language and of the sublanguages are installed for an OpenScape Voice language ID, the OpenScape Media Server uses the package of the basic language.

  If you want the package of a sublanguage to be preferred, you need to configure this preference via **preferredLanguages**.
- If only language packages of several sublanguages are installed for an OpenScape Voice language ID, you need to configure via **preferredLanguages** which of these the OpenScape Media Server is to prefer.

The following table summarizes this behavior.

Installed language packages of the OpenScape Media Server			**Preferred language package**
Basic language for language ID	**Sublanguage for language ID**	**Basic language / sublanguage for language ID**	
installed	none installed	arbitrary installed	Basic language for language ID
	one / several installed		Basic language for language ID or preferred sublanguage for language ID
not installed	one installed		Sublanguage for language ID

Installed language packages of the OpenScape Media Server			Preferred language package
Basic language for language ID	Sublanguage for language ID	Basic language / sublanguage for language ID	
	several installed		preferred sublanguage for language ID [23]

Fallback to an alternative language package

If a language package does not contain all country-specific announcements of the relevant country, the OpenScape Media Server uses an internal fallback mechanism to determine, from which alternative language package the missing announcements shall be played.

If required, you can manually control the OpenScape Media Server's falling back to an alternative language package. The expert setting **fallbackLanguages** is used for this purpose.

How the fallback mechanism behaves by default:

- If the language packages of the basic language and of at least one associated sublanguage are installed for an OpenScape Voice language ID, the OpenScape Media Server uses the package of the basic language as alternative language package.

  If you want the package of another sublanguage to be used instead, you need to configure the relevant language package as alternative language package via **fallbackLanguages**.
- If no language package of a basic language but at least two language packages of any sublanguages are installed for an OpenScape Voice language ID, you need to configure via **fallbackLanguages** which of these packages the OpenScape Media Server is to use as alternative.

  NOTICE:

  After the OpenScape Media Server setup, useful presettings are already configured for alternative language packages.
- If the language packages of a basic language and at least another language package not associated to the basic language are installed for an OpenScape Voice language ID, you need to configure via **fallbackLanguages** which of these packages the OpenScape Media Server is to use as alternative.

The following table summarizes this behavior in combination with the preference of language packages.

[23] In this case you need to configure via **preferredLanguages** which language package the OpenScape Media Server is to prefer.

Installed language packages of the OpenScape Media Server			Preferred language package	Alternative language package
Basic language for language ID	Sublanguage for language ID	Basic language / sublanguage for language ID		
installed	none installed	none installed	Basic language for language ID	–
		one / several installed	Basic language for language ID	Fallback configuration
	one / several installed	arbitrary installed	Basic language for language ID	Fallback configuration
			preferred sublanguage for language ID	Basic language for language ID
				Fallback configuration
not installed	one installed	none installed	Sublanguage for language ID	–
		one / several installed	Sublanguage for language ID	Fallback configuration
	several installed	arbitrary installed	preferred sublanguage for language ID	Fallback configuration

7.11 Participant-Controlled Conferences (Large Conference)

Participant-controlled conferences allow OpenScape Voice users to set up a conference with several participants at selected OpenScape Voice terminal devices. The OpenScape Media Server takes on mixing the media streams for such participant-controlled conferences. If required, it also takes on their transcoding – e. g. from G.729 to G.711. This transcoding ensures that conference participants hear each other even if the involved terminal devices use different codecs for the media streams.

7.12 Phone Number Handling

The OpenScape Media Server and its applications generally process phone numbers internally in the so-called normalized phone format – example:

+492404901100. A phone number in this format is either globally unique and based on the Global Number Format (GNF, E.164-based), or it has a private normalized format.

Processing a phone number exclusively in the normalized format has the following advantages:

- The phone number contains all information that uniquely identifies it. This enables optimum phone number evaluation.
- All components of the OpenScape Media Server can operate with a clearly defined phone number format which simplifies exchanging phone numbers within the Media Server.

If the OpenScape Media Server or one of its applications receives a non-normalized phone number, the relevant component uses an algorithm to normalize this phone number before its further processing. If a normalized phone number is to be transferred to an external system or played to a user, a similar algorithm is used to convert this phone number in a format that the relevant external system or a user deploys. This process is called localization.

Besides the actual phone number, the algorithms for phone number normalization or localization require further information about the context in which the phone number exists. Two types of context can be differentiated here.

- User-related contexts

  The algorithms for phone number normalization or localization deploy a user-related context in the following cases:

  – When a user transfers a phone number to the OpenScape system and this phone number needs to be normalized for further processing.
  – When the OpenScape system puts out a normalized phone number to a user in a user-friendly format.

  The settings of a user-related context result automatically from the settings of the relevant user.

  Phone number normalizations or localizations based on user-friendly contexts are performed e. g. by OpenScape Media Server applications like the voice portal.
- Server-related contexts

  The algorithms for phone number normalization or localization deploy a server-related context in the following cases:

  – When an external system transfers a phone number to the OpenScape system and this phone number needs to be normalized for further processing.
  – When the OpenScape system transfers a normalized phone number to an external system but this system does not expect a normalized but an individual phone number format.

  Such a system may be e. g. OpenScape Voice.

  The settings of a server-related context result from a system-wide valid address translation context that needs to be configured manually in the CMP. You can configure any number of such address translation contexts in the CMP.

  Phone number normalizations or localizations based on server-related contexts are performed by the SIP provider in case of the OpenScape Media Server.

7.13 Communications Assistance for Law Enforcement Act

The OpenScape Media Server can monitor the OpenScape Voice telephone connections according to the Communications Assistance for Law Enforcement Act / Lawful Intercept (CALEA / LI). It uses so-called monitoring endpoints automatically connected to the communicating subscribers for this purpose.

7.14 Trusted Transfer Mode

The Trusted Transfer Mode enables connecting the PhoneMail application of XPR servers with OpenScape UCApplication. Such a connection extends the Unified Messaging features of the PhoneMail application by the Unified Communications features of OpenScape UCApplication. If an XPR server is connected with OpenScape UCApplication via the Trusted Transfer Mode, the Unified Communications features of OpenScape UCApplication integrate in the PhoneMail user menu of the XPR server. The XPR user will not realize whether a selected feature is enabled by the XPR server or by OpenScape UCApplication. He/she will receive the impression as if working with a Unified Communications system centrally providing all available Unified Communications features.

Detailed information about the Trusted Transfer Mode is available in the manual *OpenScape UCApplication, Configuration and Administration, Administrator Documentation*.

7.15 Dual Video

During an active video-conference call, dual video capable devices (from Tandberg, Lifesize and Polycom) allow setting up a second video stream for different content, such as desktop sharing or presentation slides. Dual video requires the implementation of the Binary Floor Control Protocol (BFCP). To achieve dual video streaming on SIP/SDP level, the systems offer two video m-lines where one m-line is tagged with a media attribute "content:main" and the other with "content:slides".The presentation media stream is idle after connection establishment although it is NOT signaled with the "a=inactive" SDP direction attribute but with the "a=sendrecv". The SDP direction attribute is not used to steer the presentation streaming.
Dual video capable devices can show both streams (two Video-RTP streams) at the same time and the mixed MCU-picture stream, as well as the presentation stream. Single video capable devices provide the functionality of switching between the two provided streams.

8 Installing, Upgrading and Uninstalling the OpenScape Media Server

You can use the OpenScape Media Server at OpenScape Voice or under OpenScape UCApplication. The ways of setting up, upgrading or uninstalling the OpenScape Media Server in these environments vary accordingly.

8.1 Installing, Upgrading and Uninstalling the OpenScape Media Server at OpenScape Voice

To install, upgrade or uninstall an OpenScape Media Server for one of the possible operating modes at OpenScape Voice you need to use the setup processes of OpenScape Voice.

You find details about this in the manual *OpenScape Voice, Service Manual: Installation and Upgrades*.

Furthermore, you may have to manually install a language package of OpenScape Voice system announcements for the OpenScape Media Server.

8.1.1 How to Install a Language Package for OpenScape Voice System Announcements

If you wish to use OpenScape Voice system announcements with the OpenScape Media Server in a language the language package of which has not been installed yet, you must install this package manually. If the language package to be installed requires a fallback language, you must install the language package of this fallback language, if it is not present yet, also.

Prerequisites

The OpenScape Media Server has been installed on an individual computer system independently from OpenScape Voice.

> **NOTICE:**
>
> If the OpenScape Media Server has been set up on the same computer system as OpenScape Voice, the following manual describes how to install an additional language package retrospectively.
>
> *OpenScape Voice, Service Manual: Installation and Upgrade*

You are logged in at the computer system of the OpenScape Media Server as user *root*.

Step by Step

1) Stop the OpenScape Media Server with the following command:

```
/etc/init.d/symphoniad stop
```

2) Store at least the following repository ISO files in any directory on the computer system of the OpenScape Media Server:

- – `OpenScapeUcSuiteApps-Repository.iso`
- – `OpenScapeUcSuiteApps-BasePackage.iso`
- – All language ISO files

3) Execute a command of the following format on the computer system of the OpenScape Media Server to create in *osc-setup* a repository for all ISO files from step 2:

```
osc-setup cr -b <path to the ISO file>/OpenScapeUcSuiteApps-Repository-
<version>.iso
```

IMPORTANT:

This command creates a temporary, local repository. This repository gets lost when the ISO files used are deleted or moved or when the computer system is rebooted.

Example:

```
osc-setup cr -b /software/osuca/OpenScapeUcSuiteApps-Repository-<-version>.iso
```

4) Execute the following command on the computer system of the OpenScape Media Server to check which language packages have already been installed:

`osc-setup se mediaserver_announcements`

Example output:

```
S  ...
   | Name                                  | Summary                          | Type
--                                         +----------------------------------+----------
   +-------------------------------------
   ...                                     | mediaserver_announcements_ar     | package
i  | mediaserver_announcements_ar          | mediaserver_announcements_bg     | package
   | mediaserver_announcements_bg          | mediaserver_announcements_ca     | package
   | mediaserver_announcements_ca          | mediaserver_announcements_cs     | package
   | mediaserver_announcements_cs          | mediaserver_announcements_da     | package
   | mediaserver_announcements_da          | mediaserver_announcements_de     | package
   | mediaserver_announcements_de          |                                  | package
   |                                       mediaserver_announcements_de_at
   mediaserver_announcements_de_at
   ...
```

A package is installed on the computer system if column **S** displays an **i**.

5) Execute a command in the following format to install a new language package for the OpenScape Media Server:

```
osc-setup in mediaserver_announcements_<language token>
```

Example of the Spanish language package:

```
osc-setup in mediaserver_announcements_es_es
```

If you wish to install several language packages, use a command of the following format:

```
osc-setup in <package 1> <package 2> ... <package n>
```

6) Execute the following command on the computer system of the OpenScape Media Server to delete the provided repository:

```
osc-setup cr --clean
```

7) Start the OpenScape Media Server with the following command:

```
/etc/init.d/symphoniad start
```

8) If you use a Media Server farm, perform all described steps on each OpenScape Media Server of this Media Server farm.

8.2 Installing, Upgrading and Uninstalling the OpenScape Media Server under OpenScape UCApplication

To install, upgrade or uninstall an OpenScape Media Server for one of the possible operating modes under OpenScape UCApplication you need to use the setup processes of OpenScape UCApplication.

You find details about this in the manual *OpenScape UCApplication, Installation and Upgrade, Installation Guide*.

Installing the TTS Software

For using TTS and ASR features with the OpenScape Media Server a corresponding TTS / ASR software must be installed on the OpenScape Media Server computer system. This TTS / ASR software is the TTS / ASR engine by Loquendo, which is already shipped with OpenScape UCApplication.

You find detailed information about setting up the TTS software in the manual *OpenScape UCApplication, Installation and Upgrade, Installation Guide*.

9 Basic Configuration of the OpenScape Media Server

After you have installed the OpenScape Media Server, it operates with a pre-set basic configuration. This basic configuration makes the OpenScape Media Server already operable for many applications. Only selected features may require a manual initial configuration.

NOTICE:

In a system environment with several OpenScape Media Servers you need to perform every configuration manually for each OpenScape Media Server. An automatic mechanism for configuration exchange between different OpenScape Media Servers does not exist.

Which pre-set basic configuration the OpenScape Media Server uses and whether a manual initial configuration is required depends on whether you use the OpenScape Media Server at OpenScape Voice or under OpenScape UCApplication.

9.1 Basic Configuration of the OpenScape Media Server at OpenScape Voice

After you have installed the OpenScape Media Server for operation at OpenScape Voice, it is directly operable as a rule. The server uses a basic configuration that you need to change only if single basic settings of your individual system environment need to be adjusted.

In the following we describe the essential basic settings of the OpenScape Media Server at OpenScape Voice.

Basic MGCP Settings

Local LAN interface:	<automatically recognized IP address> (no dual network support IPV4 / IPv6)
Local ports:	2427 (MGCP)

If required, you can change these settings in the defaulted MGCP listening point **default**.

Basic Streaming Settings

Streaming route: **default-route**	
Local LAN interface:	<automatically recognized IP address> (no dual network support IPV4 / IPv6)
Local ports (RTP, RTCP):	20 000 – 25 000
Quality of service	Standard
RTCP	deactivated

If required, you can change these settings in the defaulted RTP streaming route **default-route**.

SDP-related basic Streaming-IVR Settings

Security Protocol:	SDES and MIKEY
Length of the SDES auth. tag:	32 and 80 bit
Global security settings:	Insecure only
Global audio codecs:	Opus, G7221 bitrate=48000, opus maxplaybackrate=24000; sprop-maxcapturerate=24000, G7221 bitrate=32000, G722, PCMU, PCMA, G729, G729 annexb=no telephone-event

If required, you can change these settings in the Streaming-IVR provider settings.

Basic Terminal Settings

Terminal: **Media Gateway – announcement endpoints**	
Individual security settings:	Secure preferred
Address:	ann/*@*
Data streams:	Audio (uses automatically the only streaming route **default-route**)
Terminal: **Media Gateway – CALEA / ES endpoints**	
Individual security settings:	Secure preferred
Address:	es/*@*
Data streams:	Audio (uses automatically the only streaming route **default-route**)
Terminal: **Media Gateway – conference bridge endpoints**	
Individual security settings:	Secure preferred
Address:	cnf/*@*
Data streams:	Audio (uses automatically the only streaming route **default-route**)

If required, you can change these settings in the settings of the relevant terminal.

9.2 Basic Configuration of the OpenScape Media Server under OpenScape UCApplication

After you have installed the OpenScape Media Server for operation under OpenScape UCApplication, it is largely directly operable. The server uses a basic configuration that you need to change only if single basic settings of your individual system environment need to be adjusted.

In addition to the provided basic configuration you may have to perform the following manual configurations:

1) Deleting the ASR server URI

You need to execute this configuration only if you have not installed a ASR engine.

2) Configuring the SIP provider for outbound connections

3) Configuring the voice portal

You need to execute this configuration only if you wish to use the OpenScape UCApplication voice portal.

Details about this configuration are provided in the manual *OpenScape UCApplication, Configuration and Administration*.

4) Configuring the conference portal

You need to execute this configuration only if you wish to use the OpenScape UCApplication conference portal.

Details about this configuration are provided in the manual *OpenScape UCApplication, Configuration and Administration*.

In the following we describe the essential basic settings of the OpenScape Media Server at OpenScape Voice.

Basic Streaming Settings

Streaming route: **default-route**	
Local LAN interface:	<automatically recognized IP address> (no dual network support IPV4 / IPv6)
Local ports (RTP, RTCP):	20 000 – 25 000
Quality of service	Standard
RTCP	deactivated

If required, you can change these settings in the defaulted RTP streaming route **default-route**.

SDP-related basic Streaming-IVR Settings

Security Protocol:	SDES and MIKEY
Length of the SDES auth. tag:	32 and 80 bit
Global security settings:	Insecure only

Global audio codecs:	Opus, G7221 bitrate=48000, opus maxplaybackrate=24000; sprop-maxcapturerate=24000, G7221 bitrate=32000, G722, PCMU, PCMA, G729, G729 annexb=no telephone-event
Global video codecs:	H.264, H.265, VP8

If required, you can change these settings in the Streaming-IVR provider settings.

Basic SIP Settings

Local LAN interface:	<automatically recognized IP address> (no dual network support IPV4 / IPv6)
Local ports for the operating mode Integrated Simplex:	• 5062 (UDP) • 5062 (TCP) • 5063 (TLS)
Local ports for all other operating modes:	• 5060 (UDP) • 5060 (TCP) • 5061 (TLS)

If required, you can change these settings in the SIP provider settings.

9.2.1 How to Delete the ASR Server URI

If no ASR engine has been installed with the OpenScape Media Server, the associated ASR server URI should be deleted in the OpenScape Media Server configuration. The related system check of the OpenScape Media Server will otherwise report an error as the ASR engine cannot be reached under the default- set URI.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select the **Streaming IVR** link in the provider list.

   The configuration dialog with the settings of the Streaming IVR provider opens.
3) Switch to the **TTS and ASR** tab.
4) Delete the **Server address** setting under **Automatic Speech Recognition**.
5) Select **Save** to apply the changes.

You have now deleted the server URI for the ASR engine.

9.2.2 How to Configure the SIP Provider

To enable the OpenScape Media Server setting up outbound communication connections and to ensure that phone number normalization / localization works correctly, you need to configure the connection data of a least one SIP server in the SIP provider.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the link **IP Telephony (SIP)**.

The configuration dialog with the SIP provider settings opens.

3) Select **Add** under **SIP Servers**.

The configuration dialog for creating an SIP server line to a communications system opens.

4) Enter a unique name for the new SIP server line in the **ID** field.

Under this name the SIP server line will later be administered in the CMP.

5) In the **SIP Server Name** field specify the IP address of the Master SIP server to be preferably used by the OpenScape Media Server for the relevant SIP server line.

- For OpenScape Voice this is the IP address of the SIP service manager (SIP SM) as a rule.

NOTICE:

You can determine this IP address in the CMP in the following location:

Configuration > **OpenScape Voice** > **Administration** > **Signaling Management** > **SIP** in the **Node 1 Listening IP Address 1 for UDP, TCP and TLS** field.

- For OpenScape 4000 this is the IP address of the HG gateway used as a rule.

If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.

6) Select in the **Listening Point ID** field one of the configured listening points.

This listening point defines the local network address of the OpenScape Media Server via which the OpenScape Media Server is to communicate with the Master SIP server.

7) Specify in the **Port number** field the port number of the Master SIP server via which the OpenScape Media Server is to communicate with the Master SIP server.

- If you have selected a UDP- or TCP-based listening point in the **Listening Point ID** field, you will need to enter port `5060` here as a rule, because this is the UDP / TCP default port of SIP servers.
- If you have selected a TLS-based listening point, you will need to enter port `5061` here as a rule, because this is the TLS default port of SIP servers.

NOTICE:

OpenScape Voice endpoints do not use TLS by default.

To use TLS, you need to set the **MTLS** transport protocol for the relevant endpoints via the OpenScape Voice Assistant or via the CLI console of OpenScape Voice.

8) How to configure alternative SIP server connections for the SIP server line:

In doing so please note:

In case of a co-located OpenScape Voice system you must not configure any alternative SIP servers.

In case of a geo-separated OpenScape Voice system you may configure exactly one alternative SIP server. This should be the SIP Service Manager (SIPSM) of the associated node 2.

NOTICE:

You can determine whether to use OpenScape Voice as co-located or geo-separated system in the CMP in the following location::

Configuration > **OpenScapeVoice** > **General** > **Switches**

If the **Switch-Typ** column displays typ **Duplex** theb system is a co-located one.Type **Geographically Separated Duplex** is displayed for a geo-separated system.

a) Select **Add** under **Alternative SIP servers**.

The configuration dialog for creating an alternative SIP connection to a communications system opens.

b) In the **SIP Server Name** field specify the IP address of the alternative SIP server the OpenScape Media Server is to use for the relevant SIP server line if required.

If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.

c) Specify in the **Port number** field the port number of the alternative SIP server via which the OpenScape Media Server is to communicate with the alternative SIP server.

If you have selected a UDP- or TCP-based listening point in the **Listening Point ID** field, you will need to enter port `5060` here as a rule, because this is the UDP / TCP default port of SIP servers.

If you have selected a TLS-based listening point, you will need to enter port `5061` here as a rule, because this is the TLS default port of SIP servers.

NOTICE:

OpenScape Voice endpoints do not use TLS by default.

To use TLS, you need to set the **MTLS** transport protocol for the relevant endpoints via the OpenScape Voice Assistant or via the CLI console of OpenScape Voice.

d) Select **Save** to copy the settings of the fail-over SIP connection.

e) If required, configure for the SIP server line further alternative SIP server connections in the same way.

9) Select **Save**.

10) Select **Close**.

11) Select the radio button for the **IP Telephony (SIP)** provider.

12) Click on **Restart Provider**.

IMPORTANT:

When you reboot the SIP provider (**IP Telephony**), all associated connections are interrupted that exist at the time of the reboot. Before the reboot you can switch to the **Monitoring** tab to see whether connections are currently active.

You have now modified the SIP provider settings required for outgoing connections.

9.2.3 Configuring the Voice Portal

The OpenScape UCApplication, Configuration and Administration manual describes how to configure the voice portal.

9.2.4 Configuring the Conference Portal

The OpenScape UCApplication, Configuration and Administration manual describes how to configure the conference portal.

10 Adjusting the OpenScape Media Server to individual Requirements

After you have installed and basically configured the OpenScape Media Server it is operable. You can administer the OpenScape Media Server additionally for adjusting it to individual requirements.

These additional administration options depend on the environment in which the OpenScape Media Server is used.

NOTICE:

In a system environment with several OpenScape Media Servers you need to perform every configuration manually for each OpenScape Media Server. An automatic mechanism for configuration exchange between different OpenScape Media Servers does not exist.

10.1 How to Open the OpenScape Media Server Configuration Dialog

You configure the OpenScape Media Server to a large extent via a Media-Server-individual configuration dialog. This configuration dialog is integrated in the CMP and users with CMP administrator privileges can open it there.

Prerequisites

You are logged in at the CMP with administrator privileges.

Step by Step

1) On the **Operation& Maintenance** tab of the CMP click on the **Unified Communications** menu item.
2) In the navigation tree, click on **Configuration** > **Media Server**.

   You see a list of all Media Servers that are available in the OpenScape system.
3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

10.2 Individual Administration of the OpenScape Media Server at OpenScape Voice

After you have installed and basically configured the OpenScape Media Server it is operable at OpenScape Voice. You can administer the OpenScape Media Server additionally for adjusting it to individual requirements.

NOTICE:

In a system environment with several OpenScape Media Servers you need to perform every configuration manually for each OpenScape Media Server. An automatic mechanism for configuration exchange between different OpenScape Media Servers does not exist.

10.2.1 How to Add an MGCP Listening Point

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Create an additional MGCP listening point, if you wish to connect several communications systems via different IP address type (IPv4, IPv6) to the OpenScape Media Server.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **Media-Gateway (MGCP)** from the list.

   The MGCP provider configuration dialog opens.
3) Select **Add** under Listening Points.

   The configuration dialog for a listening point opens.
4) Specify a unique name for the listening point under **ID**. Under this name the listening point is administered in the Common Management Platform.
5) Under **Bind address**, specify the IP address that the OpenScape Media Server is to monitor by the listening point.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

   If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto$IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.
6) Under **Port number**, specify the port that the OpenScape Media Server is to monitor by the listening point.

   The default port number for MGCP is **2427**.
7) Select **Save** to copy the settings of the listening point.

   The listening points list now displays the newly configured MGCP listening point.

You have now added a new MGCP listening point.

Next steps

Bind the new listening point to at least one RTP streaming route via global or terminal-specific streaming route bindings.

10.2.2 How to Edit an MGCP Listening Point

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

You may have to edit an MGCP listening point as follows:

- Change the default port number 2427 for an MGCP listening point if the communications system used does not deploy the MGCP default port for MGCP.
- Change the binding address for an MGCP listening point if the computer system of the OpenScape Media Server uses several LAN interface boards and the communications system used cannot be reached via the pre-configured default interface board.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) Select **Media-Gateway (MGCP)** from the list.

The MGCP provider configuration dialog opens.

3) Select the radio button of the MGCP listening point you want to edit in the list of available MGCP listening points.

4) Select **Edit** under Listening Points.

The configuration dialog for the selected listening point opens.

5) Under **Bind address**, specify the IP address that the OpenScape Media Server is to monitor by the listening point.

If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

6) Under **Port number**, specify the port that the OpenScape Media Server is to monitor by the listening point.

The default port number for MGCP is **2427**.

7) Select **Save** to copy the settings of the listening point.

You have now configured an existing MGCP listening point.

10.2.3 How to Configure the maximum Number of Simultaneous Announcements

You can configure the number of announcements the OpenScape Media Server can simultaneously play for OpenScape Voice.

Prerequisites

In the application partitioning of the OpenScape Media Server a sufficient number of RTP channels is reserved for the **MediaGateway** application to allow simultaneous OpenScape Voice announcements.

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Address Binding** tab.

2) Select in the list the address binding the terminal ID **Media#Gateway–announcement endpoints** is assigned to.

The configuration dialog of the selected address binding opens.

3) Enter the following text under **Address expression**:

`mgcp:ann/[1,<max. number >]@.*`

Specify the maximum number of announcements for <max. number >.

Example of 30 simultaneous announcements: `mgcp:ann/[1,30]@.*`

> **NOTICE:**
>
> If you configure several address bindings for the terminal ID **Media#Gateway – announcement endpoints**, the address numbers of these address bindings must not overlap. In the example, the address expression of a second address binding with 20 additional announcements reads as follows:
>
> `mgcp:ann/[31,50]@.*`

4) Select the **Regular expression** option under **Type**.

5) Select **Save**.

You have now configured how many announcements the OpenScape Media Server can simultaneously play for OpenScape Voice.

10.2.4 How to Configure the Maximum Number of Simultaneous Participants for a Participant-Controlled Conferences

You can configure the number of simultaneous participants for a single participant-controlled OpenScape Voice conference that the OpenScape Media Server allows.

Prerequisites

In the application partitioning of the OpenScape Media Server a sufficient number of RTP channels is reserved for the **MediaGateway** application to allow simultaneous participant-controlled conferences.

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the configuration dialog switch to the **Address Binding** tab.
2) Select in the list the address binding the terminal ID **Media#Gateway – conference bridge endpoints** is assigned to.

   The configuration dialog of the selected address binding opens.
3) Enter the following text under **Address expression**:

   `mgcp:cnf/[1,<max. number >]@.*`

   Specify the maximum number of conference participants for <max. number >.

   For 30 simultaneous conference participants: `mgcp:cnf/[1,30]@.*`

   > **NOTICE:**
   >
   > If you configure several address bindings for the terminal ID **Media#Gateway – conference bridge endpoints**, the address numbers of these address bindings must not overlap. In the example, the address expression of a second address binding with 20 additional conference participants reads as follows:
   >
   > `mgcp:cnf/[31,50]@.*`

4) Select the **Regular expression** option under **Type**.
5) Select **Save**.

You have thus configured the number of simultaneous participant-controlled conferences that the OpenScape Media Server allows for OpenScape Voice.

10.2.5 How to Configure the Maximum Number of Simultaneous Monitoring Endpoints

You can configure the number of monitoring endpoints the OpenScape Media Server allows for monitoring OpenScape Voice connections at the same time.

Prerequisites

In the application partitioning of the OpenScape Media Server a sufficient number of RTP channels is reserved for the **MediaGateway** application to allow simultaneous monitoring points.

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Address Binding** tab.
2) Select in the list the address binding the terminal ID **Media#Gateway – CALEA endpoints** is assigned to.

   The configuration dialog of the selected address binding opens.
3) Enter the following text under **Address expression**:

   `mgcp:es/[1,<max. number >]@.*`

   Specify the maximum number of monitoring endpoints for <max. number >.

   Example of 30 simultaneous monitoring endpoints: `mgcp:es/[1,30]@.*`

   > **NOTICE:**
   >
   > If you configure several address bindings for the terminal ID **Media#Gateway – CALEA endpoints**, the address numbers of these address bindings must not overlap. In the example, the address expression of a second address binding with 20 additional monitoring endpoints reads as follows:
   >
   > `mgcp:es/[31,50]@.*`
4) Select the **Regular expression** option under **Type**.
5) Select **Save**.

You have thus configured the number of monitoring endpoints the OpenScape Media Server allows for monitoring OpenScape Voice connections at the same time.

10.2.6 How to Configure a Sublanguage for a Basic Language

Several sublanguages may be installed on the OpenScape Media Server for a basic language (OpenScape Voice language ID). For example, the sublanguages for India and the US for the basic language English. In this case you can determine the sublanguage to be used for the associated basic language.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

For the basic language there are several sublanguages installed on the OpenScape Media Server.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **Announcements and Resources** from the list of names.

   The **Announcements and Resources** dialog opens.
3) Select the **Language Settings** tab.
4) In the list of preferred sublanguages, under **Language**, select the basic language for which you want to configure the sublanguage.
5) Select the sublanguage that you want to use for the selected basic language under **Preferred Sublanguage**.
6) Select **Save** to copy the modified setting.

You have now configured the sublanguage for the relevant basic language.

10.2.7 How to Configure the Fallback to Transnational OpenScape Voice Announcements

If a language package does not contain all country-specific announcements of the relevant country, the OpenScape Media Server uses an internal fallback mechanism to determine, from which alternative language package the missing announcements shall be played. You can manually control the default behavior of this fallback mechanism with the expert setting **fallbackLanguages** in the relevant configuration file.

Step by Step

1) Open the following configuration file in a text editor:

   `resourcedatabase.component.xml`

   You find this configuration file in the following directory:

   <MS#Install [24]>`/mediaserver/application_host/providers/resource database`

[24] <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

2) Specify within the **fallbackLanguages** tag which fallback language shall be used for which sublanguage.

   Use the following notation:

   <sublanguage>=<fallback language to be used>

   Example: **<fallbackLanguages>**zh_hk=en_us**</fallbackLanguages>**

   This example defines that the OpenScape Media Server is to use announcements in English (US) for the sublanguage Chinese (Hongkong) if required.
3) Save the changes in the configuration file.
4) Reboot the **Resource Database** provider in the OpenScape Media Server configuration dialog.

10.2.8 How to Upload an Individual Version for an existing OpenScape Voice Announcement File

You can load an additional individual version on the OpenScape Media Server for an existing OpenScape Voice announcement file. The OpenScape Media Server then plays this uploaded announcement file instead of the original announcement file. After uploading on the OpenScape Media Server the original announcement file is still kept.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

The announcement file to be uploaded must be available in one of the supported formats. The supported formats are listed in the chapter about the features of the OpenScape Media Server.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **Announcements and Resources** from the list of names.

   The configuration dialog for the **Announcements and Resources** provider opens.
3) Select the **Prompt and Music Files** tab.
4) Look for the following entry in the directory structure:

   MediaGateway / <version > / <language >
5) Click on the name of the announcement file for which you want to load an additional individual version on the OpenScape Media Server.

   The configuration dialog of the selected announcement file opens.
6) Switch to the **Deploy Customized Prompt** tab.
7) Select under **Import File** the file to be used instead of the existing announcement file.
8) Select **Deploy now** to load the individual version of the announcement file on the OpenScape Media Server.
9) Select **Close**.

10) Select **Save** to copy the modified setting.

You have now loaded an additional individual version for a announcement file on the OpenScape Media Server. From now on the OpenScape Media Server plays this file instead of the original announcement file.

10.2.9 How to Reactivate the Original Version of an existing OpenScape Voice Announcement File

You can load an additional individual version on the OpenScape Media Server for an existing OpenScape Voice announcement file. The OpenScape Media Server then plays this uploaded announcement file instead of the original announcement file. Subsequently, you can delete the uploaded announcement file for the OpenScape Media Server to use the original announcement file again.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **Announcements and Resources** from the list of names.

   The configuration dialog for the provider **Announcements and Resources** opens.
3) Select the **Prompt and Music Files** tab.
4) Look for the following entry in the directory structure:

   MediaGateway / <version > / <language >
5) Click on the name of the announcement file for which you have previously uploaded an individual version on the OpenScape Media Server that you want to delete now.

   The configuration dialog of the selected announcement file opens.
6) Switch to the **Download Prompt** tab.
7) Select **Remove**.
8) Select **Close**.
9) Select **Save** to copy the modified setting.

The OpenScape Media Server thus uses the original announcement file again.

10.2.10 How to Replace Default Music-on-Hold of OpenScape Voice

OpenScape Voice provides default music-on-hold. If required, you can replace it with individual music-on-hold. On the OpenScape Media Server, the default music-on-hold has names of the format: `MOH<x>`, with `<x>` representing a consecutive number between 1 and 4.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

The music-on-hold to be used must be available as file in one of the supported formats. Please refer to the chapter on the OpenScape Media Server features to look up such formats.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) Select **Media-Gateway (MGCP)** from the list.

The MGCP provider configuration dialog opens.

3) Select in the section **Music-on-Hold Files** under **File** the name of the music-on-hold for which you wish to load an individual music-on-hold file on the OpenScape Media Server.

4) Select a language for the individual music-on-hold file to be uploaded on the OpenScape Media Server under **Language**.

5) Select **Add**.

The dialog for importing a music-on-hold file opens.

6) Check that the desired language is displayed under **Language**.

7) Describe the music-on-hold shortly under **Description**.

8) Select the desired music-on-hold file under **Import File**.

9) Select the **Use default file replication** option if you wish to replicate the new music-on-hold to all other OpenScape Media Servers of a Media Server farm.

10) Select **Save** to load the music-on-hold on the OpenScape Media Server.

The new music-on-hold is displayed in the list of music-on-hold files.

NOTICE:

If several files of the same language have been loaded on the OpenScape Media Server for a music-on-hold file, the OpenScape Media Server plays such files using the round-robin procedure.

You have now loaded an individual music-on-hold file for default music-on-hold on the OpenScape Media Server.

10.2.11 How to Reset a Changed Default Music-on-Hold of OpenScape Voice to its Standard

OpenScape Voice provides default music-on-hold. If required, you can replace it with individual music-on-hold. Subsequently, you can reset a changed music-on-hold to the standard that was valid after the OpenScape Media Server installation.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

You have replaced a default music-on-hold with individual music-on-hold.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **Media-Gateway (MGCP)** from the list.

   The MGCP provider configuration dialog opens.
3) Select **Add** under Music-on-Hold Files.

   The configuration dialog for the music-on-hold files opens.
4) Select under **File** the name of the music-on-hold for which you have loaded an individual music-on-hold file on the OpenScape Media Server and which you wish to reset now.

   NOTICE:

   To play music-on-hold click on its name in the list column **ID**.
5) Select under **Language** the language for which you wish to reset the music-on-hold.

   You see a list of all music-on-hold files available on the OpenScape Media Server for the selected music-on-hold and language.
6) Select the radio button of the individual music-on-hold file you wish to reset.

   NOTICE:

   You can only select one music-on-hold file at a time for resetting it.
7) Select **Remove**.

   NOTICE:

   The **Remove** button is inactive if the selected music-on-hold file is the original file installed with the OpenScape Media Server.

   A dialog for confirming the deletion opens.
8) Select **Yes** to delete the selected individual music-on-hold file.
   The selected individual music-on-hold file is deleted from the list of music-on-hold files. If this file was the last one in the list, the music-on-hold file originally installed with the OpenScape Media Server is now displayed.

The OpenScape Media Server now uses the music-on-hold file originally installed with the OpenScape Media Server for the selected default music-on-hold and the selected language again.

10.2.12 How to Configure an Internet Radio Station for providing Music-on-Hold

Instead of audio files used for OpenScape Voice by default you can also deploy music from Internet radio stations to serve as music-on-hold. To do this you must add an Internet radio station in the Internet Radio Streaming Provider and configure this Internet radio station as music-on-hold in the MGCP provider.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

- The desired Internet radio station broadcasts with the following specifications:
  - MP3 coded
  - PLS or M3U playback lists
  - Content type HTTP
  - The Internet radio stream is broadcasted on port 80

IMPORTANT:

Playing back music is generally subject to copyrights. Make sure that you are authorized to play the selected music using the Internet Radio Streaming Provider.

NOTICE:

Owing to individual, technical restrictions, playing back music from Internet radio stations may fail even if they comply with the listed specifications.

As a test, you can open a station's URL for example in the VLC Media Player. If the VLC Media Player does not play the Internet radio station, it cannot be used as an Internet radio station in the OpenScape Media Server either.

NOTICE:

Once an Internet radio station has been added in the Internet Radio Streaming Provider, the former is automatically activated and available as a resource in the OpenScape Media Server.

Providing every configured Internet radio station allocates approximately 100 kbit/s of bandwidth on the recipient side of the OpenScape Media Server. This value is independent from the number of subscribers to whom music from an Internet radio station is played.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the **Internet radio streaming** link.

The configuration dialog of the provider opens.

3) If the Internet Radio Streaming Provider is to connect the configured Internet radio stations via a proxy, execute the following steps.

a) Specify under **HTTP proxy FQDN** the proxy's IP address (IPv4, IPv6).

If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

NOTICE:

If the placeholder value **proxy.cycos.com** appears, remove this value and use the one suitable for your environment.

b) Specify under **HTTP proxy port** the port number to which the Internet Radio Streaming Provider is to broadcast.

4) Specify under **Local FQDN** the IP address (IPv4, IPv6) the Internet Radio Streaming Provider is to use on the local computer system of the OpenScape Media Server.

If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

5) Select **Test an Internet radio station** to test a new Internet radio station.

The configuration dialog for configuring the URL of an Internet radio station opens.

6) Specify under **Station URL** the URL under which the Internet radio station can be reached.

7) Select **Save** to apply the settings for the Internet radio station.

The new Internet radio station is displayed in the list of Internet radio stations.

8) Verify that the entry **CONNECTED** appears for the new Internet radio station in the **Status** list column within the next seconds. If the result is **CONNECTED**, it means that you have a working Internet radio station which is compatible with the Media Server.

IMPORTANT:

If the Internet Radio Streaming Provider cannot connect to the new station URL, the new Internet radio station is unsuitable for acting as a music-on-hold provider.

IMPORTANT:

At this point, any Internet Radio Station tested is not permanently stored into the system configuration and will be removed after a symphonia restart. The Internet Radio Station can be permanently saved only after assigning it for Music on Hold following the steps below.

9) If required, create further Internet radio stations in the same way.

10) On the **Providers** tab of the configuration dialog, select the entry **Media Gateway (MGCP)**.

    The MGCP provider configuration dialog opens.

11) In the **Music on Hold Files** section, select under **Files** the name of the music-on-hold for which you wish to play an Internet radio station.

12) Select under **Language** the language for which you wish to play an Internet radio station.

13) Select **Add**.

    The dialog for importing a music-on-hold file opens.

14) Check that the desired language is displayed under **Language**.

15) Describe the music-on-hold shortly under **Description**.

16) Select the **Use internet radio station playing instead of prompt** option.

    The **Station URL** field is displayed.

17) Select under **Station URL** one of the internet radio stations you have just created in the Internet Radio Streaming Provider.

18) Select **Save** to copy the settings.

    The new music-on-hold is displayed in the list of music-on-hold files.

19) If required, create further Internet radio stations in the same way as a music-on-hold.

You have now configured an Internet radio station as a music-on-hold.

10.2.13 How to Restart the Connection to an Internet Radio Station

The connection to an internet radio station may have to be restarted– for example when connection problems occur.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

IMPORTANT:

A new start will interrupt the playback of Internet radio station music for some seconds.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the **Internet radio streaming** link.

   The configuration dialog of the provider opens.

3) Select the Internet radio station in the list of Internet radio stations.

4) Select **Restart**.

   The current connection to the Internet radio station is closed and reestablished.

5) Select **Cancel**.

You have now restarted the connection to an Internet radio station.

10.2.14 How to Remove an Internet Radio Station from the Music-on-Hold Configuration

If you do not wish to use a configured Internet radio station anymore, you can remove it from the configuration.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the **Internet radio streaming** link.

The configuration dialog of the provider opens.

3) Select the Internet radio station in the list of Internet radio stations.

4) Select **Remove** to delete the Internet radio station.

The selected Internet radio station is removed from the list of Internet radio stations.

5) Select **Save** to apply the changed settings.

You have now removed an Internet radio station from the configuration.

10.2.15 How to Use a Music-on-Hold Template of OpenScape Voice

OpenScape Voice provides predefined music-on-hold templates to which individual wildcard files have already been assigned in the OpenScape Media Server. Those assigned wildcard files of the OpenScape Media Server are not used by OpenScape Voice by default, but appropriate intercepts and treatments have already been preconfigured for them in OpenScape Voice. You can thus easily activate additional music-on-hold when for example a customer-individual contact center application requires additional music-on-hold. To use one of the predefined music-on-hold templates in OpenScape Voice, you must replace the assigned wildcard file with the music-on-hold file to be used in the OpenScape Media Server. On the OpenScape Media Server, the wildcard files have names of the format: `HPPC_Ann<xx>`, with `<xx>` representing a consecutive number between 1 and 50.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

The music-on-hold to be used must be available as file in one of the supported formats. Please refer to the chapter on the OpenScape Media Server features to look up such formats.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) Select **Media-Gateway (MGCP)** from the list.

The MGCP provider configuration dialog opens.

3) Select **Add** under Music-on-Hold Files.

The configuration dialog for the music-on-hold files opens.

4) Select under **File** the name of the music-on-hold for which you wish to load an individual music-on-hold file on the OpenScape Media Server.

5) Select a language for the individual music-on-hold file to be uploaded on the OpenScape Media Server under **Language**.

6) Select **Add**.

The dialog for importing a music-on-hold file opens.

7) Check that the desired language is displayed under **Language**.

8) Describe the music-on-hold shortly under **Description**.

9) Select the desired music-on-hold file under **Import File**.

10) Select the **Use default file replication** option if you wish to replicate the new music-on-hold to all other OpenScape Media Servers of a Media Server farm.

11) Select **Save** to load the music-on-hold on the OpenScape Media Server.

The new music-on-hold is displayed in the list of music-on-hold files.

NOTICE:

If several files of the same language have been loaded on the OpenScape Media Server for a music-on-hold file, the OpenScape Media Server plays such files using the round-robin procedure.

---

12) Assign in OpenScape Voice the associated pre-configured intercept as desired– e. g. to a multi line hunt group (MLHG).

You find configuration details in the administration manual for OpenScape Voice.

You have now loaded an individual music-on-hold file for a music-on-hold template on the OpenScape Media Server.

10.2.16 How to Provide additional OpenScape Voice Announcements

You can import additional announcements for OpenScape Voice in the OpenScape Media Server via the deployment interface– e. g. if you require additional announcements for a contact center application in OpenScape Voice. To this you need to create a deployment package that contains all required files and import this package in the OpenScape Media Server. Subsequently, you need to configure a new intercept in OpenScape Voice for each additional announcement.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

All pre-defined music-on-hold templates of OpenScape Voice are already used for the `HPPC_Ann<xx>.wav` announcements.

NOTICE:

If predefined music-on-hold templates are still available, you should use them first.

Each deployment file must contain the following files. They form the so-called deployment package.

- `package.xml` – it contains meta data for the deployment package.
- *<name of the deployment package* >`.prompt.xml` – it describes all announcements to be imported and their storage path within the deployment package.
- The announcement files that OpenScape Voice is to use in addition must be available in one of the supported formats. Please refer to the chapter on the OpenScape Media Server features to look up such formats.

Step by Step

1) Create a temporary deployment folder on your computer system in which all of the following files are stored.

2) Store all announcement files you wish to import in the OpenScape Media Server in the temporary deployment folder.

NOTICE:

The names of the announcement files must not contain any blanks. Replace the blanks with underscores, for example.

3) Create the `package.xml` file as follows:

a) Open a text editor and enter the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<package>
 <packageName> <package name > </packageName>
 <version> <version number > </version>
 <description> <package description> </description>
</package>
```

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<package>
 <packageName>MyAnnouncements</packageName>
```

Example:

```
 <version>4.0.0</version>

 <description>MS-Announcements</description>

</package>
```

NOTICE:

All packages available in an OpenScape Media Server must have a unique name. Consequently, you cannot import a deployment package in OpenScape Media Server that has the same package name as a package already available in the OpenScape Media Server.

b) Save the new file under the name `package.xml` directly in the previously created temporary deployment folder.

4) Create the `<package name>.prompt.xml` file as follows:

a) Open a text editor and enter the following text:

```
<resources applicationId="MediaGateway">

 <resource id="<unique denominator>">

  <properties>

   <property name="lang" value="<language token 1>"/
   >

   <property name="lang" value="<language token 2>"/
   >

   …

  </properties>

  <content>

   <promptDescriptions>

    <audio uri="<announcement file>"/>

   </promptDescriptions>

  </content>

 </resource>

 <resource id="<unique denominator>">

  …

 </resource>

 …
```

```
</resources>
```

NOTICE:

If an announcement file to be imported is independent from languages, do not specify an associated **<properties>** section.

Example:

```
<resources applicationId="MediaGateway">
 <resource id="NewPrompt1">
  <properties>
   <property name="lang" value="en"/>
   <property name="lang" value="de"/>
   …
  </properties>
  <content>
   <promptDescriptions>
    <audio uri="CompleteNewPrompt1.wav"/>
   </promptDescriptions>
  </content>
 </resource>
 <resource id="NewPrompt2">
  <content>
   <promptDescriptions>
    <audio uri="CompleteNewPrompt2.wav"/>
   </promptDescriptions>
  </content>
 </resource>
 …
```

Example:

```
</resources>
```

NOTICE:

The specification under **<resource id>** will later be referenced in the treatment ID of OpenScape Voice.

NOTICE:

You can use all OpenScape Voice language tokens as language tokens.

Examples: de, en, es, fr, …

b) Save the new file under the name <*package name*>`.prompt.xml` directly in the previously created temporary deployment folder.

In doing so, use the package name you previously specified in the `package.xml` file instead of <*package name*>.

5) Create the deployment package from the files of the deployment folder as follows.

a) Create a Zip archive from the files of the deployment folder.

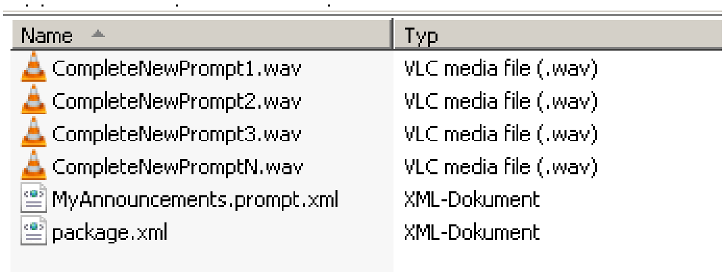


Figure 7: Example:

NOTICE:

The Zip archive must not contain the actual deployment folder but exclusively the files contained therein.

b) Replace the file extension `.zip` of the Zip archive with `mdp.zip`.

6) Import the deployment package in the OpenScape Media Server as follows.

a) In the OpenScape Media Server configuration dialog switch to the **Applications** tab.

b) Select **Import**.

The deployment dialog for applications opens.

c) Select the just created deployment file under **Import File**.

d) Select **Import Now**.

The selected deployment file is loaded onto the OpenScape Media Server.

7) Check whether the deployment package was imported correctly by executing the following steps:

a) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

b) In the provider list select the **Deployment Manager** link.

The Deployment Manager dialog opens.

c) Verify that the list of available packages also features the just imported deployment package and **Deployed** is indicated as status.

NOTICE:

If the deployment package was not imported correctly, switch to the following directory:

`/opt/siemens/mediaserver/application_host/deployment-custom/`

Delete the relevant `mdp.zip` file in there. If after a few seconds the associated *<package name>* directory has not also been deleted automatically, delete it manually.

The deployment package has now been successfully imported in the OpenScape Media Server. If the import has failed, check the contents of the XML files of your deployment package once again.

8) Create a new intercept in OpenScape Voice for each additional announcement according to the following guide.

You find configuration details in the administration manual for OpenScape Voice.

> **NOTICE:**
>
> If you import an announcement file for several languages, you need to configure only one intercept for this announcement file.

a) Add a new intercept and assign it a unique name.

b) Add a new treatment in the newly added intercept.

c) Assign the following value to the treatment as **ID**:

`pa@*(an=file:///~la/`***<Resource-ID*** *from* *`<package name>.prompt.xml>.wav`*`)`

Example:

`pa@*(an=file:///~la/NewPrompt1)`

If the relevant announcement of OpenScape Voice shall be played as loop, suffix the URI with the expression `it=-1`.

Example:

`pa@*(an=file:///~la/NewPrompt1 it=-1)`

If the relevant announcement is independent from languages, do not specify a `~la/`.

Example:

`pa@*(an=file:///NewPrompt1)`

d) Select the option **MGCP Media Service** as **Destination Type** for the treatment.

e) Select the OpenScape Media Server for the treatment under **Destination Name**.

f) Select the Media Server circuit **ann/$** for the treatment under **Destination Circuit**.

9) Assign in OpenScape Voice the new intercept as desired– e. g. to a multi line hunt group (MLHG).

You find configuration details in the administration manual for OpenScape Voice.

You can now invoke the new announcement of OpenScape Voice.

10.2.17 How to Add Multiple Music-on-Hold Files

The OpenScape Media Server provides the functionality to add multiple music-on-hold audio files in order to avoid playing the same message repeatedly. The OpenScape Media Server plays multiple music-on-hold audio files using the round-robin procedure. On the OpenScape Media Server, the default music-on-hold has names of the format: `MOH<x>`, with `<x>` representing a number, e.g. 0.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

The music-on-hold files to be used must be available in one of the supported formats. Please refer to the chapter on the OpenScape Media Server features to look up such formats.

Appropriate intercepts and treatments have already been preconfigured for the additional music-on-hold files in OpenScape Voice. You find further information about configuring intercepts and treatments in OpenScape Voice, Administrator Documentation).

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) Select **Media-Gateway (MGCP)** from the list.

The MGCP provider configuration dialog opens.

3) Select in the section **Music-on-Hold Files** under **File** the prompt-id of the music-on-hold for which you wish to load an individual music-on-hold file on the OpenScape Media Server, e.g. MOH0.

4) Select a language for the individual music-on-hold file to be uploaded on the OpenScape Media Server under **Language**, e.g. English (USA).

5) Select **Add**.

The dialog for importing a music-on-hold file opens.

6) Check that the desired language is displayed under **Language**, e.g. en_us.

7) Describe the music-on-hold shortly under **Description**.

8) Click **Browse** to select the desired music-on-hold file.

9) Select the **Use default file replication** option if you wish to replicate the new music-on-hold to all other OpenScape Media Servers of a Media Server farm.

10) Alternatively, you can select to play an internet radio station instead of a prompt:

a) Enable the check box **Use internet radio station playing instead of prompt**.

b) Select the desired internet radio station from the **Station URL** drop-down list.

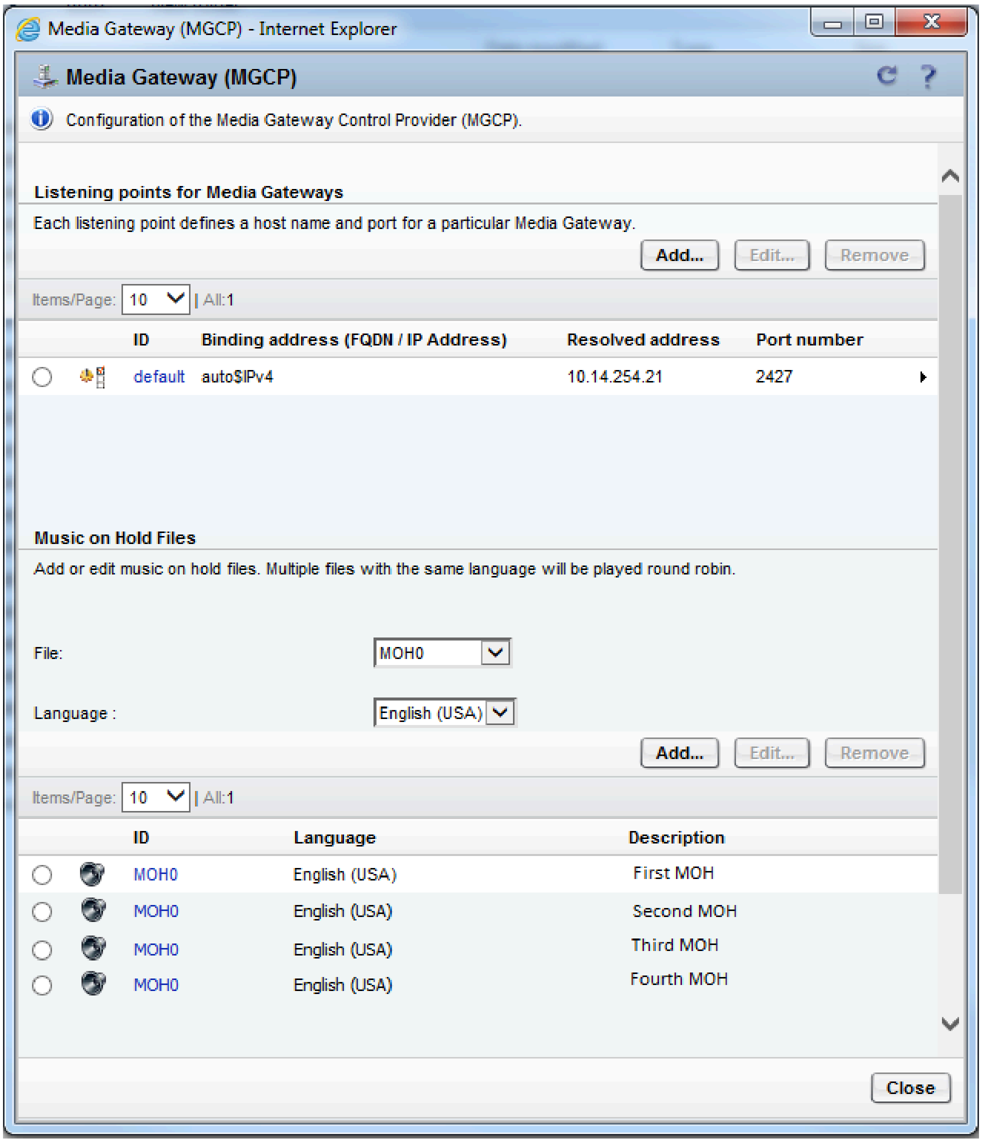
NOTICE:

You must have configured the Internet radio station URL via the **Providers** tab > **Internet Radio Streaming** (section How to Configure an Internet Radio Station for providing Music-on-Hold).

---

11) Select **Save** to load the music-on-hold on the OpenScape Media Server.

The new music-on-hold is displayed in the list of music-on-hold files.



12) Repeat steps 3-11 to load each additional music-on-hold file under the same prompt-id (step 3), e.g. MOH0.

You have now loaded multiple music-on-hold files on the OpenScape Media Server that will be served in round-robin fashion, ensuring a low chance of playing the same message repeatedly.

10.2.18 How to Delete a Deployment Package

The deployment interface lets you import additional deployment packages in the OpenScape Media Server– e. g. to provide additional announcements in

OpenScape Voice for a contact center application. You can delete deployment packages thus imported at a later date.

Prerequisites

A deployment package has been imported in the OpenScape Media Server.

Step by Step

1) Switch to the following directory on the computer system of the OpenScape Media Server:

<MS#Install [25]>`/mediaserver/application_host/deployment-custom`

2) Delete the `mdp.zip` file of the deployment package you wish to remove.

After a few seconds, the directory associated to the relevant deployment package will be automatically deleted also. This directory carries the same name as the deployment package.

NOTICE:

If the deployment package to be deleted was not imported correctly, the directory of the relevant deployment package may not be deleted automatically. Delete it manually in this case.

You have now deleted the relevant deployment package from the OpenScape Media Server.

10.2.19 How to Configure Simultaneously Used IPv4 / IPv6 Addresses at OpenScape Voice

After its installation the OpenScape Media Server is pre-configured to use an IPv4-based network at OpenScape Voice. However, you can configure the OpenScape Media Server to operate simultaneously at IPv4- and IPv6-based networks.

For the following configuration we assume that the OpenScape Media Server has exclusively been using IPv4 addresses so far. If it has exclusively been using IPv6 addresses instead, the associated address changes in the following configuration steps accordingly.

Step by Step

1) Select the desired Dual Network Protocol in the SDP settings of the Streaming IVR Provider.

25 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

2) Configure the MGCP listening point that exists by default for IPv4.

Use the following settings:

Setting	UDP ListeningPoint
Bind address	<IPv4 address for the MGCP listening point>
Port number	2427

3) Create a new MGCP listening point for IPv6.

Use the following settings:

Setting	UDP ListeningPoint
ID	ListeningPoint v6
Bind address	<IPv6 address for the MGCP listening point>
Port number	2427

4) Configure the RTP streaming route that exists by default with the ID **default**.

Use the following settings:

Setting	Value
Bind address	<IPv4 address for the RTP streaming route>
Start range of RTP ports	20000 [26]
Number of RTP ports [27]	500 [28]
Quality of service	<any setting>
RTCP reports	<any setting>

5) Create a new RTP streaming route.

Use the following settings:

Setting	Value
Streaming Route ID	IPv6
Bind address	<IPv6 address for the RTP streaming route>

---

26 Adjust this default value if required. Please note that this port must be released in a possibly available firewall.

27 Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the same number of UDP ports set here is once again allocated for the RTCP communication– even if the option **RTCP Reporting** is deactivated for the RTP streaming routes. Please note that all ports must be released in a possibly available firewall.

28 Adjust this default value if required. Please note that this port must be released in a possibly available firewall.

Setting	Value
Start range of RTP ports	20100 [29]
Number of RTP ports [30]	500 [31]
Quality of service	<any setting>
RTCP reports	<any setting>

6) Configure a global streaming route binding that determines the RTP streaming routes **default** and **IPv6** as primary or alternative streaming route for the MGCP listening point.

Setting	Streaming Route Binding
Listening point	MGCP (*)
Streaming route	Default
Altern. streaming route	IPv6

NOTICE:

If required, you can also configure streaming routes specific to the terminal instead of the global streaming route binding.

Next steps

If you use a firewall, you need to ensure that in this firewall the additional IPv6 addresses are released besides the ports used and the IPv4 addresses.

If you use the OpenScape Media Server at OpenScape UCApplication also, you need to configure the IPv4 / IPv6 addresses for use under OpenScape UCApplication, too.

10.2.20 How to Enable the Whisper Mode for all cnf-Circuits

By default, the OpenScape Media Server is configured not to use the Whisper mode for the silent monitoring of OpenScape Voice. This is because the Whisper mode allocates about 25% more system resources in the OpenScape Media Server for conferences than for the conference function without the Whisper functionality. However, the Whisper mode can be enabled for all cnf-circuits.

29 Adjust this default value if required. Make sure that the port ranges of different RTP streaming routes do not overlap. Please also note that this port must be released in a possibly available firewall.

30 Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the same number of UDP ports set here is once again allocated for the RTCP communication– even if the option **RTCP Reporting** is deactivated for the RTP streaming routes. Please note that all ports must be released in a possibly available firewall.

31 Adjust this default value if required. Make sure that the port ranges of different RTP streaming routes do not overlap. Please also note that this port must be released in a possibly available firewall.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the configuration dialog switch to the **Terminals** tab.

2) Select in the list the terminal the following applet is assigned to:

application:/MediaGateway#conference-bridge

The configuration dialog of the selected terminal opens.

3) Select the following entry under **Application**:

application:/MediaGateway#whisper-conference

4) Select **Save**.

You have thus enabled the Whisper mode for all cnf-circuits.

10.2.21 How to Disable the Whisper Mode for all cnf-Circuits

You can disable the Whisper mode system-wide for all cnf-circuits.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the configuration dialog switch to the **Terminals** tab.

2) Select in the list the terminal the following applet is assigned to:

application:/MediaGateway#whisper-conference

The configuration dialog of the selected terminal opens.

3) Select the following entry under **Application**:

application:/MediaGateway#conference-bridge

4) Select **Save**.

You have thus deactivated the Whisper mode for all cnf-circuits.

10.2.22 How to Configure parameter reuseLocalAddressEnabled for all cnf-Circuits

By default, OpenScape Media Server changes its media port when a new remote party is connected to same MGCP endpoint via a MGCP MDCX/SDP request, in order to avoid to have two remote parties to stream RTP towards the same MGCP endpoint.If there is a need to reuse media port when a new remote party is connected to same MGCP endpoint via a MGCP MDCX/SDP request, reuseLocalAddressEnabled should be set to true.This is needed when the remote party is configured with “Don’t send INVITE without SDP” (e.g, Genesys SIP Server)You can configure OpenScape Media Server to reuse media port when a new remote party is connected to same MGCP endpoint for all cnf-Circuits

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Access to Command Line Interface of Media Server

Step by Step

1) The parameter **reuseLocalAddressEnabled** can be configured in the following terminal configuration file for all cnf-Circuits:

- Configuration file for all cnf-Circuits: *conference-bridge.terminal.xml*
- Storage location: */<host >/deployment/mediagateway-application/conference-bridge.terminal.xml*
- <host > corresponds to one of the following paths:
  - */enterprise/mediaserver/application_host*
  - */opt/siemens/mediaserver/application_host*

2) Edit the terminal configuration file for all cnf-Circuits and set **reuseLocalAddressEnabled** to `true`

3) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

4) Select the radio button for the Media Gateway (MGCP) provider.

5)) Restart the Media Gateway provider by clicking on the arrow to the right of "Media Gateway (MGCP)" and selecting "**Restart Provider**"

10.2.23 Adjusting the volume level of an Internet Radio Station Stream

In case the volume level of an Internet radio station stream needs to be adjusted, this can be achieved by following the steps below.

Step by Step

1) On the OpenScape Media Server node navigate to directory: `/opt/siemens/mediaserver/application_host/providers/internetradio`

2) Edit the xml file `internetradio.component.xml`

e.g: `vi internetradio.component.xml`

Before </component> and just after the previous parameter add the following:

<volumeLevel>100</volumeLevel>

e.g:

```
<defaultPollIRStatusSec>10</defaultPollIRStatusSec>
<volumeLevel>40</volumeLevel>
</component>
```

NOTICE:

Accepted values for 'volumeLevel' are 0 to 100. The lower the value, the lower the volume.

---

3) Restart symphonia services:

```
/etc/init.d/symphoniad stop
/etc/init.d/symphoniad start
```

10.3 Individual Administration of the OpenScape Media Server under OpenScape UCApplication

After you have installed and basically configured the OpenScape Media Server it is operable under OpenScape UCApplication. You can administer the OpenScape Media Server additionally for adjusting it to individual requirements.

NOTICE:

In a system environment with several OpenScape Media Servers you need to perform every configuration manually for each OpenScape Media Server. An automatic mechanism for configuration exchange between different OpenScape Media Servers does not exist.

10.3.1 General Administration of the OpenScape Media Server under OpenScape UCApplication

10.3.1.1 How to Add an SIP Listening Point

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

The SIP listening points are not used if the OpenScape Media Server is exclusively deployed at OpenScape Voice.

Create additional SIP listening points if the OpenScape Media Server is to receive inbound SIP connections e.g. via additional ports or LAN interface boards.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the link **IP Telephony (SIP)**.

   The configuration dialog with the SIP provider settings opens.
3) Select **Add** in the **Listening points for SIP networking** section.

   The configuration dialog for a listening point opens.
4) Specify a unique name for the listening point under **ID**. Under this name the listening point is administered in the Common Management Platform.
5) Under **Bind address**, specify the IP address that the OpenScape Media Server is to monitor by the listening point.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

   If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.
6) Under **Port number**, specify the port that the OpenScape Media Server is to monitor by the listening point.
7) Select **Save** to copy the settings of the listening point.

   The listening points list now displays the newly configured SIP listening point.

You have now added a new SIP listening point.

Next steps

Bind the new listening point to at least one RTP streaming route via global or terminal-specific streaming route bindings.

10.3.1.2 How to Connect SIP Servers via SIP Server Lines

To ensure that the OpenScape Media Server can set up outbound communications connections and the phone number normalization / localization works correctly, it must be connected to an SIP server via at least one SIP server line.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

SIP server lines are not used if the OpenScape Media Server is exclusively deployed at OpenScape Voice.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the link **IP Telephony (SIP)**.

   The configuration dialog with the SIP provider settings opens.
3) Select **Add** in the **SIP Servers** section.

   The configuration dialog for an SIP server line opens.
4) Specify a unique name for the new SIP server line under **ID**. Under this name the SIP server line is administered in the Common Management Platform.
5) Enter the IP address under which the relevant SIP server can be reached in the **SIP Server Name** field.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.
6) Specify under **Port number** the port configured on the relevant SIP server for inbound SIP communication.
7) Select under **Address translation context** the address translation context that the SIP Provider is to use for normalizing and localizing phone numbers for the relevant SIP server line.
8) Select under **Listening Point ID** the ID of the SIP listening point the local IP address and transport protocol of which the OpenScape Media Server is to use for the SIP communication with the relevant SIP server.
9) In the **Alternative SIP servers** section you can connect alternative SIP servers for the relevant SIP server.
10) Select **Save**.

    The SIP server list now displays the newly configured SIP server.

You have thus connected an SIP server to the OpenScape Media Server via a new SIP server line.

10.3.1.3 How to Configure SIP Server Lines

To enable the OpenScape Media Server setting up outbound communication connections and to ensure that phone number normalization / localization works correctly, you need to configure the connection data of a least one SIP server in the SIP provider.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

SIP server lines are not used if the OpenScape Media Server is exclusively deployed at OpenScape Voice.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the link **IP Telephony (SIP)**.

   The configuration dialog with the SIP provider settings opens.
3) In the **SIP Servers** section, select the radio button of the SIP server line you want to configure.
4) Select **Edit**.

   The configuration dialog for the selected SIP server line opens.
5) Enter the IP address under which the relevant SIP server can be reached in the **SIP Server Name** field.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.
6) Specify under **Port number** the port configured on the relevant SIP server for inbound SIP communication.
7) Select under **Address translation context** the address translation context that the SIP Provider is to use for normalizing and localizing phone numbers for the relevant SIP server line.
8) Select under **Listening Point ID** the ID of the SIP listening point the local IP address and transport protocol of which the OpenScape Media Server is to use for the SIP communication with the relevant SIP server.
9) In the **Alternative SIP servers** section you can connect alternative SIP servers for the relevant SIP server.
10) Select **Save**.

You have now configured an existing SIP server line.

10.3.1.4 How to Connect an Alternative SIP Server via SIP Server Lines

For each SIP server that you connect to the OpenScape Media Server, you can define any number of individual alternative SIP servers.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

You must not configure any alternative SIP servers for the SIP connection to a co-located OpenScape Voice system. For a geo-separated system, you may configure only a single alternative SIP server. In this case, the master connection to the SIP service manager (SIPSM) must lead from node 1 and the alternative connection to the SIP service manager (SIPSM) from node 2.

NOTICE:

SIP server lines are not used if the OpenScape Media Server is exclusively deployed at OpenScape Voice.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the link **IP Telephony (SIP)**.

   The configuration dialog with the SIP provider settings opens.
3) In the **SIP Servers** section select the radio button of the SIP server line for which you want to configure an alternative SIP server.
4) Select **Edit**.

   The configuration dialog for the selected SIP server line opens.
5) Select **Add** in the **Alternative SIP servers** section.

   The configuration dialog for connecting an alternative SIP server opens.
6) Enter the IP address under which the alternative SIP server can be reached in the **Remote Host Name (FQDN / IP Address)** field.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.
7) Under **Port number**, specify the port via which the OpenScape Media Server is to send outbound SIP communication to the alternative SIP server.
8) Select **Save**.

   The list of alternative SIP servers now displays the newly configured alternative SIP server.

You have now connected an alternative SIP server to the OpenScape Media Server.

10.3.1.5 How to Configure SIP Routing for a Terminal

You can define the local network addresses for the OpenScape Media Server to route outbound SIP communication. You configure this SIP routing individually for each terminal.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.
2) Select from the list the terminal for the SIP communication of which you want to configure the routing.

   The configuration dialog of the selected terminal opens.
3) Under **Outbound line**, select the ID of the SIP server line via which the OpenScape Media Server is to route the SIP communication.
4) Select **Save** to copy the modified setting.

You have now configured SIP routing for a terminal.

10.3.1.6 How to Configure a Communication Billing Address via a Terminal

Applications can independently establish outgoing communication connections via the OpenScape Media Server. If costs are incurred for such a connection, the OpenScape Voice can assign such costs to a billing address that you can configure specific to a terminal.

Prerequisites

The relevant terminal uses SIP as connection control protocol.

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.
2) Select the terminal for which you want to configure the billing address.

   The configuration dialog of the selected terminal opens.
3) Select the **SIP** button.

   The configuration dialog for SIP-specific terminal settings opens.
4) Specify the phone number of an OpenScape Voice subscriber under **Billing address**. Call charges incurred by communication connections of the relevant terminal are then assigned to this subscriber.

   > **NOTICE:**
   >
   > In this field only digits and a leading + character are permitted.
5) Select **Save**.
6) Select **Save** to copy the modified setting.

You have now configured the billing address for a terminal.

10.3.1.7 How to Configure the OpenScape Web Collaboration Provider

The settings of the OpenScape Web Collaboration provider determine how the OpenScape Media Server provides Web Collaboration services.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) Select **OpenScape Web Collaboration** from the list.

The configuration dialog for the OpenScape Web Collaboration provider opens.

3) Specify under **Download address for WebCollaboration clients** the IP address under which the Web Collaboration services shall be accessible on the local computer systems of the OpenScape Media Server.

If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

4) Specify under **Web Client URL** the URL under which OpenScape Web Collaboration clients can access the Web Collaboration services.

This URL has the following general format.

`http://`<FQDN of the Web Collaboration Web Client Server>`:80/JoinClient.aspx?inv=%1`

For `<FQDN of the Web Collaboration Web Client Server>` you need to enter the fully qualified host name under which OpenScape Web Collaboration clients can reach the Web Client Collaboration services from outside.

5) Specify under **Quality of Service** the quality of service class for transmitting the data of the Web Collaboration services.

6) Verify that the list of OpenScape Web Collaboration clients displays the program files of all required clients. If the program file is missing for a client the OpenScape Media Server shall provide for downloading, add it.

7) Verify that in the connection point list all connection points are configured under which users shall download the program files of the OpenScape Web Collaboration clients. If a connection point is missing or the created connection points have not been correctly configured, change the configuration accordingly.

8) Select **Save** to copy the settings.

You have now configured the OpenScape Web Collaboration provider.

10.3.1.8 How to Provide the Program File of an OpenScape Web Collaboration Client for Downloading

Users can download the program files of OpenScape Web Collaboration clients from OpenScape Media Server to participate in web conferences. Before you can download the program file of an OpenScape Web Collaboration client from the OpenScape Media Server, it must be provided on the OpenScape Media Server.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **OpenScape Web Collaboration** from the list.

   The configuration dialog for the OpenScape Web Collaboration provider opens.

   NOTICE:

   The list of OpenScape Web Collaboration clients shows which OpenScape Web Collaboration client are already available for downloading.

3) Select **Import** in the **OpenScape Web Collaboration clients** section.

   The deployment dialog for program files opens.
4) Specify under **Import File** the program file of the OpenScape Web Collaboration client to be provided on the OpenScape Media Server for downloading.
5) Select **Import Now**.

   The selected program file is loaded onto the OpenScape Media Server and added in the list of the OpenScape Web Collaboration clients.
6) Select **Save** to copy the settings.

You have now provided the program file of a OpenScape Web Collaboration client for downloading.

10.3.1.9 How to Add a Web Collaboration Connection Point

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

You need to add a new Web Collaboration connection point if users shall download program packages of the OpenScape Web Collaboration client under additional port numbers.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **OpenScape Web Collaboration** from the list.

   The configuration dialog for the OpenScape Web Collaboration provider opens.
3) Select **Add** in the **Connection Points** section.

   The configuration dialog for a Web Collaboration connection point opens.
4) Specify a unique name for the new connection point under **ID**. Under this name the connection point is administered in the Common Management Platform.
5) Specify under **Binding address** the IP address the OpenScape Media Server shall use for the connection point.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

   If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.
6) Select under **Transport protocol** the protocol the OpenScape Media Server shall use for the connection point.

   IMPORTANT:

   If you create a connection point for the HTTPS transport protocol, you need to configure the settings **Certificate**, **Root Certificate** and **Certificate Password** in the settings of the OpenScape Web Collaboration provider.
7) Specify under **Port number** the port the OpenScape Media Server shall use for the connection point.
8) Select **Save** to apply the new settings for the connection point.

   The connection point list now displays the newly configured Web Collaboration connection point.

You have now added a new Web Collaboration connection point.

10.3.1.10 How to Edit a Web Collaboration Connection Point

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

You need to edit a Web Collaboration connection point if users are not to download program packages of the OpenScape Web Collaboration client under the pre-set port number 5000 (TCP), 88 (HTTP) or 444 (HTTPS).

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) Select **OpenScape Web Collaboration** from the list.

   The configuration dialog for the OpenScape Web Collaboration provider opens.
3) Select in the list of configured Web Collaboration connection points the radio button of the connection point you wish to edit.
4) Select **Edit**.

   The configuration dialog of the selected connection point opens.
5) Specify a unique name for the new connection point under **ID**. Under this name the connection point is administered in the Common Management Platform.
6) Specify under **Binding address** the IP address the OpenScape Media Server shall use for the connection point.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

   If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.
7) Select under **Transport protocol** the protocol the OpenScape Media Server shall use for the connection point.

   > **IMPORTANT:**
   >
   > If you create a connection point for the HTTPS transport protocol, you need to configure the settings **Certificate**, **Root Certificate** and **Certificate Password** in the settings of the OpenScape Web Collaboration provider.
8) Specify under **Port number** the port the OpenScape Media Server shall use for the connection point.
9) Select **Save** to apply the new settings for the connection point.

You have now configured an existing Web Collaboration connection point.

10.3.1.11 How to Configure Simultaneously Used IPv4 / IPv6 Addresses under UC Application

After its installation the OpenScape Media Server is pre-configured to use an IPv4-based network under OpenScape UCApplication. However, you can configure the OpenScape Media Server to operate simultaneously at IPv4- and IPv6-based networks.

To do this you need to:

- configure SIP listening points for the IPv4- and IPv6-based network.

- create SIP server lines for at least two SIP servers– one line for an SIP server in the IPv4-based network and the other one for an SIP server in the IPv6-based network. The two SIP server lines may also share one SIP server that uses an IPv4- and an IPv6-based network board.
- configure at least two terminals for each application – one terminal for the connection into the IPv4-based network and the other one for the connection into the IPv6-based network. In this case, the relevant application needs to decide for outbound connection requests which terminal to use for routing a connection request; the OpenScape Media Server itself does not take this decision.

For the following configuration we assume that the OpenScape Media Server has exclusively been using IPv4 addresses so far. If it has exclusively been using IPv6 addresses instead, the associated address changes in the following configuration steps accordingly.

Step by Step

1) Select the desired Dual Network Protocol in the SDP settings of the Streaming IVR Provider.

2) Configure the SIP listening points that exist by default with the following IDs:

a) UDP ListeningPoint

b) TCP ListeningPoint

c) TLS ListeningPoint

Use the following settings:

Setting	UDP ListeningPoint	TCP ListeningPoint	TLS ListeningPoint
Bind address	<IPv4 address for the SIP listening point>	<IPv4 address for the SIP listening point>	<IPv4 address for the SIP listening point>
Port number	5060	5060	5061
Transport protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)	Transport Layer Security (TLS)

NOTICE:

In the Integrated Simplex operation mode, OpenScape Voice uses already the ports 5060 and 5061 as a rule. Configure then port 5062 for TCP and UDP and 5063 for TLS.

3) Create three new SIP listening points.

Use the following settings:

Setting	**UDP ListeningPoint**	**TCP ListeningPoint**	**TLS ListeningPoint**
ID	UDP ListeningPoint v6	TCP ListeningPoint v6	TLS ListeningPoint v6

Setting	UDP ListeningPoint	TCP ListeningPoint	TLS ListeningPoint
Bind address	<IPv6 address for the SIP listening point>	<IPv6 address for the SIP listening point>	<IPv6 address for the SIP listening point>
Port number	5060	5060	5061
Transport protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)	Transport Layer Security (TLS)

NOTICE:

In the Integrated Simplex operation mode, OpenScape Voice uses already the ports 5060 and 5061 as a rule. Configure then port 5062 for TCP and UDP and 5063 for TLS.

4) Configure the RTP streaming route that exists by default with the ID **default**.

Use the following settings:

Setting	Value
Bind address	<IPv4 address for the RTP streaming route>
Start range of RTP ports	20000 [32]
Number of RTP ports [33]	2 500 [34]
Quality of service	<any setting>
RTCP reports	<any setting>

NOTICE:

Using the OpenScape UCApplication TTS / ASR engine always requires at least one IPv4-based RTP streaming route to be configured in the OpenScape Media Server.

5) Create a new RTP streaming route.

Use the following settings:

Setting	Value
Streaming Route ID	IPv6

32 Adjust this default value if required. Please note that this port must be released in a possibly available firewall.

33 Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the same number of UDP ports set here is once again allocated for the RTCP communication– even if the option **RTCP Reporting** is deactivated for the RTP streaming routes. Please note that all ports must be released in a possibly available firewall.

34 Adjust this default value if required. Please note that the relevant ports must be released in a possibly available firewall.

Setting	Value
Bind address	<IPv6 address for the RTP streaming route>
Start range of RTP ports	20000 [35]
Number of RTP ports [36]	2 500 [37]
Quality of service	<any setting>
RTCP reports	<any setting>

6) Configure a global streaming route binding that determines the RTP streaming routes **default** and **IPv6** as primary or alternative streaming route for all SIP listening points.

Setting	Streaming Route Binding
Listening point	SIP (*)
Streaming route	Default
Altern. streaming route	IPv6

NOTICE:

If required, you can also configure streaming routes specific to the terminal instead of the global streaming route binding.

7) Create two new SIP server lines.

Use the following settings:

Setting	SIP server line 1	SIP server line 2
ID	Server line IPv4	Server line IPv6
Name of the remote host	<IPv4 address of the relevant SIP server>	<IPv6 address of the relevant SIP server>
Listening point ID	UDP ListeningPoint [38]	UDP ListeningPoint v6 [39]

35 Adjust this default value if required. Please note that this port must be released in a possibly available firewall.

36 Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the same number of UDP ports set here is once again allocated for the RTCP communication– even if the option **RTCP Reporting** is deactivated for the RTP streaming routes. Please note that all ports must be released in a possibly available firewall.

37 Adjust this default value if required. Please note that the relevant ports must be released in a possibly available firewall.

38 If you want to use TCP or TLS as transport protocol, select the relevant IPv4-based SIP listening point.

39 If you want to use TCP or TLS as transport protocol, select the relevant IPv6-based SIP listening point.

Setting	SIP server line 1	SIP server line 2
Port number	5060 [40]	5060 [41]

8) Configure two terminals for each application that is to route connection requests via the IPv4- and IPv6-based SIP server line.

Under **Outbound line**, select the SIP server line **Server Line IPv4** for one terminal, and **Server Line IPv6** for the other terminal.

The OpenScape Media Server may now simultaneously use the relevant IPv4- and IPv6-based network. The implementation of the applications used determines which of these networks is used for an outbound SIP connection by selecting the respective terminal.

Next steps

If you use a firewall, you need to ensure that in this firewall the additional IPv6 addresses are released besides the ports used and the IPv4 addresses.

If you use the OpenScape Media Server at OpenScape Voice also, you need to configure the IPv4 / IPv6 addresses for use at OpenScape Voice, too.

10.3.1.12 How to Import an Application

If you use the OpenScape Media Server under OpenScape UCApplication, you can manually import individual applications in the OpenScape Media Server - for example applications created with the Application Builder.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

Instead of importing an individual application manually into the OpenScape Media Server you can also use the Application Builder for an automatic import. Information about this procedure describes the manual *OpenScape UCApplication, Application Builder, User Guide*.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Applications** tab.

40 The port number must be adjusted to the transport protocol of the selected SIP listening point. If you select a different SIP listening point under Listening Point ID, you need to configure the port number accordingly.

41 The port number must be adjusted to the transport protocol of the selected SIP listening point. If you select a different SIP listening point under Listening Point ID, you need to configure the port number accordingly.

2) Select **Import**.

The deployment dialog for applications opens.

3) Specify the import file of the application you wish to import under **Import File**.

NOTICE:

The import file must have the extension `.mdp.zip`. If you attempt to import a file with a differing extension, the import process is aborted with an error message.

---

4) Select **Import Now**.

The selected import file is loaded on the OpenScape Media Server and your application starts automatically.

The application is displayed on the **Applications** tab. You have now imported an individual application in the OpenScape Media Server and started it.

10.3.1.13 How to Remove Applications from the OpenScape Media Server

If you use the OpenScape Media Server under OpenScape UCApplication, you can remove previously imported applications from the OpenScape Media Server.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Applications** tab.
2) Tick off the checkboxes of the applications you wish to remove from the OpenScape Media Server.

IMPORTANT:

The following step removes the selected applications from the OpenScape Media Server. Users being connected to one of these applications are then cut off without any further query or waiting time.

---

3) Select **Remove**.

The selected applications are removed from the OpenScape Media Server and disappear from the list of available applications.

The OpenScape Media Server immediately closes existing connections to application users.

Address bindings for the removed applications are automatically deleted.

10.3.2 Administering the Voice Portal under OpenScape UCApplication

The OpenScape UCApplication, Configuration and Administration manual describes how to administer the voice portal.

10.3.3 Administering the Conference Portal under OpenScape UCApplication

The OpenScape UCApplication, Configuration and Administration manual describes how to administer the conference portal.

10.4 Administering the OpenScape Media Server for General Use

After you have installed and basically configured the OpenScape Media Server it is operable. You can administer the OpenScape Media Server additionally for adjusting it to individual requirements that are independent from whether you use the Media Server at OpenScape Voice or under OpenScape UCApplication.

NOTICE:

In a system environment with several OpenScape Media Servers you need to perform every configuration manually for each OpenScape Media Server. An automatic mechanism for configuration exchange between different OpenScape Media Servers does not exist.

10.4.1 How to Restart a Provider

If you need to change provider settings, you must as a rule reboot the provider for the modifications to take effect. Whether or not a provider needs to be rebooted is displayed in the node management of the OpenScape Media Server.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

IMPORTANT:

When you reboot the Streaming provider (**Streaming**), SIP provider (**IP telephony**) or MGCP provider (**Media Gateway**), all associated connections that exist at the time of the reboot are interrupted. Before the reboot you can switch to the **Monitoring** tab to see whether connections are currently active.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) Check the provider list for providers that are indicated for a reboot in the **Restart Needed** column.

3) Select the radio button of the provider that you want to reboot.

4) Click on **Restart Provider**.

The selected provider stops and restarts. All changed settings in the rebooted provider take effect.

10.4.2 How to Add an RTP Streaming Route

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

You may have to add an RTP streaming route for the following reasons:

- For enabling the OpenScape Media Server to route RTP data via additional LAN interfaces – in particular via additional IPv6 interfaces.
- For enabling the OpenScape Media Server to route RTP data for an individual VLAN.
- For enabling the OpenScape Media Server to route RTP data of various media types via different LAN interfaces.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the link **Streaming (RTP)**.

The configuration dialog with the Streaming provider settings opens.

3) Select **Add**.

The configuration dialog that contains the settings of a new RTP streaming route opens.

4) Specify a unique name for the RTP streaming route under **Streaming Route ID**. The RTP streaming route is administered in the Common Management Platform under this name.

5) Specify under **Bind address** the IP address that the OpenScape Media Server is to use for outbound RTP communication via the RTP streaming route.

If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

6) Under **Start range of RTP ports** specify the first port of the port range to be used by the OpenScape Media Server for outbound RTP communication via the RTP streaming route.

7) Under **Number of RTP ports** specify how many RTP ports the RTP streaming route is to use at the most.

   Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the number of RTP ports set here is once again allocated for the RTCP communication– even if you deactivate RTCP for the RTP streaming route.

   Example: **Number of RTP ports** = 75

   A total of 150 RTP ports is allocated. 75 for the RTP and 75 for the RTCP communication.
8) Under **Quality of Service** specify the quality of service class to be used by the RTP streaming route for sending RTP data.
9) Select **Save** to copy the settings of the RTP streaming route.

   The list of RTP streaming routes now displays the newly configured RTP streaming route.

You have now added a new RTP streaming route.

Next steps

Bind the new RTP streaming route to at least one listening point via global or terminal-specific streaming route bindings.

10.4.3 How to Edit an RTP Streaming Route

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

You may have to edit an RTP streaming route e.g. as follows:

- Change the binding address for an RTP streaming route if the computer system of the OpenScape Media Server uses several LAN interface boards and RTP data is not to be transmitted via the pre-configured default interface board.
- Change the port settings used if the OpenScape Media Server is to use additional or other ports for transmitting RTP data.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the link **Streaming (RTP)**.

   The configuration dialog with the Streaming provider settings opens.
3) Select the radio button of the RTP streaming route that you want to configure in the list of available RTP streaming routes.
4) Select **Edit**.

   The configuration dialog for the selected RTP streaming route opens.

5) Specify under **Bind address** the IP address that the OpenScape Media Server is to use for outbound RTP communication via the RTP streaming route.

   If the host name of the computer system can be resolved into the desired IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

   If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.
6) Under **Start range of RTP ports** specify the first port of the port range to be used by the OpenScape Media Server for outbound RTP communication via the RTP streaming route.
7) Under **Number of RTP ports** specify how many RTP ports the RTP streaming route is to use at the most.

   Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the number of RTP ports set here is once again allocated for the RTCP communication– even if you deactivate RTCP for the RTP streaming route.

   Example: **Number of RTP ports** = 75

   A total of 150 RTP ports is allocated. 75 for the RTP and 75 for the RTCP communication.
8) Under **Quality of Service** specify the quality of service class to be used by the RTP streaming route for sending RTP data.
9) If you want to activate RTCP for the RTP streaming route, select the **RTCP Reporting** option.

You have now configured an existing RTP streaming route.

10.4.4 configure RTP-Routing

The network addresses (streaming route) to be used by a data stream for transmitting data must always be determined.

This is done using the following options – also combined. Their prioritization declines from 1) to 3).

1) Assigning statistic streaming routes to the respective data stream.

   NOTICE:

   Even if several streaming routes are assigned to a data stream, it always uses only one of these streaming routes for transferring data of a specific RTP connection.
2) Assigning individual streaming route bindings to the terminal. Such streaming route bindings define the streaming route to be used dynamically, depending on the listening point respectively used.
3) Configuring globally valid streaming route bindings.

10.4.4.1 How to Configure Statistic Streaming Routes for the Data Stream of a Terminal

You can statically assign the data stream a streaming route to define the local network address the OpenScape Media Server uses for routing the outbound RTP communication of a data stream. To define several local network addresses you can also assign several streaming routes to a data stream. Example: You can define a local IPv4-based and a local IPv6-based network address for a data stream. You can configure this statistic RTP routing individually for each data stream of a terminal.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

> **NOTICE:** Static streaming routes you define for a data stream have a higher priority than streaming route bindings you may have configured in the terminal or in the Streaming IVR provider.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.
2) Select the terminal for the RTP communication of which you want to define the routing.

   The configuration dialog of the selected terminal opens.
3) In the list of configured RTP data streams select the radio button of the data stream for the media type of which you want to configure the RTP routing.
4) Click on **Edit** in the **Streams** section.

   The configuration dialog of the selected RTP data stream opens.
5) In the list of configured RTP streaming routes select the checkboxes of those routes that the OpenScape Media Server is to use for routing the relevant RTP communication.

   > **NOTICE:**
   >
   > You can only see the RTP streaming routes list if more than one RTP streaming route is configured in the OpenScape Media Server.
6) Click on **OK** to copy the changed setting for the data stream.
7) Click on **Save** to copy the changed setting for the terminal.

You have now configured the RTP routing for a terminal.

10.4.4.2 How to Add Dynamic Streaming Route Bindings Specific to a Terminal

You can assign individual streaming route bindings to the relevant terminal by defining the local network addresses that the OpenScape Media Server uses for routing the outbound RTP communication of a data stream. Such streaming route bindings are valid for all data streams of the respective terminal and define the network address to be used dynamically, depending on the respectively deployed listening point. You can define up to two local network addresses for each streaming route binding. Example: You can define a local IPv4-based and a local IPv6-based network address for a data stream.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE: Terminal-specific streaming route bindings have a higher priority than those valid across the system that you may have configured in the Streaming-IVR provider.

You may have to add a terminal-specific streaming route binding for the following reasons:

- For enabling the OpenScape Media Server to use a newly added streaming route terminal-specific.
- For enabling the OpenScape Media Server to use a newly added listening point terminal-specific.

NOTICE:

If you wish to configure a streaming route binding that is to be valid across the system, create in the Streaming-IVR provider a streaming route binding valid across the system instead of a terminal-specific one.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

2) Select the terminal for which you want to add the streaming route binding from the list.

The configuration dialog of the selected terminal opens.

3) Select **Streaming Route Bindings**.

The configuration dialog for terminal-specific streaming route bindings opens. This dialog shows all streaming route bindings configured for the relevant terminal.

4) Select **Define terminal specific binding**.

5) Select under **Listening point** the listening point from which the individual routing of RTP data is to depend.

If signaling data is transmitted via this listening point, the associated RTP data is routed via the streaming route you define under **Streaming route**.

To make routing dependent from all configured SIP listening points, select **(SIP) ***.

6) Select under **Streaming route** the streaming route you wish to specify as streaming route for the selected listening point.

7) If required, select under **Alternative streaming route** a streaming route that the OpenScape Media Server is to use as alternative streaming route for the selected listening point.

NOTICE:

You need to specify an alternative streaming route if the OpenScape Media Server is simultaneously connected to an IPv4- and IPv6-based network. In this case, select under **Streaming route** e. g. a route into the IPv4-based network and under **Alternative streaming route** a route into the IPv6-based network. In this case you need to additionally select a Dual Network Protocol in the SDP settings of the Streaming-IVR provider.

8) Select **Save** to copy the settings of the streaming route binding address.
9) If required, define further terminal-specific streaming route bindings in the described manner.
10) Select **Close** to close the configuration dialog for terminal-specific streaming route bindings.
11) Click on **Save** to copy the settings for the terminal.

You have now added a new terminal-specific streaming route binding.

10.4.4.3 How to Add Dynamic Streaming Route Bindings across the System

You can configure streaming route bindings valid across the system by defining the local network addresses that the OpenScape Media Server uses for routing the outbound RTP communication of data streams. Such streaming route bindings are valid for the data streams of all terminals and define the network address to be used dynamically, depending on the respectively deployed listening point. You can define up to two local network addresses for each streaming route binding. Example: You can define a local IPv4-based and a local IPv6-based network address for a data stream.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

When you define individual streaming route bindings in a terminal, such settings specific to the terminal are used preferably.

You may have to add a streaming route binding valid across the system for the following reasons:

- For enabling the OpenScape Media Server to use a newly added streaming route system-wide.
- For enabling the OpenScape Media Server to use a newly added listening point system-wide.

NOTICE:

If you wish to configure a streaming route binding that is to be valid for a selected terminal only, create a terminal-specific streaming route binding instead of one valid across the system.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the link **Streaming-IVR**.

   The configuration dialog with the Streaming-IVR provider settings opens.
3) Select **Add** under Streaming Route Binding
4) Select under **Listening point** the listening point from which the individual routing of RTP data is to depend.

   If signaling data is transmitted via this listening point, the associated RTP data is routed via the streaming route you define under **Streaming route**.

   To make routing dependent from all configured SIP listening points, select **(SIP) ***.
5) Select under **Streaming route** the streaming route you wish to specify as streaming route for the selected listening point.
6) If required, select under **Alternative streaming route** a streaming route that the OpenScape Media Server is to use as alternative streaming route for the selected listening point.

   NOTICE:

   You need to specify an alternative streaming route if the OpenScape Media Server is simultaneously connected to an IPv4- and IPv6-based network. In this case, select under **Streaming route** e. g. a route into the IPv4-based network and under **Alternative streaming route** a route into the IPv6-based network. In this case you need to additionally select a Dual Network Protocol in the SDP settings of the Streaming IVR Provider.
7) Select **Save** to copy the settings of the streaming route binding address.
8) If required, define further terminal-specific streaming route bindings in the described manner.
9) Select **Save** to copy the settings.

You have thus added a streaming route binding valid across the system.

10.4.5 How to Add an Address Binding

You use a new address binding to determine an additional address under which incoming calls can reach a selected application.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Address Binding** tab.
2) Select **Add**.

   The address binding configuration dialog opens.
3) Under **Terminal-ID** select the terminal of the desired application.
4) Specify the desired phone number expression under **Address-expression**. This expression defines the phone numbers under which the selected terminal is to be reached in the OpenScape Media Server.

   NOTICE:

   Always specify the phone numbers in the normalized phone number format – e. g. +492404901100.

   If you want to specify several phone numbers that cannot be constituted in the form of a single phone number expression, you need to create at least one more address binding with the same terminal ID.

   NOTICE:

   You need to ensure that the phone numbers configured here are routed on the SIP trunk to the OpenScape Media Server in the communications system.

   ---
5) Determine under **Type** in which format the specified phone number expression is to be interpreted by the OpenScape Media Server.
6) Select **Save**.

   The **Address Binding** tab now displays the newly configured address binding.

You now added a new address binding.

10.4.6 Configuring the Application Partitioning

You perform the application partitioning of the OpenScape Media Server in various configuration steps that need to be executed in a fixed sequence.

1) Defining for the different resource types that can be partitioned, how many system resources the OpenScape Media Server can provide in total.
2) Assigning shares of the available system resources to the various applications.

10.4.6.1 How to Specify the total Number for System Resources

You can determine the maximum number of resources the OpenScape Media Server can provide for the different resource types that can be partitioned.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the link **Application Partitioning**.

   The configuration dialog for application partitioning opens.
3) Select under **Resource Type** the resource type for which you want to specify the total number of available resources.
4) Then click the **Edit** button.

   The configuration dialog for editing the resource type opens.
5) Specify under **Number of available resources** how many resources of this type are to be available in the OpenScape Media Server.

   The * wildcard defines an infinite number of resources.
6) Select the **Save** button to copy the settings for the resource type.
7) If required, specify in a similar way how many system resources are to be available for the other resource types that can be partitioned.

You have now specified how many system resources are to be available for the selected resource type in the OpenScape Media Server.

Next steps

Proportionally assigning available system resources to individual applications.

10.4.6.2 How to Assign System Resources to Applications

You can proportionally assign the maximum number of provided OpenScape Media Server system resources that can be partitioned to individual applications.

Prerequisites

The maximum number of system resources OpenScape Media Server can provide for the various resource types that can be partitioned is fixed.

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the link **Application Partitioning**.

   The configuration dialog for application partitioning opens.

3) In the configuration dialog for the resource management select **Configure Applications**.

   The configuration dialog for administering resources application-based opens.

4) Under **Application** select the application that you want to assign system resources.

   You can now see a list of all resource types that have already been assigned to the selected application.

5) Select **Add** to assign system resources of a new resource type to the selected application.

   The configuration dialog for assigning resources to a application opens.

6) Select under **Resource Type** the name of the resource type of which you want to assign system resources to the application.

7) Specify under **Maximum** how many system resources of the selected resource type you want to assign to the application.

   NOTICE:

   The amount of all assigned system resources of a resource type must not exceed the total number of system resources that you have previously specified for the relevant resource type.

8) Select the **Save** button to copy the settings for the application.

9) If required, specify in a similar way how many system resources of other resource types you want to assign to the application in addition.

You have now specified how many system resources are available to a application.

10.4.7 How to Configure the Security Protocol for Encrypted RTP Communication

You can configure the security protocol valid across the system in the Streaming-IVR provider of the OpenScape Media Server. This security protocol is used if secured RTP communication is activated system-wide or specific to terminals via the **Security mode** setting.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the link **Streaming-IVR**.

The configuration dialog with the Streaming-IVR provider settings opens.

3) Switch to the **SDP** tab.

4) Select under **Security Protocol** the protocol to be used for RTP communication between OpenScape Media Server and terminals.

5) If you have selected an option with SDES under **Security Protocol**, set the length of the associated authentication tag under **SDES Authentication tag length**.

6) Perform the **Security mode** setting to determine in which way the security protocol shall be used by default for all configured terminals.

If required, you can adjust this default setting for selected terminals in the relevant terminal settings.

IMPORTANT:

Using SRTP with MIKEY requires the system time of all systems involved in the SRTP communication to be synchronized – OpenScape Media Server, RTP-based devices (e. g. phone), VoIP gateway etc. The Network Time Protocol (NTP) may be used for this purpose.

The possible settings have the following meaning.

- **Secure only**

  A connection is only set up if the communications system and the RTP terminal use SRTP with MIKEY or SDES for the RTP communication.

  IMPORTANT:

  The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

- **Insecure only**

  A connection is only set up if the communications system and the RTP terminal use an unencrypted RTP communication.

- **Secure preferred**

  If the communications system and the RTP terminal can use SRTP with MIKEY or SDES for the RTP communication, the OpenScape Media Server uses this type of communication.

  If the communications system and the RTP terminal can only use an unencrypted RTP communication, the RTP connection is set up unencrypted.

  IMPORTANT:

  The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

  ---

7) Select **Save** to copy the modifications.

You have now configured the RTP security settings system-wide for all terminals.

10.4.8 How to Specify Codec Settings Valid Across the System

You can determine which codecs the OpenScape Media Server uses for in- and outbound RTP communication and also the priority with which the OpenScape Media Server uses these codecs. You can perform such settings for data streams system-wide in the streaming IVR provider or terminal-specific.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

If individual codec settings are specified in the data stream of a terminal, such terminal-specific settings are used preferably.

NOTICE:

The codec the OpenScape Media Server eventually uses for a connection also depends on the codecs the connection partner supports. Especially when inbound connections are set up, the connection partner sends the OpenScape Media Server a prioritized list of his/her supported codecs. The OpenScape Media Server then uses this list preferably for specifying the codec to be used.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the link **Streaming-IVR**.

The configuration dialog with the Streaming-IVR provider settings opens.

3) Switch to the **SDP** tab.

4) How to remove a system-wide configured codec:

a) Switch to the **Audio Codecs** or **Video codecs** tab.

b) Select the radio button of the codec you wish to remove.

c) Select **Remove**.

The relevant codec is removed from the codec list.

5) How to configure a codec system-wide:

a) Switch to the **Audio Codecs** or **Video codecs** tab.

b) Select **Add**.

The codec configuration dialog opens.

c) Select under **Codec** the codec you wish to configure system-wide.

d) Select **OK** to copy the new codec system-wide.

The newly configured codec is displayed in the codec list.

6) If you wish to change the priority of added codecs, use **Move up** and **Move down** for adjusting the codec display sequence.

> **NOTICE:**
>
> If several codecs have been configured, the codec display sequence determines the priority with which a codec in used. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

7) Select **Save** to copy the settings.

You have now performed codec settings valid across the system.

10.4.9 How to Configure a Dual Network Protocol

You can configure the OpenScape Media Server to operate at IPv4- and IPv6-based networks simultaneously. For this purpose, you need to define the Dual Network Protocol in particular. The OpenScape Media Server uses this protocol to inform communication partners about alternatively available IP addresses.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the link **Streaming-IVR**.

The configuration dialog with the Streaming-IVR provider settings opens.

3) Switch to the **SDP** tab.

4) Select under **Dual Network Protocol (IPV4 / IPV6)** the protocol the OpenScape Media Server is to use for informing communication partners about alternatively available IP addresses.

5) Select **Save** to copy the modifications.

You have thus configured the Dual Network Protocol.

10.4.10 How to Configure the Binary Floor Control Protocol

You can set up the OpenScape Media Server to control the access to the media resources in a dual video conference by configuring the Binary Floor Control Protocol (BFCP).

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

2) In the provider list select the link **Streaming-IVR**.

The configuration dialog with the Streaming-IVR provider settings opens.

3) Switch to the **BFCP** tab.

4) Enter the bind address at the **Bind Address** field, e.g. `auto$IPv4`.

5) Enter the **TCP Port number**. The default value is `5070`.

6) Click **Save**.

You have thus configured the Binary Floor Control Protocol.

10.4.11 How to Add a Terminal

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

You may have to add a terminal for the following reasons:

- For making a new OpenScape Media Server application available.
- For configuring varying security settings for access to an application.
- For configuring varying codec settings for access to an application.
- For configuring a varying RTP routing behavior for access to an application.
- For configuring a varying SIP routing behavior for access to an application.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

2) Select **Add**.

The terminal configuration dialog opens.

3) Specify a unique identifier for the terminal under **Terminal ID**. Under this name the terminal is administered in the Common Management Platform.

4) Select the application to be the terminal's communication endpoint under **Application**.

5) Select the desired option under **Security mode**.

> **IMPORTANT:**
>
> Using SRTP with MIKEY requires the system time of all systems involved in the SRTP communication to be synchronized – OpenScape Media Server, RTP-based devices (e. g. phone), VoIP gateway etc. The Network Time Protocol (NTP) may be used for this purpose.

> **IMPORTANT:**
>
> The keys for encrypting the RTP communication are exchanged via SIP. In case of the **Secureonly** and **Secure preferred** settings it is therefore important to configure the TLS transport protocol in the SIP configuration also.

6) If you have selected an **Application** that uses SIP as connection control protocol, click on the **SIP** button for performing SIP-specific settings.

The configuration dialog for SIP-specific terminal settings opens.

7) Specify the phone number of an OpenScape Voice subscriber under **Billing address**. Call charges incurred by communication connections of the relevant terminal are then assigned to this subscriber.

> **NOTICE:**
>
> In this field only digits and a leading + character are permitted.

8) Select an SIP server line under **Outbound line**.

This SIP server line is used for signaling communication connections for the selected application.

9) Click on **Save** to copy the SIP-specific settings for the terminal.

10) If you wish to define terminal-specific streaming route bindings, execute the following steps.

A streaming route binding specifies which streaming route the OpenScape Media Server uses to transmit connection payloads when the associated connection signaling is handled via a specific listening point.

NOTICE: Terminal-specific streaming route bindings have a higher priority than those valid across the system that you may have configured in the Streaming-IVR provider.

a) Select **Streaming Route Bindings**.

The configuration dialog for terminal-specific streaming route bindings opens. This dialog shows all streaming route bindings configured for the relevant terminal.

b) Select **Define terminal specific binding**.

c) Select under **Listening point** the listening point for which you wish to determine the streaming route for transmitting connection payload.

d) Select under **Streaming route** the streaming route you wish to specify as streaming route for the selected listening point.

e) If required, select under **Alternative streaming route** a streaming route that the OpenScape Media Server is to use as alternative streaming route for the selected listening point.

NOTICE:

You need to specify an alternative streaming route if the OpenScape Media Server is simultaneously connected to an IPv4- and IPv6-based network. In this case, select under **Streaming route** e. g. a route into the IPv4-based network and under **Alternative streaming route** a route into the IPv6-based network.

f) Select **Save** to copy the settings of the streaming route binding address.

g) If required, define further terminal-specific streaming route bindings in the described manner.

h) Select **Close** to close the configuration dialog for terminal-specific streaming route bindings.

11) Execute the following steps to bind at least one phone number to the terminal:

NOTICE:

If you want to specify several phone numbers that cannot be constituted in the form of a single phone number expression, you need to bind at least one more address to the terminal.

a) Click on **Add** in the **Addresses** section.

The configuration dialog for an address opens.

b) Specify the desired phone number expression under **Address-expression**.

This expression defines the phone numbers under which the selected terminal is to be reached in the OpenScape Media Server.

NOTICE:

Always specify the phone numbers in the normalized phone number format – e. g. +492404901100.

NOTICE:

You need to ensure that the phone numbers configured here are routed on the SIP trunk to the OpenScape Media Server in the communications system.

c) Determine under **Type** in which format the specified phone number expression is to be interpreted by the OpenScape Media Server.

d) Click on **OK** to copy the address settings.

e) If required, bind further addresses to the terminal in the described manner.

12) If you wish to use terminal-specific codecs or a terminal-specific codec prioritization for the audio data stream pre-configured by default, execute the following steps:

NOTICE:

If you define terminal-specific codec settings, the codec settings configured system-wide in the Streaming-IVR provider are no longer used for the terminal.

NOTICE:

The codec the OpenScape Media Server eventually uses for a connection also depends on the codecs the connection partner supports. Especially when inbound connections are set up, the connection partner sends the OpenScape Media Server a prioritized list of his/her supported codecs. The OpenScape Media Server then uses this list preferably for specifying the codec to be used.

a) Select the radio button of the audio data stream in the **Streams** section.
b) Click on **Edit** in the **Streams** section.

The data stream configuration dialog opens. This dialog displays a list of the codecs configured system-wide in the Streaming-IVR provider.

c) Click on **Define terminal specific codecs**.

The configuration dialog for adding codecs opens.

d) Select under **Codec** the codec that you wish to use for the audio data stream of the terminal.
e) Select **OK** for adding the new codec to the audio data stream.

In the data stream configuration dialog the list of system-wide configured codecs is replaced with the newly added codec.

f) If required, add further codecs to the audio data stream in the same manner.

NOTICE:

If you add several codecs to the audio data stream, the codec display sequence determines the priority with which a codec in used. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

g) If you wish to change the priority of added codecs, use **Move up** and **Move down** for adjusting the codec display sequence.
h) Select **OK** to copy the data stream settings.

13) If several RTP streaming routes have been configured in the OpenScape Media Server, define the RTP streaming routes the data stream pre-configured by default is to use. Perform the following steps:

NOTICE:

You can define RTP streaming routes for a data stream only if several RTP streaming routes are configured in the OpenScape Media Server.

a) Select the radio button of the audio data stream in the **Streams** section.
b) Click on **Edit** in the **Streams** section.

The data stream configuration dialog opens. In this dialog you see a list of the RTP streaming routes configured in the OpenScape Media Server.

a) Select the checkboxes of the RTP streaming routes the data stream is to use.
b) Select **OK** to copy the data stream settings.

14) If an application that uses further media types in addition to media type **audio** is assigned to a terminal, configure in the terminal a corresponding data stream for every media type used. Perform the following steps:

a) Click on **Add** in the **Streams** section.

> **NOTICE:**
>
> **Add** is unavailable if a data stream has already been added to the terminal for each available media type.

The data stream configuration dialog opens.

b) Select the desired media type under **Media Type**.

> **NOTICE:**
>
> The entry under **Media Type** is allocated and cannot be changed if only the data stream of one media type can be added to the terminal.

c) If required, define the codec settings of the data stream as described.

d) If several RTP streaming routes have been configured for the OpenScape Media Server, select the checkboxes of the RTP streaming routes the data stream is to use.

> **NOTICE:**
>
> You can only see the RTP streaming routes list if more than one RTP streaming route is configured in the OpenScape Media Server.

e) Select **OK** to copy the data stream settings.

15) Click on **Save** to copy the settings for the terminal.

You have thus added a new terminal.

10.4.12 How to Configure the Security Settings for the Communication of an Individual Terminal

You can set an encrypted RTP data transfer for the OpenScape Media Server. You can perform this setting individually for each terminal, thus adjusting the system-wide valid setting of the Streaming-IVR provider for selected terminals.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

2) Select from the list the terminal for which you want to configure the security settings.

   The configuration dialog of the selected terminal opens.

3) Select the desired value under **Security mode**.

> **IMPORTANT:**
>
> Using SRTP with MIKEY requires the system time of all systems involved in the SRTP communication to be synchronized – OpenScape Media Server, RTP-based devices (e. g. phone), VoIP gateway etc. The Network Time Protocol (NTP) may be used for this purpose.

> **IMPORTANT:**
>
> The keys for encrypting the RTP communication are exchanged via SIP. In case of the **Secureonly** and **Secure preferred** settings it is therefore important to configure the TLS transport protocol in the SIP configuration also.

4) Select **Save** to copy the modified setting.

You have thus configured the security settings specific to a terminal.

10.4.13 How to Define Terminal-Specific Codec Settings

You can determine which codecs the OpenScape Media Server uses for in- and outbound RTP communication and also the priority with which the OpenScape Media Server uses these codecs. You can perform such settings for data streams system-wide in the Streaming-IVR provider or terminal-specific. If individual codec settings are specified in the data stream of a terminal, such terminal-specific settings are used preferably.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

> **NOTICE:**
>
> The codec the OpenScape Media Server eventually uses for a connection also depends on the codecs the connection partner supports. Especially when inbound connections are set up, the connection partner sends the OpenScape Media Server a prioritized list of his/her supported codecs. The OpenScape Media Server then uses this list preferably for specifying the codec to be used.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

2) Select from the list the terminal for the RTP communication of which you want to define the codec settings.

The configuration dialog of the selected terminal opens.

3) In the list of configured RTP data streams select the radio button of the data stream for the media type of which you want to define the codec settings.

4) Click on **Edit** in the **Streams** section.

The data stream configuration dialog opens. As a rule, this dialog displays a list of the codecs configured system-wide in the Streaming-IVR provider. If you have already performed terminal-specific codec settings, only those terminal-specific settings are displayed instead.

5) Click on **Define terminal specific codecs**.

The configuration dialog for adding codecs opens.

6) Select under **Codec** the codec that you wish to add to the terminal's data stream.

The OpenScape Media Server can use the following codecs:

Media Type	Codec	Performance Factor [42]	Voice Quality	Use
Audio	G.711A	1	ISDN quality	Default PCM transmission with A-Law for volume compression. Mainly used in Europe.
	G.711µ	1	ISDN quality	Default PCM transmission with µ-Law for volume compression. Mainly used in North America and Japan.
	G.722	2	good	ISDN broadband codec with better voice quality than G.711
	G.729	3	reduced	Compressed voice transmission with speech pause suppression.
	G722.1 (Polycom Siren 7)[43]	-	high (mono)	All media-applications for a better user experience especially during Video-Conference Calls
	G722.1 Appendix C (Polycom Siren 14)[44]	-	high (wideband)	All media-applications for a better user experience especially during Video-Conference Calls

42 The higher the performance factor, the more computing power the OpenScape Media Server needs to expend for the codec.

43 Royalty free offered by Polycom

44 Royalty free offered by Polycom

Media Type	Codec	Performance Factor [42]	Voice Quality	Use
	Telephone-event	low	–	Recognition of outband DTMF (RFC 2833)
Video	H.264	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4 / AVC.
Video	H.265	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4/AVC.

IMPORTANT:

If you do not configure the audio codec **Telephone-event** for a terminal, DTMF signals must be transmitted inband if the OpenScape Media Server is to recognize such DTMF signals. This inband-based recognition requires additional system capacity.

NOTICE:

Using a codec that requires increased computing power reduces the number of channels the OpenScape Media Server supports in parallel.

7) Select **OK** for adding the new codec to the data stream.

8) If required, add further codecs to the data stream in the same manner.

NOTICE:

If you add several codecs to the audio data stream, the codec display sequence determines the priority with which a codec in used. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

9) If you wish to change the priority of added codecs, use **Move up** and **Move down** for adjusting the codec display sequence.

10) Select **OK** to copy the data stream settings.

11) Click on **Save** to copy the changed settings for the terminal.

You have thus performed terminal-specific codec settings.

42 The higher the performance factor, the more computing power the OpenScape Media Server needs to expend for the codec.

10.4.14 How to Prioritize Terminal-Specific Codecs for Use

For the inbound and outbound RTP communication of the OpenScape Media Server you can define the priority with which the OpenScape Media Server uses the codecs that are configured specific to a terminal.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

The codec the OpenScape Media Server eventually uses for a connection also depends on the codecs the connection partner supports. Especially when inbound connections are set up, the connection partner sends the OpenScape Media Server a prioritized list of his/her supported codecs. The OpenScape Media Server then uses this list preferably for specifying the codec to be used.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

2) Select from the list the terminal for the RTP communication of which you want to change the codec settings.

The configuration dialog of the selected terminal opens.

3) In the list of configured RTP data streams select the radio button of the data stream for the media type of which you want to configure the codec prioritization.

4) Click on **Edit** in the **Streams** section.

The configuration dialog of the selected data stream opens. This dialog shows the codecs the OpenScape Media Server uses specific to a terminal.

The codec display sequence determines the priority with which a codec is used. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

5) If you wish to change the priority of added codecs, use **Move up** and **Move down** for adjusting the codec display sequence.

6) Select **OK** to copy the data stream settings.

7) Click on **Save** to copy the changed settings for the terminal.

You have thus defined, with which priority the OpenScape Media Server uses the codecs that are configured specific to a terminal.

10.4.15 How to Remove a Codec from Terminal-Specific Settings

You can determine which codecs the OpenScape Media Server uses for in- and outbound RTP communication of the OpenScape Media Server terminal-specific for each media type.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.
2) Select from the list the terminal for the RTP communication of which you want to change the codec settings.

   The configuration dialog of the selected terminal opens.
3) In the list of configured RTP data streams select the radio button of the data stream for the media type of which you want to change the codec settings.
4) Click on **Edit** in the **Streams** section.

   The configuration dialog of the selected data stream opens. This dialog shows the codecs the OpenScape Media Server uses specific to a terminal.
5) Select in the list of terminal-specific codecs the codec you wish to remove from the codec settings.
6) Select **Remove**.

   The selected codec is removed from the list of terminal-specific codecs.
7) Select **OK** to copy the data stream settings.
8) Click on **Save** to copy the changed settings for the terminal.

You have thus removed a codec from the terminal-specific settings.

10.4.16 How to Reset Terminal-Specific Codec Settings

For the inbound and outbound RTP communication of the OpenScape Media Server you can define terminal-specific for each media type which codecs the OpenScape Media Server uses with which priority. You can reset this terminal-specific setting to the codec settings valid across the system, which have been configured in the Streaming-IVR provider.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

2) Select from the list the terminal for the RTP communication of which you want to reset the terminal-specific codec settings.

   The configuration dialog of the selected terminal opens.

3) In the list of configured RTP data streams select the radio button of the data stream for the media type of which you want to reset the terminal-specific codec settings.

4) Click on **Edit** in the **Streams** section.

   The configuration dialog of the selected data stream opens. This dialog displays the terminal-specific codec settings.

5) Select **Reset to default codecs**.

   You see the codec settings valid across the system instead of the terminal-specific ones.

6) Click on **OK** to copy the settings for the data stream.

7) Click on **Save** to copy the changed settings for the terminal.

You have thus reset the terminal-specific codecs to the codec settings valid across the system.

10.4.17 How to Add a Data Stream

The audio data stream is configured for every new terminal by default. If an application that uses further media types in addition to media type audio is assigned to a terminal, you can add an additional data stream for each further media type in the terminal.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

NOTICE:

Not more than one data stream per media type can be configured in each terminal.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

2) Select from the list the terminal to which you wish to add an additional data stream.

   The configuration dialog of the selected terminal opens.

3) Click on **Add** in the **Streams** section.

> **NOTICE:**
>
> **Add** is unavailable if a data stream has already been added to the terminal for each available media type.

The data stream configuration dialog opens.

4) Select the desired media type under **Media Type**.

> **NOTICE:**
>
> The entry under **Media Type** is allocated and cannot be changed if only the data stream of one media type can be added to the terminal.

5) If required, define the codec settings of the data stream as described.
6) If several RTP streaming routes have been configured for the OpenScape Media Server, select the checkboxes of the RTP streaming routes the data stream is to use.

> **NOTICE:**
>
> You can only see the RTP streaming routes list if more than one RTP streaming route is configured in the OpenScape Media Server.

7) Click on **OK** to copy the settings for the data stream.
8) Click on **Save** to copy the settings for the terminal.

You have thus added another data stream to a terminal.

10.4.18 How to Configure Settings for System, Security and Remote Access

The settings for system, security and remote access let you control how external systems can access the OpenScape Media Server. This includes e. g. the OpenScape system monitor accessing the statistics framework of the OpenScape Media Server using JMX (Java Management eXtensions).

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
2) In the provider list select the **System, Security and Remote Access** link.

   The configuration dialog with the settings of the provider System, Security and Remote Access opens.

3) Specify in the **Bind Address** field under **JMX (Java Management eXtensions)** the IP address under which the Java Management eXtensions can be reached on the OpenScape Media Server.

   If you want the Java Management eXtensions to be reached only locally from the computer system of the OpenScape Media Server, enter value `localhost` here.
4) Leave the settings of all other fields unchanged.
5) Select **Save**.
6) Enable the radio button for the provider **System, Security and Remote Access**.
7) Click on **Restart Provider**.

> **IMPORTANT:**
>
> Restarting the provider System, Security and Remote Access interrupts all external accesses via JMX and HTTP that exist at the time of the reboot. Before the reboot you can switch to the **Monitoring** tab to see whether connections are currently active.

You have now changed the settings of the provider System, Security and Remote Access.

10.4.19 How to Configure an Application

You can configure the OpenScape Media Server applications in individual configuration dialogs. The layout of an application's configuration dialog depends on the individual configuration module of the relevant application. If an application does not provide an individual configuration module, the OpenScape Media Server uses a generic configuration dialog.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the configuration dialog switch to the **Applications** tab.
2) Select the application that you want to configure.

The configuration dialog of the selected application opens.

10.4.20 TLS Certificate of the OpenScape Media Server

So that the OpenScape Media Server can encrypt data via TLS, it needs a corresponding certificate. Therefore, the OpenScape Media Server keystore already contains the default certificate of the OpenScape Media Server signed with the default certificate authority (CA) of OpenScape Voice. With this certificate the OpenScape Media Server is accepted by OpenScape Voice as authorized communication partner, as long as you use the default certificate authority of OpenScape Voice. If you wish to use an individual certificate authority or an individual certificate, you need to import a new certificate in the OpenScape Media Server.

NOTICE:

A certificate is only required if the OpenScape Media Server is used under OpenScape UCApplication.

The OpenScape Media Server is installed with the following Java keystore by default:

`tls-keystore.jks`

You find this keystore in the following OpenScape Media Server directory:

<MS#Install [45]>`/mediaserver/application_host/providers/sip-connectivity`

10.4.20.1 How to Back up an Existing Keystore

Before you modify the OpenScape Media Server keystore you need to save the original keystore.

Step by Step

1) Switch to the following directory on the computer system of the OpenScape Media Server:

<MS#Install [46]>`/mediaserver/application_host/providers/sip-connectivity`

2) Create a copy of the following file and save this copy to a secure location on the computer system:

`tls-keystore.jks`

You have now saved the original OpenScape Media Server keystore and may restore the original state at a later date.

10.4.20.2 How to Remove the Default Certificates from the Keystore

Before you can import new certificates for the default aliases in the OpenScape Media Server keystore, you need to remove the relevant certificates installed by default from the keystore.

IMPORTANT:

The certificate with the alias *polycomequipmentca* must not be removed from the OpenScape Media Server keystore.

45 <MS-Install > is the setup directory of the OpenScape Media Server: `/opt/siemens/` or `/enterprise/`

46 <MS-Install > is the setup directory of the OpenScape Media Server: `/opt/siemens/` or `/enterprise/`

Step by Step

1) Switch to the following directory on the computer system of the OpenScape Media Server:

   <MS#Install [47]>`/mediaserver/application_host/providers/sip-connectivity`

2) Execute the following command in one line to remove the default certificate of the OpenScape Voice certificate authority from the OpenScape Media Server keystore:

   ```
   /opt/siemens/share/ibm-java-<version>/jre/bin/keytool
   -delete
   -alias rootca_h8k
   -keystore tls-keystore.jks
   ```

3) Execute the following command in one line to remove the default certificate and default key of the OpenScape Media Server from the OpenScape Media Server keystore:

   ```
   /opt/siemens/share/ibm-java-<version>/jre/bin/keytool
   -delete
   -alias mediaserver
   -keystore tls-keystore.jks
   ```

4) Execute the following command in one line to check whether the relevant certificates and keys have been correctly removed from the OpenScape Media Server keystore:

   ```
   /opt/siemens/share/ibm-java-<version>/jre/bin/keytool
   -list
   -v
   -keystore tls-keystore.jks
   ```

   No certificates with the aliases *mediaserver* or *rootca_h8k* should now be displayed anymore.

The relevant certificates installed by default and the keys are removed from the keystore. You can now import new certificates and keys for the default aliases in the OpenScape Media Server keystore.

10.4.20.3 How to Import the Certificate and Key of the OpenScape Media Server

You need to import the new certificate of the OpenScape Media Server and the associated pair of keys in the OpenScape Media Server keystore.

Prerequisites

You have a PEM file that contains the following: the pair of keys created of the OpenScape Media Server.

47 <MS-Install > is the setup directory of the OpenScape Media Server: `/opt/siemens/` or `/enterprise/`

NOTICE:

By a comprehensive example, the general process on how to generate a new key pair is described in the manual *OpenScape UC Application, Configuration and Administration*. Derive e.g. from the explanations for the application computer how to generate a new key pair for the OpenScape Media Server.

You have a CRT file that contains the following: the certificate for the OpenScape Media Server signed by the certificate authority.

NOTICE:

By a comprehensive example, the general process on how to create a signed certificate from a new pair of keys is described in the manual *OpenScape UC Application, Configuration and Administration*. Derive e.g. from the explanations for the application computer how to create a signed certificate for the OpenScape Media Server.

Step by Step

1) Switch to the following directory on the computer system of the OpenScape Media Server:

<MS#Install [48]>`/mediaserver/application_host/providers/sip-connectivity`

2) Execute the following command in one line to combine the pair of keys (`*.pem`) and the signed certificate (`*.crt`) of the OpenScape Media Servers password protected in a PKCS#12 file:

`openssl pkcs12`

`-export`

`-in` *<path and name of the CRT file>*

`-inkey` *<path and name of the PEM file>*

`-name mediaserver`

`-out media-temp.p12`

NOTICE:

If the system prompts you for a password while you execute the command, enter password `password`.

The password protected PKCS#12 file `media-temp.p12` is stored in the local directory.

48 <MS-Install > is the setup directory of the OpenScape Media Server: `/opt/siemens/` or `/enterprise/`

3) Execute the following command in one line to import the pair of keys and the signed certificate of the OpenScape Media Server in the form of the PKCS#12 file `media-temp.p12` in the OpenScape Media Server keystore:

```
/opt/siemens/share/ibm-java-<version>/jre/bin/keytool
-importkeystore
-deststorepass password
-destkeypass password
-destkeystore tls-keystore.jks
-srckeystore media-temp.p12
-srcstoretype PKCS12
-srcstorepass password
-alias mediaserver
```

4) Execute the following command in one line to check whether the pair of keys and the signed certificate of the OpenScape Media Server have been imported in the OpenScape Media Server keystore correctly:

```
/opt/siemens/share/ibm-java-<version>/jre/bin/keytool
-list
-v
-keystore tls-keystore.jks
```

A certificate with the alias *mediaserver* should now be displayed.

You have thus imported the pair of keys and the signed certificate of the OpenScape Media Server correctly in the OpenScape Media Server keystore.

10.4.20.4 How to Import the Certificate of the Root Certificate Authority

For the new certificate of the OpenScape Media Server to be acknowledged as valid by a communication partner, the certificate of the associated certificate authority too must be imported in the OpenScape Media Server keystore.

Prerequisites

You have a CRT file that contains the following: the self-signed certificate of the certificate authority that has issued the newly imported certificate of the OpenScape Media Server.

Step by Step

1) Switch to the following directory on the OpenScape Media Server computer system:

<MS#Install [49]>`/mediaserver/application_host/providers/sip-connectivity`

49 <MS-Install > is the setup directory of the OpenScape Media Server: `/opt/siemens/` or `/enterprise`/

2) Execute the following command in one line to import the certificate of the new certificate authority in the OpenScape Media Server keystore:

```
/opt/siemens/share/ibm-java-<version>/jre/bin/keytool
-import -trustcacerts
-alias rootca
```

`-file` *<path and name of the CRT file>*

```
-keystore tls-keystore.jks
```

3) Execute the following command in one line to check whether the certificate of the new certificate authority has been correctly imported in the OpenScape Media Server keystore:

```
/opt/siemens/share/ibm-java-<version>/jre/bin/keytool
-list
-v
-keystore tls-keystore.jks
```

A certificate with the alias *rootca* should now be displayed.

You have now correctly imported the certificate of the new certificate authority in the OpenScape Media Server keystore.

10.4.20.5 How to Activate the new Certificate

So that the new certificate is used you need to reboot the OpenScape Media Server services.

Step by Step

Execute the following command on the computer system of the OpenScape Media Server to reboot the Media Server services:

```
/etc/init.d/symphoniad restart
```

The OpenScape Media Server now uses the new certificate.

11 Monitoring Operating Parameters of the OpenScape Media Server

Central operating parameters of the OpenScape Media Server can be monitored via the OpenScape Media Server configuration dialog.

The OpenScape Media Server monitors operating parameters for the following areas:

- SIP
- MGCP
- Streaming

11.1 Monitored Application Sessions

The OpenScape Media Server monitors the connection sessions that exist with the OpenScape Media Server applications.

All existing connection sessions are represented in the form of a table. The following information of each connection session is displayed:

- **Applet**

  Specifies the application of the OpenScape Media Server with which the connection session exists.
- **Seconds since created**

  Indicates how long the connection session for the relevant application exists without interruption.
- **Seconds since last task**

  Indicates the period in which the relevant application has not processed any task requests as regards the respective connection session anymore.

11.2 Monitored Streaming Operating Parameters

The OpenScape Media Server monitors different streaming operating parameters.

NOTICE:

All accumulated counters are reset when the OpenScape Media Server is rebooted.

- **Number of call endpoints**

  Number of all Media-Server-internal call endpoints currently occupied. Every inbound and outbound call allocates a call endpoint in the OpenScape Media Server that processes the associated RTP data stream.
- **Number of audio RTP data streams**

  Number of all currently active audio data streams.

- **Number of dialog endpoints**

  Number of all Media-Server-internal dialog endpoints currently occupied. Every inbound and outbound call that demands announcements, TTS or ASR services allocates a dialog endpoint in the OpenScape Media Server.
- **Number of endpoints**

  Number of all Media-Server-internal communication endpoints currently occupied. Such communication endpoints comprise the endpoints for calls, conferences and dialog communication.
- **Number of G711 data streams**

  Number of all audio data streams currently active with G.711 coding.
- **Number of G722 data streams**

  Number of all audio data streams currently active with G.722 coding.
- **Number of G722.1 (Polycom Siren 7) data streams**

  Number of all audio data streams currently active with G.722.1 (Polycom Siren 7) coding
- **Number of G722.1 Appendix C (Polycom Siren 14) data streams**

  Number of all audio data streams currently active with G.722.1 (Polycom Siren 14) coding
- **Number of G729 data streams**

  Number of all audio data streams currently active with G.729 coding.
- **Number of conference endpoints**

  Number of all Media-Server-internal conference endpoints that are currently occupied. Every conference allocates a conference endpoint in the OpenScape Media Server that mixes the involved RTP data streams.
- **Number of video RTP data streams**

  Number of all currently active video data streams.
- **Sum of audio RTP data streams**

  Number of all audio data streams that were and are active since the last OpenScape Media Server start.
- **Sum of end points**

  Number of all connection endpoints of the OpenScape Media Server that were and are active since the last OpenScape Media Server start.
- **Sum of G711 data streams**

  Number of all audio data streams with G.711 coding that were and are active since the last OpenScape Media Server start.
- **Sum of G722 data streams**

  Number of all audio data streams with G.722 coding that were and are active since the last OpenScape Media Server start.
- **Sum of G722.1 (Polycom Siren 7) data streams**

  Number of all audio data streams with G.722.1 (Polycom Siren 7) coding that were and are active since the last OpenScape Media Server start.
- **Sum of G722.1 Appendix C (Polycom Siren 14) data streams**

  Number of all audio data streams with G.722.1 Appendix C (Polycom Siren 14) coding that were and are active since the last OpenScape Media Server start.

- **Sum of G729 data streams**

  Number of all audio data streams with G.729 coding that were and are active since the last OpenScape Media Server start.
- **Sum of video RTP data streams**

  Number of all video data streams that were and are active since the last OpenScape Media Server start.

11.3 Monitored MGCP Operating Parameters

The OpenScape Media Server monitors different MGCP operating parameters.

NOTICE:

All accumulated counters are reset when the OpenScape Media Server is rebooted.

- **Current connections**

  Number or currently existing MGCP connections.
- **Requests per minute**

  Number of MGCP connection requests in the last minute.
- **Requests per hour**

  Number of MGCP connection requests in the last hour.
- **Number of requests**

  Number of MGCP connection requests received since the last OpenScape Media Server start.
- **Number of announcement endpoints**

  Number of Media-Server-internal connection endpoints that are currently occupied for OpenScape Voice announcement connections.
- **Number of responses**

  Number of sent MGCP responses since the last OpenScape Media Server start.
- **Number of ES endpoints**

  Number of Media-Server-internal connection endpoints that are currently occupied for OpenScape Voice monitoring connections.
- **Number of inactive endpoints**

  Number of Media-Server-internal connection endpoints that are currently available but not occupied.
- **Number of conference endpoints**

  Number of all Media-Server-internal conference endpoints that are currently occupied. Every MGCP-controlled conference allocates a conference endpoint in the OpenScape Media Server that mixes the involved RTP data streams.
- **Number of NTFYs**

  Number of sent MGCP notifications (NTFY) since the last OpenScape Media Server start.

- **Number of RQNTs**

  Number of received MGCP notification requests (RQNT) since the last OpenScape Media Server start.
- **Number of invalid requests**

  Number of invalid MGCP connection requests since the last OpenScape Media Server start.
- **Number of connection timeouts**

  Number of MGCP connections that were closed since the last OpenScape Media Server start because of a timeout.
- **Number of rejected requests**

  Number of MGCP connection requests rejected since the last OpenScape Media Server start.
- **Average response time**

  Average time it took the OpenScape Media Server to response to MGCP connection requests. Calculating this average time is based on the last 100 MGCP transactions.
- **Average processing time**

  Average time for processing MGCP connection requests. Calculating this average time is based on the last 100 MGCP transactions.

11.4 Monitored SIP Operating Parameters

The OpenScape Media Server monitors different SIP operating parameters.

NOTICE:

All accumulated counters are reset when the OpenScape Media Server is rebooted.

- **Current number of established connections**

  Number of SIP connections that currently exist.
- **Current number of connections being set up**

  Number of SIP connections being set up.
- **Current number of connections being closed**

  Number of SIP connections being closed.
- **Current connections**

  Number of SIP connections that the OpenScape Media Server is processing according to their respective connection status.
- **Runtime**

  Time that elapsed since the last OpenScape Media Server start.

  Representation format: <SS>:<MM>:<ss>
- **Max. number of simultaneous connections of the current hour**

  Maximum number of simultaneously existing SIP connections in the current hour.

- **Max. number of simultaneous connections of the current day**

  Maximum number of simultaneously existing SIP connections within the current day.
- **Maximum total number of simultaneous connections**

  Maximum number of simultaneously existing SIP connections since the last OpenScape Media Server start.
- **Sum of established connections**

  Number of SIP connections set up since the last OpenScape Media Server start.
- **Sum of connections**

  Number of SIP connection requests since the last OpenScape Media Server start.
- **Sum of requests rejected because of overload**

  Number of SIP connection requests rejected since the last OpenScape Media Server start because of overload.
- **Sum of rejected connections**

  Number of SIP connection requests rejected since the last OpenScape Media Server start.

11.5 How to Display Monitored Operating Parameters of the OpenScape Media Server

You can display central operating parameters that the OpenScape Media Server monitors.

Prerequisites

The configuration dialog of the OpenScape Media Server to be configured is open.

Step by Step

1) In the OpenScape Media Server configuration dialog switch to the **Monitoring** tab.
2) Select **Details** for the operating parameter group the parameters of which you want to display.

You see the operating parameters monitored for the OpenScape Media Server.

12 OpenScape Media Server Logging

Logging for operating the OpenScape Media Server is configured via the Common Management Platform. For this purpose, Log4J configuration files are used, which can be loaded with the Common Management Platform. Preconfigured configuration files are shipped with the Common Management Platform, which can be adjusted if required.

IMPORTANT:

Logging may consume a significant amount of computing power of the Media Server system. This may deteriorate the OpenScape Media Server system performance from the user's point of view.

Therefore, always only activate logging in periods when you really need to look for errors. In addition, always only activate the log categories and log levels required for the error search.

The log files for the OpenScape Media Server live operation are stored on the computer system of the OpenScape Media Server in one of the following directories:

- `/log`
- `/var/siemens/common/log`

The log files are named as follows:

- `symphonia.log`
- `symphonia.log.<consecutive number>.`

You can display these log files with any text editor.

The logging information written in the log files during the OpenScape Media Server operation is determined by two settings:

- The OpenScape Media Server log categories
- The log levels of the log categories

You find detailed information about Log4J under the following address:

`http://logging.apache.org/log4j/1.2/manual.html`

12.1 Log Categories of the OpenScape Media Server

The log categories are used to specify which components of the OpenScape Media Server issue log messages.

The OpenScape Media Server log categories have a fixed notation.

Example:

`com.cycos.connectivity.sip`

12.2 Log Level of the Log Categories

The log level defines for each log category how detailed the associated system messages are put out.

In the Log4J configuration files you can use the following log levels for the OpenScape Media Server log categories.

- **FATAL**
- **ERROR**
- **WARN**
- **INFO**
- **UNEXPECTED**
- **DEBUG**
- **FINE**
- **FINEST**

FATAL

A log message of the **FATAL** level logs the crash of a central system component or of the entire OpenScape Media Server.

Example: Crash of the runtime environment of the OpenScape Media Servers.

ERROR

A log message of the **ERROR** level logs a serious system error that cannot be fixed independently by the system. A serious system error will in most cases cause the relevant OpenScape Media Server function not to work properly anymore.

Example: Network connection crash.

WARN

A log message of the **WARN** level points to potential system problems. The administrator should rectify the cause for this message.

Example: Message about errors in the configuration of a system component.

INFO

A log message of the **INFO** level points to processes in the smooth OpenScape Media Server operation.

Example: Message about the error-free start of a system component.

UNEXPECTED

A log message of the **UNEXPECTED** level is created when an unexpected event occurs that does not negatively affect the OpenScape Media Server operation, though.

Example: Start of a system component that has already been booted.

DEBUG

A log message of the **DEBUG** level contains general system information for locating a system error.

FINE

A log message of the **FINE** level contains detailed system information about interfaces or protocol stacks of the OpenScape Media Server.

FINEST

A log message of the **FINEST** level contains detailed system information for software developers. Based on this information, errors can be located on the level of the program code.

12.3 Default Log4J Configuration Files for the OpenScape Media Server

Pre-configured Log4J configuration files are already installed with the OpenScape Media Server. You may adjust and activate them via the Common Management Platform.

The following Log4J configuration files are installed with the OpenScape Media Server:

- `log4j_mediaserver_basic.xml`
- `log4j_mediaserver_configuration.xml`
- `log4j_mediaserver_essential.xml`

  Activates the most important log categories of the OpenScape Media Server.
- `log4j_mediaserver_full_log.xml`

  Activates all log categories of the OpenScape Media Server.
- `log4j_mediaserver_mgcp.xml`

  Activates all log categories that are important for MGCP monitoring.
- `log4j_mediaserver_sip.xml`

  Activates all log categories that are important for SIP monitoring.
- `log4j_mediaserver_streaming.xml`

  Activates all log categories that are important for RTP monitoring.
- `log4j_mediaserver_vxml.xml`

  Activates all log categories that are important for VoiceXML monitoring.

13 Raw Statistics Data of the OpenScape Media Server

The OpenScape Media Server uses a statistics framework for collecting detailed statistics data about the OpenScape Media Server operation. Such collected statistics data comprise in particular information about internally used Media Server entities and their interaction. The Statistics framework provides the collected information in the form of raw statistics, which can be further processed using external statistics applications.

You can use raw statistics especially for the following purposes:

- For monitoring the status of the most important Media Server entities in real time. Such entities include:
  - Application Host sessions
  - SIP connections
  - MGCP connections
  - Terminals
  - Data streams
  - Streaming endpoints
  - MGCP endpoints
- For creating individual statistics reports that reflect the communication behavior and the load of the OpenScape Media Server.
- For creating entity and sequence diagrams that optimize error analysis and error correction.

The OpenScape Media Server can put out the collected raw statistics data in the following ways:

- In a file system with several files, which are filled linear or using the round-robin method.

  NOTICE:

  Writing in a file system using the round robin method is the default setting for the statistics output of the OpenScape Media Server.

- In a Media-Server-internal database table.
- Via a socket client or server-based.

Controlling the Output of Raw Statistics Files

You can customize the output of the collected raw statistics data in a file system. To this, the following configuration file exists:

`statistic-framework.xml`

You find this configuration file on the computer system of the OpenScape Media Server in the following directory.

<MS#Install [50]>`/common/conf`

50 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

13.1 Raw Statistics Output in a File System

The OpenScape Media Server can put out the collected raw statistics data in a file system.

There are two output options.

- Round-robin output

  The OpenScape Media Server uses a file system with a default of 20 files, which are filled using the round-robin method. Each of these files may amount up to 50 MB by default.

  This type of output is default.
- Linear output

  The OpenScape Media Server uses a file system with any number of files that can adopt any size. In this case a timer defines the period in which the collected raw statistics data is written in the same file. When the time is up, another file is created and the timer starts all over again from zero.

> **NOTICE:**
>
> With this setting the single files may quickly become rather big; approximately 10 – 20 KB of data is created per connection.

In both cases the files of the file system are stored in the following directory of the OpenScape Media Server by default.

<MS#Install [51]>`/logs/traces`

The statistics files are named by default as follows:

`statistic-data.txt.<consecutive number>`

Controlling the Output of Raw Statistics Files

The following parameters control the statistics output in a file system:

- `property name="Append"`

  Defines whether statistics data is appended to the content of a file if a file of the required name already exists (`Append = true`), or whether files are always newly created instead (`Append = false`).

  This parameter is valid for the round-robin as well as linear output.

  The default setting for **Append** is **false**.
- `property name="File"`

  Defines the storage location and the basic file name for the statistics files. The specified file name is subsequently extended with a consecutive number.

  This parameter is valid for the round-robin as well as linear output.

  The default setting for **File** is:

  `${SYMPHONIA_LOG}/traces/statistic-data.txt`

51 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

- `property name="BackupInterval"`

  If the linear output shall be used, this parameter defines how long the raw statistics data is written in a single file.

  The default setting for **BackupInterval** is **0**. Linear output is then inactive.

  You can specify one of the following units for **BackupInterval**.

  – **ms** for milliseconds
  – **s** for seconds
  – **m** for minutes
  – **h** for hours
  – **d** for days

  If you do not specify a unit, the OpenScape Media Server uses the unit for milliseconds by default.

  > **NOTICE:**
  >
  > If this parameter is active in the configuration file, the settings for the parameters **MaxFileSize** and **MaxBackupFiles** are disregarded.

- `property name="MaxFileSize"`

  If you wish to use the round-robin output, this parameter defines the maximum size of each of the statistics files. When this size has been reached, the next file of the file system is filled.

  The default setting for **MaxFileSize** is **50 MB**.

  You can specify one of the following units for **MaxFileSize**.

  – **KB** for kilobytes
  – **MB** for megabytes
  – **GB** for gigabytes
  – **TB** for terabytes

  If you do not specify a unit, the OpenScape Media Server uses the unit for kilobytes by default.

  > **NOTICE:**
  >
  > When you activate this parameter in the configuration file, you definitely need to comment out the parameter **BackupInterval** at the same time.

- `property name="MaxBackupFiles"`

  If you wish to use the round-robin output, this parameter defines the total number of statistics files that may be used.

  The default setting for **MaxBackupFiles** is **20**.

  > **NOTICE:**
  >
  > When you activate this parameter in the configuration file, you definitely need to comment out the parameter **BackupInterval** at the same time.

13.1.1 How to Configure Linear File Output for Raw Statistics

You can customize the linear file output of the collected raw statistics data in the associated configuration file.

Step by Step

1) Open the following configuration file in a text editor:

   `statistic-framework.xml`

   You find this configuration file in the following directory:

   <MS#Install [52]>`/common/conf`

2) Search the configuration file for the section the beginning of which is marked with the following **appender class**:

   `com.cycos.statistic.tracing.impl.RollingFileAppender`

3) Specify under **File** under which file name and in which directory the raw statistics files are to be stored.
4) Remove the comment for the **BackupInterval** parameter.
5) Specify under **BackupInterval** how long raw statistics data is to be written in a statistics file. When this time is up, a new statistics file is created.

   Example: `1h`

   Use one of the following units for the specified value:

   - **ms** for milliseconds
   - **s** for seconds
   - **m** for minutes
   - **h** for hours
   - **d** for days

   If you do not specify a unit, the OpenScape Media Server uses the unit for milliseconds by default.

   NOTICE:

   If you choose a setting too great, the single files may quickly become rather big; approximately 10 – 20 KB of data is created per connection.

   NOTICE:

   If this parameter is active in the configuration file, the settings for the parameters **MaxFileSize** and **MaxBackupFiles** are disregarded.

6) Leave all other settings of the configuration file unchanged.
7) Save the changes in the configuration file.

You have now configured linear database output for raw statistics data.

52 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

13.1.2 How to Configure Round-Robin File Output for Raw Statistics

You can customize the round-robin output of the collected raw statistics data in the associated configuration file.

Step by Step

1) Open the following configuration file in a text editor:

   `statistic-framework.xml`

   You find this configuration file in the following directory:

   <MS#Install [53]>`/common/conf`

2) Search the configuration file for the section the beginning of which is marked with the following **appender class**:

   `com.cycos.statistic.tracing.impl.RollingFileAppender`

3) Specify under **File** under which file name and in which directory the raw statistics files are to be stored.

4) Specify the maximum size of the single raw statistics files under **MaxFileSize**.

   Example: `100MB`

   Use one of the following units for the specified value:

   - **KB** for kilobytes
   - **MB** for megabytes
   - **GB** for gigabytes
   - **TB** for terabytes

   If you do not specify a unit, the OpenScape Media Server uses the unit for kilobytes by default.

5) Specify under **MaxBackupFiles** how many raw statistics files are to be used for the round-robin output.

6) Verify that the **BackupInterval** setting is commented out.

   The settings **MaxFileSize** and **MaxBackupFiles** will otherwise not be considered and the OpenScape Media Server uses the linear file output.

7) Leave all other settings of the configuration file unchanged.

8) Save the changes in the configuration file.

You have thus configured the round-robin output for the raw statistics data.

13.2 Server-based Raw Statistics Output via a Socket

The OpenScape Media Server can provide the collected raw statistics data via a socket from where it can be read out by an independent statistics client.

The following parameter controls the server-based statistics output via a socket:

53 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

- `property name="Port"`

  Defines the number of the local port via which an independent statistics client can read out the collected raw statistics data.

  The default setting for **Port** is **7 000**.

13.2.1 How to Configure the Server-based Socket Output for Raw Statistics

You can customize the server-based socket output of the collected raw statistics data in the associated configuration file.

Step by Step

1) Open the following configuration file in a text editor:

`statistic-framework.xml`

You find this configuration file in the following directory:

<MS#Install [54]>`/common/conf`

2) Search the configuration file for the section the beginning of which is marked with the following **appender class**:

`com.cycos.statistic.tracing.impl.SocketHubAppender`

3) Specify under **Port** the number of a local port via which the OpenScape Media Server is to put out the raw statistics data.

> **NOTICE:**
>
> This port needs to be released in a firewall possibly used.

4) Leave all other settings of the configuration file unchanged.

5) Save the changes in the configuration file.

You have thus configured the server-based socket output for the raw statistics data.

13.3 Client-based Raw Statistics Output via a Socket

The OpenScape Media Server can send the collected raw statistics data to a port of an independent statistics server. There, the raw statistics data can then be prepared to individual purpose.

The following parameters control the client-based statistics output via a socket:

- `property name="Host"`

  Defines the IP address of the computer system to which the OpenScape Media Server is to send the raw statistics data.

  The default setting for **Host** is **localhost**.

54 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

- `property name="Port"`

  Defines the number of the port to which the OpenScape Media Server is to send the raw statistics data.

  The default setting for **Port** is **7 000**.

13.3.1 How to Configure the Client-based Socket Output for Raw Statistics

You can customize the client-based socket output of the collected raw statistics data in the associated configuration file.

Step by Step

1) Open the following configuration file in a text editor:

`statistic-framework.xml`

You find this configuration file in the following directory:

<MS#Install [55]>`/common/conf`

2) Search the configuration file for the section the beginning of which is marked with the following **appender class**:

`com.cycos.statistic.tracing.impl.SocketAppender`

3) Remove the comment for the entire appender class.

4) Specify under **Host** the IP address of the computer system to which the OpenScape Media Server is to send the raw statistics data.

5) Specify under **Port** the number of the port to which the OpenScape Media Server is to send the raw statistics data.

NOTICE:

This port needs to be released in a firewall possibly used.

6) Leave all other settings of the configuration file unchanged.

7) Save the changes in the configuration file.

You have thus configured the client-based socket output for the raw statistics data.

13.4 Raw Statistics Output in an Internal Database Table

The OpenScape Media Server can file collected raw statistics data in a Media-Server-internal database table. There the data can be read out by an independent statistics client.

The following parameters control the statistics output in a Media-Server-internal database table:

55 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

- `property name="MaxDatabaseSize"`

  Defines the maximum number of rows the Media-Server-internal database source may allocate. Every row offers space for the data of one statistics event.

  If the specified table size has been reached, the database table is completely emptied before the next statistics data is stored in it.

  The default setting for **MaxDatabaseSize** is **200 000**.
- `property name="GarbageCollectionInterval"`

  Defines a period in milliseconds after which the OpenScape Media Server checks whether the size of the Media-Server-internal database table has exceeded its upper limit (**MaxDatabaseSize**).

  If the upper limit has been reached, the database table is completely emptied before the next statistics data is stored in it.

  The default setting for **GarbageCollectionInterval** is **1 000**.

13.4.1 How to Configure the Database Output for Raw Statistics

You can customize the database output of the collected raw statistics data in the associated configuration file.

Step by Step

1) Open the following configuration file in a text editor:

`statistic-framework.xml`

You find this configuration file in the following directory:

<MS#Install [56]>`/common/conf`

2) Search the configuration file for the section that is introduced with the following **appender class**:

`com.cycos.statistic.tracing.impl.DatabaseAppender`

3) Remove the comment for the entire appender class.

4) Specify under **MaxDatabaseSize** the maximum number of rows the Media-Server-internal database table may contain before it is completely emptied.

5) Specify under **GarbageCollectionInterval** a period in milliseconds after which the OpenScape Media Server checks whether the size of the database table has exceeded its upper limit (**MaxDatabaseSize**).

6) Leave all other settings of the configuration file unchanged.

7) Save the changes in the configuration file.

8) Reboot the OpenScape Media Server for changed settings to take effect.

You have now configured the database output for raw statistics data.

56 <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ or /enterprise/

14 OpenScape Media Server Error Management

In case of an error the OpenScape Media Server generates an error message and transfers this message to the error management of the Common Management Platform. The Common Management Platform then takes over the further processing of the information collected in this way.

The OpenScape Media Server error messages are divided into the following categories:

- Application Host Service
- Host-IVR component
- Media Framework component
- Media Processing provider
- Media Gateway provider
- MRCP client
- SIP provider

14.1 Application Host Service

The OpenScape Media Server supports the following error messages for the Application Host Service:

Table 3: Error messages of the Application Host Service

ID	Message	Description
1000	Unknown application host fault	An unknown error occurred in the Application Host Service.
1001	ApplicationHost configuration fault	The configuration of the Application Host Service is invalid.
1002	Failed to instantiate ApplicationHost	Error on starting the Application Host Service. No Application Host Container could be instantiated.

14.2 Media Framework Component

The OpenScape Media Server supports the following error messages for the Media Framework component:

Table 4: Error messages of the Media Framework component

ID	Message	Description
1000	Unknown MFW fault	Unspecified Media Framework Component fault.
1001	Native Media Framework startup failed	Java could not start the native Media Framework part.

ID	Message	Description
1002	Native Media Framework not responding	The native Media Framework part does not react to system requests any more. An error may have caused the components crash.
1003	Java Media Framework receive socket overrun	The Media Framework receive socket (Java part) receives to many data.
1004	Native Media Framework receive socket overrun	The Media Framework receive socket (native part) receives to many data.
1005	Java Media Framework receive socket sequence error	The Media Framework receive socket (Java part) has experienced a loss of messages.
1006	Native Media Framework receive socket sequence error	The Media Framework receive socket (native part) has experienced a loss of messages.
1007	Native Media Framework socket error	In the native part of the Media Framework, linking up to a socket failed.
1008	Java Media Framework unrecoverable error	In the Java part of the Media Framework, an error that cannot be eliminated leads to a permanent loss of system services.
1009	Native Media Framework unrecoverable error	In the native part of the Media Framework, an error that cannot be eliminated leads to a permanent loss of system services.
1010	Native Media Framework out of memory	In the native part of the Media Framework, memory allocation failed.
1011	Native Media Framework out of UDP ports	In the native part of the Media Framework, UDP port allocation failed.
1012	Native Media Framework crypto session not found	The key management does not have an encryption session.
1013	Native Media Framework srtp error	The native part of the Media Framework returned an SRTP error.
1014	Native Media Framework keyManagement fatal error	The key management is in a state of error that cannot be rectified.

ID	Message	Description
1015	Media Framework control port bind error	The control port for the native Java communication could not be opened. Check the port configuration for other processes using the same ports.
1016	Native Media Framework realtime error	The native Media Framework process could not be started in realtime mode. This may lead to inferior voice quality. Check the access privileges for the native image.
1019	Illegal command option	The native Media Framework was invoked with an invalid command option. Check the configuration in the entity file of the Media Framework.
1020	No more free UDP ports available	No more free UDP ports are available to the Media Framework (MFW). Ensure that the port range of the Media Server is configured sufficiently great.

14.3 Media Gateway Provider

The OpenScape Media Server supports the following error messages for the Media Gateway provider:

Table 5: Error messages of the Media Gateway provider

ID	Message	Description
1000	Failed to initialize Media Gateway provider	An error occurred upon the Media Gateway provider start. Check the Media Gateway configuration and verify that the Prompt DB provider has started.
1001	Failed to activate configuration changes	An error occurred upon activating configuration changes. Correct the Media Gateway configuration and reboot the provider.
1002	Failed to deactivate Media Gateway provider	An unexpected error occurred upon stopping the Media Gateway provider.
1003	Failed to activate Media Gateways	No listening point is defined in the Media Gateway configuration. Configure at least one listening point.
1004	Failed to create connection	The command to set up a connection is ignored since no inbound connection listener is registered. Verify that the Terminal Binder has been started.
1010	Create connection failed	An internal problem has occurred during the connection setup.

ID	Message	Description
1011	Modify connection failed	An internal problem has occurred during a connection change.
1012	Delete connection failed	An internal problem has occurred during deleting a connection.
1013	NotificationRequest failed	An internal problem has occurred during handling a notification request.
1030	Lost the resource associated with the connection	An unexpected error has occured and the gateway closes the connection.

14.4 Media Processing Provider

The OpenScape Media Server supports the following error messages for the Media Processing provider:

Table 6: Error messages of the Media Processing (MPS) provider

ID	**Message**	**Description**
1000	Missing MFW provider	No Media Framework (MFW) provider received from the Application Host.
1001	Missing MPS provider	No Media Processing (MPS) provider received from the Application Host.
1002	Failed to initialize MPS Media Processing provider	The Media Processing (MPS) provider could not be initialized.

14.5 Streaming-IVR Component

The OpenScape Media Server supports the following error messages for the Streaming-IVR component:

Table 7: Error messages of the Streaming-IVR component

ID	Message	Description
1000	Missing MFW provider	No MediaFramework (MFW) provider could be received from the Application Host.
1002	Failed to initialize MPS Media Processing provider	Initializing the Media Processing (MPS) provider failed.
1003	No more RTP channel available	Allocating an RTP channel resource for call handling failed. Please check the configuration for the resource management of this application.

ID	Message	Description
1004	No (more) TTS license available	Allocating a text-to-speech port license failed. Verify that a sufficient number of licenses has been installed and that the service **licensing service** is active.
1005	No (more) ASR license available	Allocating a speech recognition license failed. Verify that a sufficient number of licenses has been installed and that the service **licensing service** is active.

14.6 MRCP Client

The OpenScape Media Server supports the following error messages for the MRCP client.

Table 8: Error messages of the MGCP Client

ID	Message	Description
1000	Unable to setup a connection with MRCP server	No connection could be set up to the MRCP server.

14.7 SIP Provider

The OpenScape Media Server supports the following error messages for the SIP provider.

Table 9: Error messages of the SIP provider

ID	Message	Description
1000	Failed to start sip provider	No SIP stack entity could be created. Check javax.sip.STACK_NAME in the settings file sip-provider.properties.
1001	Failed to start sip provider	No listening point could be created. The address or the port may already be used. Check provider.LISTENING_POINTS in the settings file sip-provider.properties.
1002	Failed to start sip provider	No SIP provider could be created. The reason for this is unknown.
1003	Failed to start sip provider	The SIP manager could not be registered as SIP listener. The reason for this is unknown.
1004	Failed to stop sip provider	The SIP provider entity could not be deleted by the SIP stack. The reason for this is unknown.

ID	Message	Description
1005	Failed to stop sip provider	A listening point could not be deleted by the SIP stack. The reason for this is unknown.
1006	Failed to start sip provider	No configuration available

15 Reference to the OpenScape Media Server

15.1 Dashboard for the OpenScape Media Server System Node

For each OpenScape Media Server system node exist a dashboard that can be accessed via the CMP. This dashboard contains information on the corresponding system node. The information includes for example hardware information, alarm information, installed applications and their software level.

The following functions and information are available in the dashboard of a OpenScape Media Server system node.

- **Node Note**

  By means of **Edit** you can add a individual note for the corresponding system node. In this way you are able to document information like the physical location of the node or the configuration of the corresponding computer system.
- **Alarm Summary**

  Shows a summary of the alarms that are currently existing for the corresponding system node.
- **System Info**

  Shows general information about the hardware of the corresponding system node. E. g.:

  – CPU load
  – Memory allocation
- **Applications**

  Shows which applications are installed on the corresponding system node.
- **Actions**

  By means of **Show** you are able to access the following information and functions of the corresponding system node.

  – **UC Rapidstat**

    You find detailed information about Rapidstat in the manual *OpenScape UCApplication, Configuration and Administration*.
  – **Show service status**

    Opens a dialog in which all components are shown that are installed on the corresponding system node for the available applications.

    For each component is shown if it is started.

    Furthermore you can configure settings for the individual components.

    IMPORTANT:

    Changing the component settings without appro-priate knowledge may lead to wrong operation or no operation at all for the relative application. Therefore, perform modifications only if the producer documentation or the producer's service personnel ask you to do so.

– **Show software packages**

Opens a dialog which shows all software packages that are installed on the corresponding system node with its individual software version.

15.2 Provider Settings in the Common Management Platform

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Providers tab**

The **Providers** tab shows a list of all providers used by the OpenScape Media Server.

The following information is displayed for each provider:

- **Name**

  Displays the name of the relevant provider. When you click on a provider's name you reach a dialog for configuring the provider.
- **Running**

  Displays whether the software components of the relevant provider have been started.
- **Restart Needed**

  Displays whether the relevant provider needs to be restarted. You need to restart a provider when you change a provider setting that would otherwise not take effect.

- **Sanity Status**

  Displays the status that resulted from the last Sanity Check for the relevant provider.

  When you click on a status text, a window opens that displays the results of the latest Sanity Check.
- **Check Time**

  Displays the date when the last Sanity Check was performed for the relevant provider.

Furthermore, the **Providers** tab contains the following buttons:

- **Restart Provider**

  Restarts the provider selected in the provider list.

  You need to restart a provider when you change a provider setting that would otherwise not take effect.

> **IMPORTANT:**
>
> When you reboot the Streaming provider (**Streaming**), SIP provider (**IP telephony**) or MGCP provider (**Media Gateway**), all associated connections that exist at the time of the reboot are interrupted. Before the reboot you can switch to the **Monitoring** tab to see whether connections are currently active.

- **Check Sanity of Providers**

  Starts the Sanity Check for all providers of the provider list.
- **Edit**

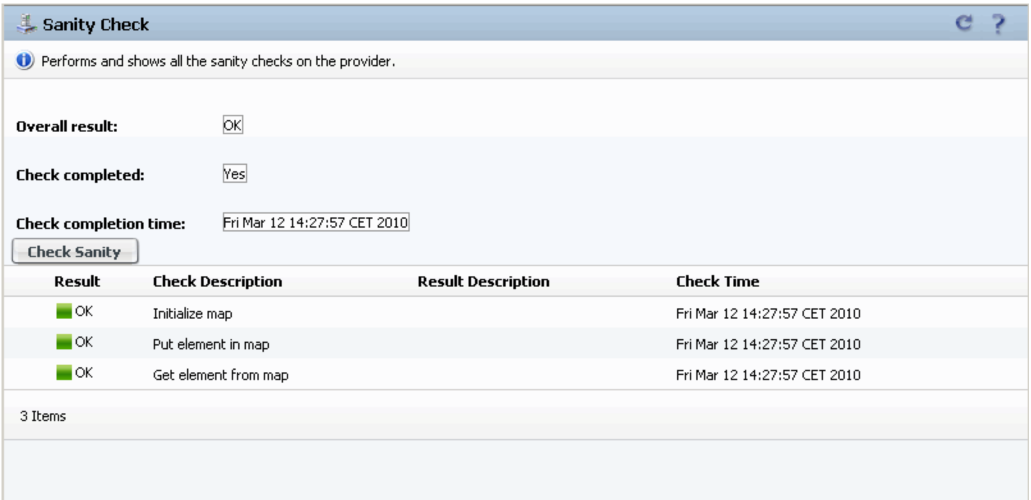
  Opens the configuration dialog for the provider selected in the provider list.

15.2.1 Sanity Check

Invocation in the Common Management Platform:
[Provider] <result of a Sanity Check >

This dialog displays the results of the last Sanity Check and its single checks for a selected provider.

> **NOTICE:**
>
> All Sanity Check information is displayed in English language only.



- **Overall result**

  Displays the overall result of the last Sanity Check for the relevant provider.

Possible values:	– OK – The check does not point to any problems. – Warning – The check points to potential problems. – Error – The check points to definite problems.

- **Check completion time**

  Shows the date and time when the last Sanity Check for the relevant provider was finished.

- **Check completed**

  Shows whether all individual checks for the relevant provider are complete.

Possible values:	– Yes – All individual checks for the provider are finished. – No – At least one individual check for the provider is still pending.

- **Check Sanity**

  Starts a new Sanity Check for the relevant provider.

- **<List of all single checks >**

  Displays all individual checks that were performed for the relevant provider in the scope of the last Sanity Check. For each individual check you can see the result, a test description, a result description and the time when the individual check was performed.

  The result of an individual check may have the same values as are described under **Overall result**.

15.2.2 Media Gateway (MGCP)

Invocation in the CMP:
[Providers] Media Gateway (MGCP)

NOTICE:

You need to consider the Media Gateway settings only if you use the OpenScape Media Server at OpenScape Voice.

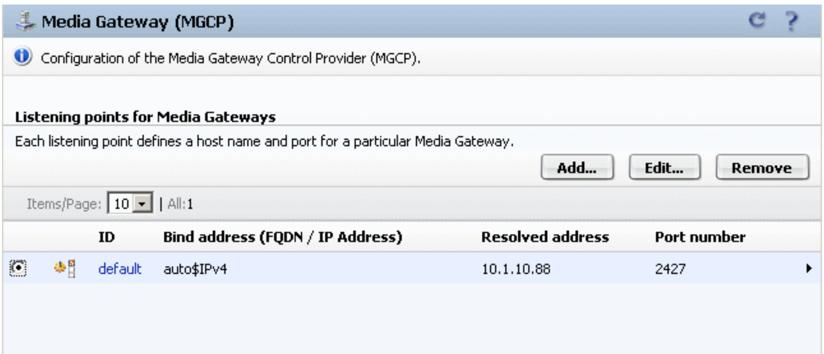
In this dialog you perform the MGCP settings the MGCP provider of the OpenScape Media Server uses for the MGCP communication with OpenScape Voice.

You configure so-called MGCP listening points for the MGCP communication. Such an MGCP listening point consists of an assignment of:

- Hostname / IPv4 address / IPv6 address
- Port number

NOTICE:

Earlier versions of the OpenScape Media Server allowed configuring maximum numbers of simultaneous announcements, conference participants and monitoring end points for the MGCP provider. You can perform such settings now via the address expression of different address bindings.



- **<List of all MGCP listening points >**

  Displays all MGCP listening points configured in the OpenScape Media Server for the MGCP communication.

  To select the relevant MGCP listening point, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected MGCP listening point or remove the selected MGCP listening point.
- **Edit**

  Opens a dialog in which you can edit the settings of the selected MGCP listening point.
- **Remove**

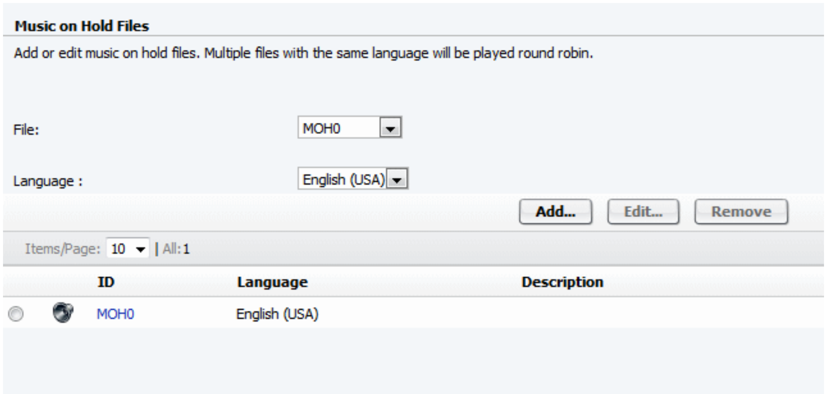
  Removes the selected MGCP listening point from the OpenScape Media Server configuration.
- **Add**

  Opens a configuration dialog in which you can create a new MGCP listening point.

Furthermore, you can manage the music-on-hold files of OpenScape Voice in this dialog. Such music-on-hold files comprise:

- The music-on-hold files that OpenScape Voice uses after the system installation by default.
- Additional music-on-hold files that can be activated in OpenScape Voice when needed.

  Though OpenScape Voice does not use those additional music-on-hold files by default, wildcard files are already available for them in the OpenScape Media Server. Preconfigured intercepts and treatments are assigned to them in OpenScape Voice. This enables you to activate additional music-on-hold for OpenScape Voice, which can then be used for example in a customer-individual contact center application.



- **File**

  Specifies the name of the music-on-hold file for which you can load individual music-on-hold on the OpenScape Media Server.

  The files named **MOH x** correspond to the default music-on-hold files of OpenScape Voice and the files named **HPPC_Ann x** correspond to the music-on-hold you can activate additionally.
- **Language**

  Specifies the language for which you can load an individual music-on-hold file on the OpenScape Media Server.

  If several files of the same language have been loaded on the OpenScape Media Server for a music-on-hold, the OpenScape Media Server plays such files using the round-robin procedure.
- **<List of all music-on-hold files >**

  Displays all individual music-on-hold files loaded on the OpenScape Media Server for the music-on-hold file name under **File**.

  To play music-on-hold click on its name in the list column **ID**.

  To select the relevant individual music-on-hold file, enable the radio button that precedes the associated list entry. Subsequently, you can remove the music-on-hold file or edit its settings.

  > **NOTICE:**
  >
  > You can only select one list entry at a time.
- **Edit**

  Opens a dialog in which you can edit the settings for the selected individual music-on-hold.

- **Remove**

  Deletes the selected individual music-on-hold file from the OpenScape Media Server. It will then be replaced with the music-on-hold file originally installed with the OpenScape Media Server.

  > **NOTICE:**
  >
  > The **Remove** button is inactive if the selected music-on-hold file is the original file installed with the OpenScape Media Server.

- **Add**

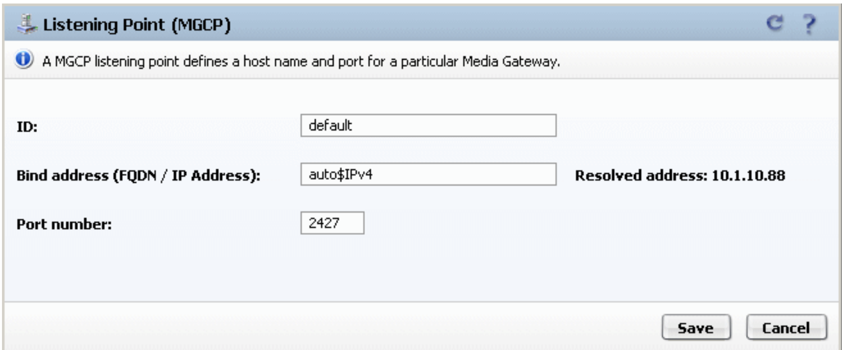
  Opens a configuration dialog in which you can load an individual music-on-hold file on the OpenScape Media Server. It replaces the associated music-on-hold file installed with the OpenScape Media Server originally.

15.2.2.1 Listening Point (MGCP)

Invocation in the CMP:
[Providers] Media Gateway (MGCP)> Add / Edit (listening points)

> **NOTICE:**
>
> You need to consider the settings for MGCP listening points only if you use the OpenScape Media Server at OpenScape Voice.

In this dialog you perform the settings of a listening point used for inbound MGCP connections.



- **ID**

  Defines the unique name of the listening point. Under this name the listening point is administered in the CMP.

Default:	–
Possible values:	<unique name >

- **Bind Address**

  Defines the IP address (IPv4, IPv6) that the OpenScape Media Server uses on the local computer system for the relevant listening point. If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

  If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

Default:	<is automatically determined >
Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name> – auto$IPv4 – auto$IPv6
Remark:	Please heed the following when using the OpenScape Media Server at OpenScape Voice: When you configure the IP address freshly or change it, you must implement the following packet filter rules (firewall rules) in OpenScape Voice via the startCli interface. Only in this way, the full OpenScape Media Server functionality is activated. – If the OpenScape Media Server is installed on the computer system of OpenScape Voice, **RTP Voice** must be released. – If the OpenScape Media Server is not installed on the computer system of OpenScape Voice, **MGCP Signaling** must be released. – In case of an OpenScape Voice cluster installation, **RTP Voice** as well as **MGCP Signaling** must be released.

- **Port number**

  Specifies the port that the OpenScape Media Server for the relevant listening point.

Default:	2427
Possible values:	<port number>
Remark:	If a firewall exists between the OpenScape Media Server and OpenScape Voice, you need to activate the port configured here in this firewall.

15.2.2.2 Music-on-Hold File

File as Music-on-Hold

Internet radio station as the music-on-hold provider

Invocation in the CMP:
[Providers] Media Gateway (MGCP)> Add / Edit (music-on-hold files)

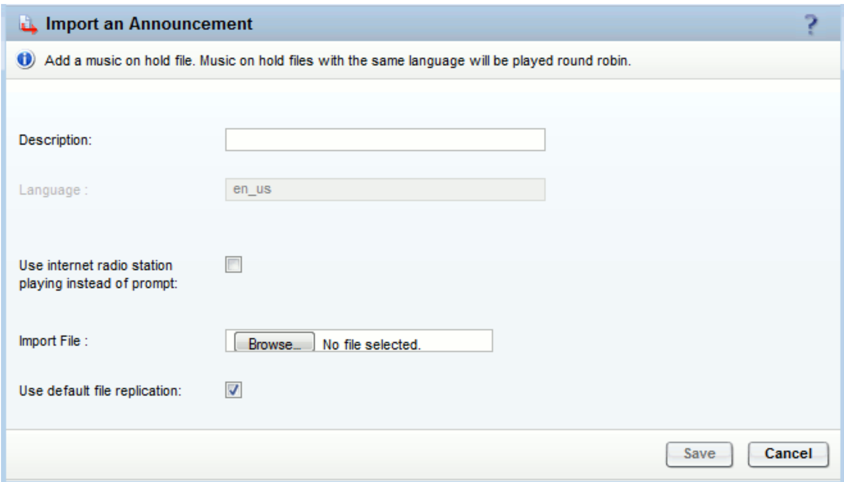
NOTICE:

You need to consider the settings for music-on-hold files only if you use the OpenScape Media Server at OpenScape Voice.

In this dialog you manage the music-on-hold of OpenScape Voice for one language.

If several files of the same language have been loaded on the OpenScape Media Server for an OpenScape Voice music-on-hold, the OpenScape Media Server plays such files using the round-robin procedure.

The dialog for the music-on-hold file differs subject to whether you wish to use an actual prompt file or an Internet radio station.



- **Description**

  Provides a short description of the music-on-hold file.
- **Language**

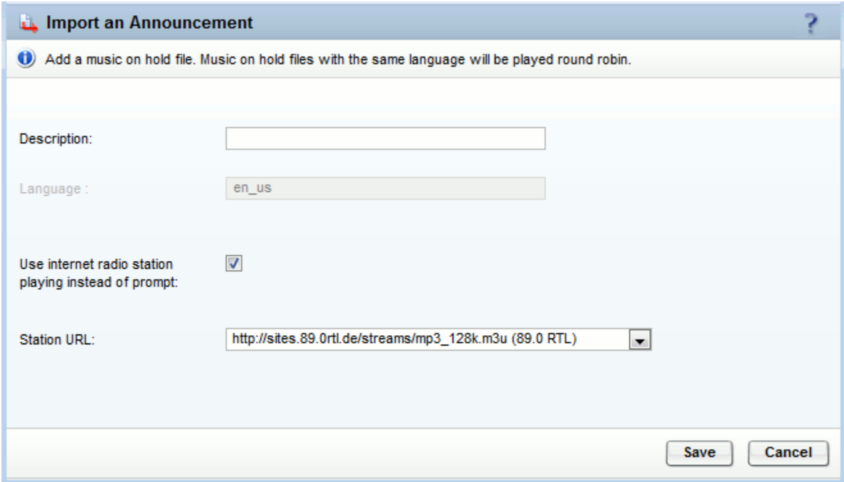
  Indicates the language for which you can load an individual music-on-hold file on the OpenScape Media Server.
- **Use internet radio station playing instead of prompt**

  If you wish to use a file as music-on-hold, this option must be disabled.
- **Import File**

  Specifies the file to be loaded on the OpenScape Media Server as individual music-on-hold file. It replaces the associated music-on-hold file installed with the OpenScape Media Server originally.

- **Use default file replication.**

  Determines whether the individual music-on-hold file shall be automatically replicated to all other OpenScape Media Servers of a Media Server farm.



- **Description**

  Provides a short description of the music-on-hold.
- **Language**

  Indicates the language for which you configure an Internet radio station.
- **Use internet radio station playing instead of prompt**

  If you wish to use an Internet radio station for your music-on-hold, this option must be active.
- **Station URL**

  Specifies the Internet radio station the program of which shall be used as music-on-hold.

  In this field you can select only URLs of those Internet radio stations that were configured in the **Internet Radio Streaming** Provider.

15.2.3 IP Telephony (SIP)

Invocation in the Common Management Platform:
[Provider] IP Telephony (SIP)

NOTICE:

You need to consider the IP telephony settings only if you use the OpenScape Media Server under OpenScape UCApplication.

In this dialog you define the communication settings the SIP provider of the OpenScape Media Server uses for incoming and outgoing calls with SIP servers – e. g. with OpenScape Voice.

- SIP listening point

  Each SIP listening point consists of a combination of:

  – SIP listening point ID
  – Hostname / IPv4 address / IPv6 address of the OpenScape Media Server
  – Port number on which the OpenScape Media Server expects inbound SIP communication
  – Transport protocol the OpenScape Media Server uses for SIP communication
- SIP server line

  Each SIP server line consists of a combination of:

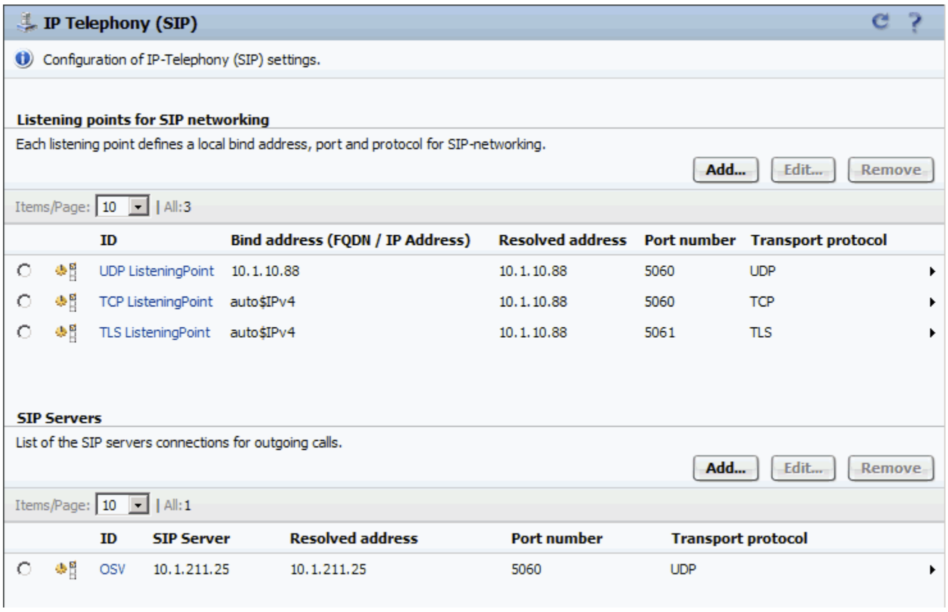
  – SIP server line ID
  – Hostname / IPv4 address / IPv6 address of the primary SIP server
  – Port number configured on the primary SIP server for inbound SIP communication
  – Address translation context for normalizing addresses transmitted within SIP signaling.
  – ID of the SIP listening point via which local IP address and transport protocol the OpenScape Media Server is to communicate.
  – Connection information for alternative SIP servers.

IMPORTANT:

The OpenScape Media Server always requires an SIP trunk for communicating with a communications system. If no SIP trunk is used, communication between OpenScape Media Server and the communications system fails.

NOTICE:

OpenScape Voice endpoints do not use TLS by default. To use TLS, you need to set the **MTLS** transport protocol for the relevant endpoints via the OpenScape Voice Assistant or via the startCli console of OpenScape Voice.



- **<List of all SIP listening points >**

  Displays all SIP listening points configured in the OpenScape Media Server.

  To select the relevant SIP listening point, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected SIP listening point or remove it.
- **Edit**

  Opens a dialog in which you can edit the settings of the selected SIP listening point.
- **Remove**

  Removes the selected SIP listening point from the OpenScape Media Server configuration.
- **Add**

  Opens a configuration dialog in which you can create a new SIP listening point.
- **<List of all SIP servers >**

  Displays all SIP server lines configured in the OpenScape Media Server.

  To select the relevant SIP server line, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected SIP server line or remove the selected SIP server line.
- **Edit**

  Opens a dialog in which you can edit the settings of the selected SIP server line.
- **Remove**

  Removes the selected SIP server line from the OpenScape Media Server configuration.
- **Add**

  Opens a configuration dialog in which you can create a new SIP server line.

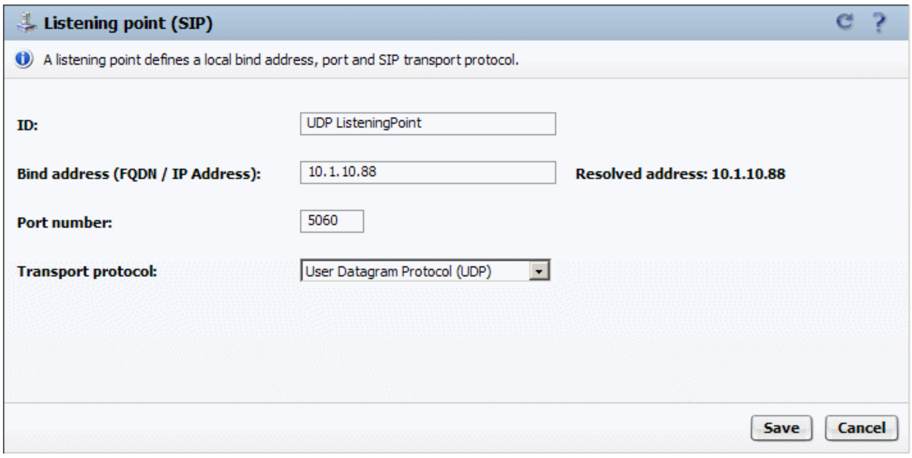
15.2.3.1 Listening Point (SIP)

Invocation in the Common Management Platform:
[Providers] IP Telephony (SIP) > Add / Edit (Listening Points)

NOTICE:

You need to consider the SIP listening point settings only if you use the OpenScape Media Server under OpenScape UCApplication.

In this dialog you specify the settings of a listening point.



- **ID**

  Defines the unique name of the listening point. Under this name the listening point is administered in the CMP.

Default:	–
Possible values:	<unique name >

- **Bind address**

  Defines the IP address (IPv4, IPv6) that the OpenScape Media Server uses on the local computer system for the relevant listening point. If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

  If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

Default:	<is automatically determined >

Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name> – auto$IPv4 – auto$IPv6

- **Port number**

  Specifies the port that the OpenScape Media Server for the relevant listening point.

Default:	5060
Possible values:	<port number>
Remark:	If a firewall exists between the OpenScape Media Server and the communications system, you need to activate the port configured here in this firewall.

- **Transport protocol**

  Specifies the transport protocol that the OpenScape Media Server uses for the relevant listening point.

Default:	TCP
Possible values:	– UDP – TCP – TLS

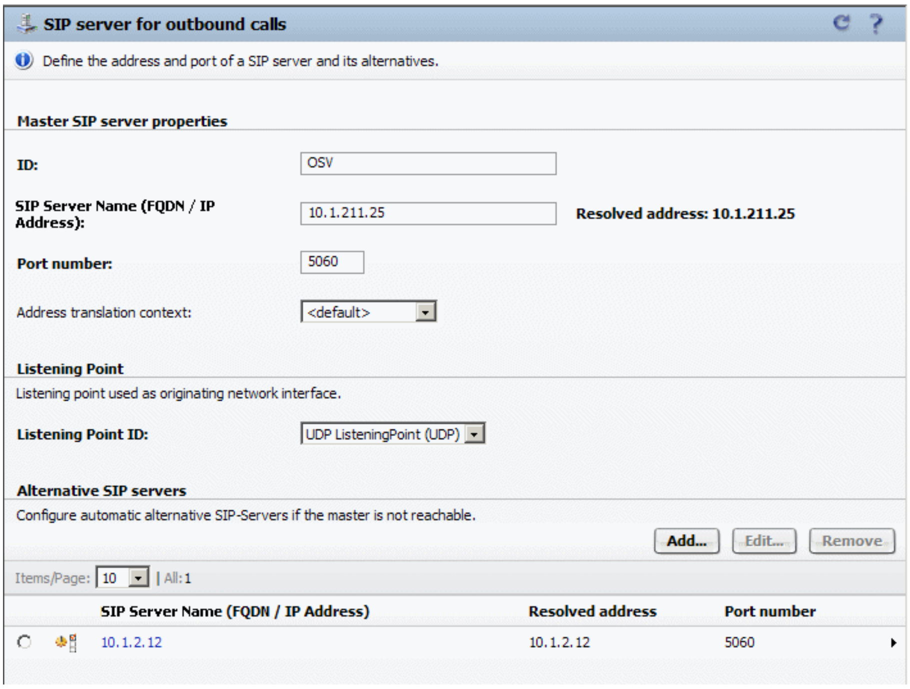
15.2.3.2 SIP Server Line

Invocation in the Common Management Platform:
[Provider] IP Telephony (SIP)> Add / Edit (SIP Servers)

NOTICE:

You need to consider the SIP server line settings only if you use the OpenScape Media Server under OpenScape UCApplication.

In this dialog you define the communication settings the SIP provider of the OpenScape Media Server uses for outbound connections with SIP servers and for phone number normalization / localization.



- **ID**

  Defines the unique name of the SIP server line. Under this name the SIP server line is administered in the CMP.

Default:	–
Possible values:	<unique name >

- **SIP Server Name (FQDN / IP Address)**

  Defines the IP address (IPv4, IPv6) of the master SIP server that the OpenScape Media Server prefers for the relevant SIP server line.

  – If you wish to use OpenScape Voice as master SIP server, this is normally the IP address of the SIP service manager (SIP SM) of OpenScape Voice.

  – If you wish to use OpenScape 4000 as master SIP server, this is the IP address of the HG module used.

  If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

Default:	–
Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name>

- **Port number**

  Defines the port configured on the master SIP server for inbound SIP communication

  Port **5060** should be set by default for the transport protocols UDP and TCP under **Port number**, and port **5061** for TLS. The listening point specified under **Listening Point ID** determines which transport protocol is used.

Default:	–
Possible values:	<port number>
Remark:	If a firewall exists between the OpenScape Media Server and OpenScape Voice, you need to activate the port configured here in this firewall.

- **Address translation context**

  Defines the ID of an address translation context configured in the CMP. The SIP provider uses this context to normalize and localize phone numbers for the relevant SIP server line.

- **Listening point ID**

  Defines the SIP listening point the communication settings of which the OpenScape Media Server uses when it deploys the relevant SIP server line for an outgoing call.

Default:	–
Possible values:	<ID of a configured SIP listening point >

- **<List of all alternative SIP servers >**

  Displays all SIP server connections that are configured as alternative connections for the relevant SIP server line.

  To select the relevant alternative SIP server connection, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected alternative SIP server connection or remove the selected alternative SIP server connection. See **Edit** and **Remove**.

- **Edit**

  Opens a dialog in which you can edit the settings of the selected alternative SIP server connection.

- **Remove**

  Removes the selected alternative SIP server connection from the OpenScape Media Server configuration.

- **Add**

  Opens a configuration dialog in which you can create a new alternative SIP server connection.

15.2.3.3 Alternative SIP Server Connection

Invocation in the Common Management Platform:
[Provider] IP Telephony (SIP)> Add / Edit (SIP Servers)> Add/ Edit(AlternativeSIP servers)

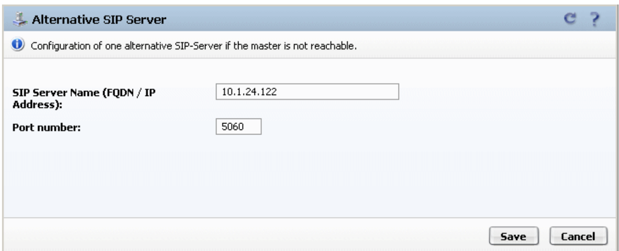
NOTICE:

You need to consider the settings for alternative SIP server connections only if you use the OpenScape Media Server under OpenScape UCApplication.

NOTICE:

You must not configure any alternative SIP servers for the SIP connection to a co-located OpenScape Voice system.
For a geo-separated system, you may configure only a single alternative SIP server. In this case, the master connection to the SIP service manager (SIPSM) must lead from node 1 and the alternative connection to the SIP service manager (SIPSM) from node 2.

In this dialog, you define the settings of an alternative SIP server connection.



- **SIP Server Name (FQDN / IP Address)**

  Defines the IP address (IPv4, IPv6) of the alternative SIP server that the OpenScape Media Server uses for outgoing calls if required.

  – If you wish to use OpenScape Voice as SIP server, this is normally the IP address of the SIP service manager (SIP SM) of OpenScape Voice.
  – If you wish to use OpenScape 4000 as SIP server, this is the IP address of the HG module used.

  If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

Default:	–
Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name>

- **Port number**

  Defines the port to which the OpenScape Media Server sends the data for outbound connections when it uses the relevant alternative SIP server.

  Port **5060** should be set by default for the transport protocols UDP and TCP, and port **5061** for TLS.

  The listening point specified in the settings of the SIP server line under **Listening-Point-ID** determines which transport protocol is used.

Default:	–
Possible values:	<port number>
Remark:	If a firewall exists between the OpenScape Media Server and OpenScape Voice, you need to activate the port configured here in this firewall.

15.2.4 Streaming (RTP)

Invocation in the Common Management Platform:
[Providers] Streaming (RTP)

In this dialog you specify the RTP settings that the Streaming provider of the OpenScape Media Server uses for the RTP communication with RTP terminal devices.

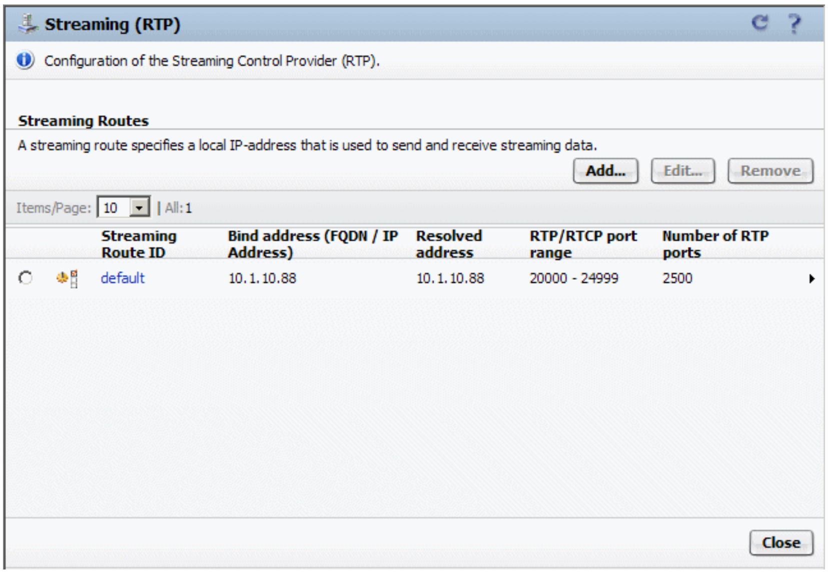
IMPORTANT:

If you change important Streaming provider settings, you must as a rule reboot the provider for the modifications to take effect. All RTP connections that exist until the time of the reboot will be interrupted in this process.

Whether or not a provider reboot is necessary is displayed in the node management of the OpenScape Media Server.

IMPORTANT:

If there is a firewall between the OpenScape Media Server and the RTP terminal devices, you need to activate the RTP ports in this firewall that are configured in the OpenScape Media Server for the streaming.



- **<List of all streaming routes >**

  Displays all RTP streaming routes configured in the OpenScape Media Server.

  To select the relevant streaming route, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected streaming route or remove the selected streaming route. See **Edit** and **Remove**.
- **Edit**

  Opens a dialog in which you can edit the settings of the selected streaming route.
- **Remove**

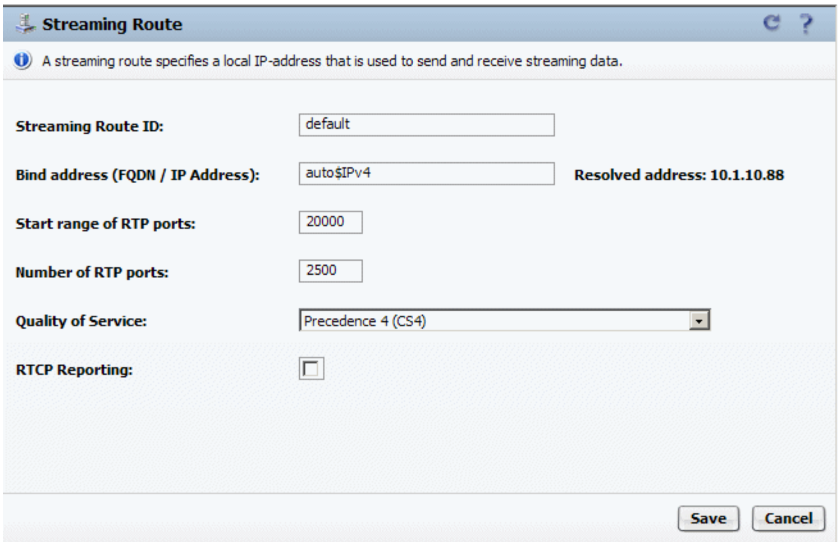
  Removes the selected streaming route from the OpenScape Media Server configuration.
- **Add**

  Opens a configuration dialog in which you can create a new streaming route.

15.2.4.1 Streaming Route

Invocation in the Common Management Platform:
[Providers] Streaming (RTP)> Add / Edit

In this dialog you define the settings of an RTP streaming route via which the OpenScape Media Server routes RTP data to RTP devices.



- **Streaming Route ID**

  Defines the unique name streaming route.
- **Bind address**

  Defines the IP address (IPv4, IPv6) that the OpenScape Media Server uses on the local computer system for the RTP communication via the relevant RTP streaming route.

  If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

  If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

Default:	<is automatically determined >
Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name> – auto$IPv4 – auto$IPv6

Remark:	If you use the OpenScape Media Server at OpenScape Voice, please note the following: When you newly set up the IP address or modify it, you need to implement the following Packet Filter Rules (Firewall Rules) in OpenScape Voice via the startCli interface. Only in this way the full OpenScape Media Server functionality is activated. – If the OpenScape Media Server is installed on the computer system of OpenScape Voice, **RTP Voice** must be released. – If the OpenScape Media Server is not installed on the computer system of OpenScape Voice, **MGCP Signaling** must be released. – In case of an OpenScape Voice cluster installation, **RTP Voice** as well as **MGCP Signaling** must be activated. If the OpenScape Media Server is not installed on the computer system of OpenScape Voice, you need to release the configured reference address also in the IP Tables of the Media Server computer system.

- **Start range of RTP ports**

  Defines the first UDP port of the port range that the OpenScape Media Server uses for the RTP-based communication via the relevant RTP streaming route.

  RTP communication requires two UDP ports: one for transmitting the actual media stream via RTP, and one for RTCP that monitors the connection quality.

  An even port number is used as port for RTP, and the next higher odd port number as port for the associated RTCP communication.

  Therefore, you need to specify an even number as the starting point for the port range.

Default:	20000
Permissible values:	<even-numbered port number>
Remark:	The port ranges of different streaming route must not overlap. If a firewall exists between the OpenScape Media Server and the RTP terminal devices, you need to activate the port configured here in this firewall.

- **Number of RTP ports**

  Defines the maximum number of UDP ports that the OpenScape Media Server uses for the RTP-based communication via the relevant RTP streaming route.

  Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the number of UDP ports set here is once again allocated for the RTCP communication– even if the **RTCP Reporting** option for the RTP streaming routes is disabled.

Default:	2 500
Possible values:	The maximum permissible amount of RTP ports of all RTP streaming routes is generally restricted by: – the settings **maxNumRtpPorts** in the configuration file of the Streaming provider. – the hardware you use for the OpenScape Media Server.
Remark:	If an individual traffic measurement reveals that not all RTP streaming routes use their maximum number of RTP ports at the same time, you may also individually “overbook” the **Number of RTP ports** setting. In this case you should regularly verify that the configured overbooking matches the RTP traffic behavior. The port ranges of different streaming route must not overlap. If a firewall exists between the OpenScape Media Server and the RTP terminal devices, you need to activate the ports configured here in this firewall.
Example:	**Number of RTP ports** = 75 A total number of 150 UDP ports is allocated – e. g. the UDP ports 20 000 to 20 149. Half of them are for RTP communication and the other half for RTCP communication.

- **Quality of Service**

  Defines the quality of service (DSCP) used for the RTP communication between OpenScape Media Server and RTP-based devices via the relevant RTP streaming route.

  The standardized and experimental service qualities can be selected.

Default:	Standard

Possible values:	– Assured Forwarding Class 1, Low Drop Precedence (AF11) – Assured Forwarding Class 1, Medium Drop Precedence (AF12) – Assured Forwarding Class 1, High Drop Precedence (AF13) – Assured Forwarding Class 2, Low Drop Precedence (AF21) – Assured Forwarding Class 2, Medium Drop Precedence (AF22) – Assured Forwarding Class 2, High Drop Precedence (AF23) – Assured Forwarding Class 3, Low Drop Precedence (AF31) – Assured Forwarding Class 3, Medium Drop Precedence (AF32) – Assured Forwarding Class 3, High Drop Precedence (AF33) – Assured Forwarding Class 4, Low Drop Precedence (AF41) – Assured Forwarding Class 4, Medium Drop Precedence (AF42) – Assured Forwarding Class 4, High Drop Precedence (AF43) – Expedited Forwarding (EF) – Precedence 1 (CS1) – Precedence 2 (CS2) – Precedence 3 (CS3) – Precedence 4 (CS4) – Precedence 5 (CS5) – Precedence 6 (CS6) – Precedence 7 (CS7) – Standard (CS0) – <further experimental DSCP code points in binary format>
Remark:	If the OpenScape Media Server is used at OpenScape Voice, usually the DSCP of OpenScape Voice to be used is transferred to the MGCP service of the OpenScape Media Server. The setting performed in this field is only used if OpenScape Voice transfers no DSCP information to the OpenScape Media Server or the transfer fails.

- **RTCP reports**

  Defines whether RTCP is used for RTP connections.

15.2.5 Streaming-IVR (TTS, ASR, SDP)

Invocation in the Common Management Platform:
[Provider] Streaming-IVR (TTS, ASR, SDP)

In this dialog you manage the MRCP and SDP settings that the Streaming-IVR provider of the OpenScape Media Server uses.

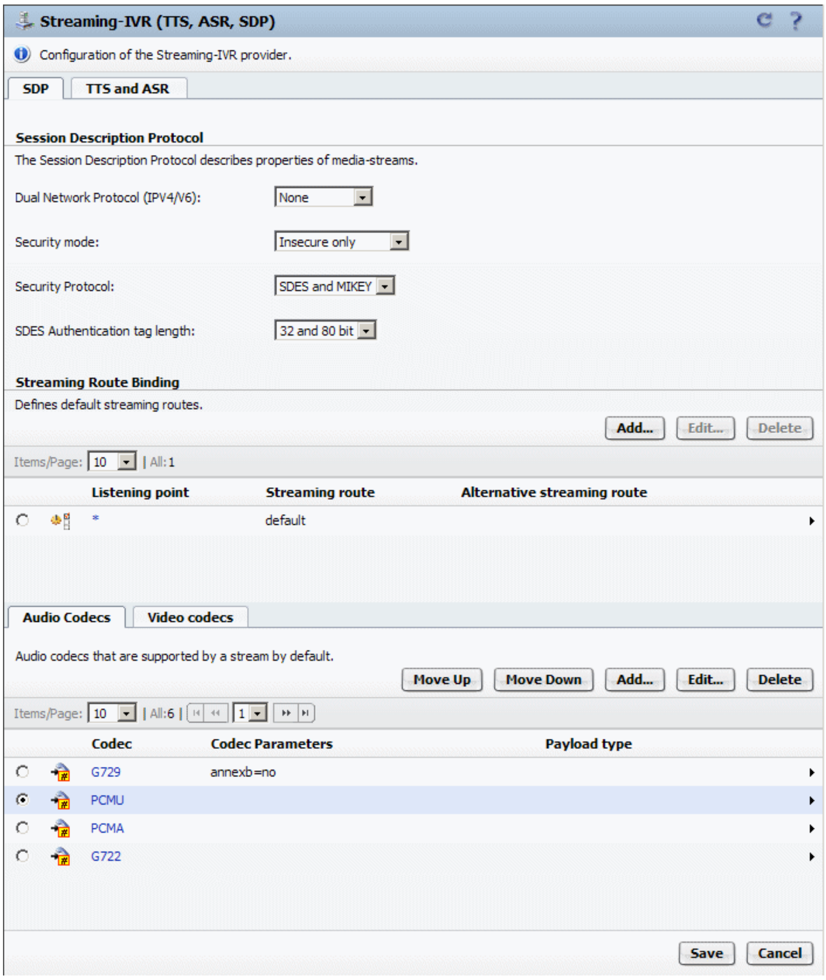
The settings in this dialog are grouped as follows:

- SDP-related settings
- TTS and ASR settings

15.2.5.1 SDP

Invocation in the Common Management Platform:
[Providers] Streaming-IVR (TTS, ASR, SDP) > **[tab] SDP**

On this tab you define the settings that the Streaming-IVR provider of the OpenScape Media Server can use for communications connections. When the connection is set up, the Streaming-IVR provider negotiates with the communication partner which of the possible settings to actually use for an individual communications connection. The Session Description Protocol (SDP) is used for this negotiation.



Session Description Protocol

In this section you define general settings that the Streaming-IVR provider of the OpenScape Media Server can use for communications connections.

- **Dual Network Protocol (IP V4 / V6)**

  You can connect the OpenScape Media Server to the network via IPv4 and IPv6 addresses simultaneously.

  In this case **Dual Network Protocol (IP V4 / V6)** defines which protocol the OpenScape Media Server uses to inform communications partners about the alternatively available IP addresses.

Default:	None
Possible values:	– None – ICE – ICE lite – ANAT

- **Security mode**

  Specifies system-wide, which type of security the OpenScape Media Server uses (preferably) for communication.

  IMPORTANT:

  Using SRTP with MIKEY requires the system time of all systems involved in the SRTP communication to be synchronized – OpenScape Media Server, RTP-based devices (e. g. phone), VoIP gateway etc. The Network Time Protocol (NTP) may be used for this purpose.

  NOTICE: If you define a **security mode** specific to a terminal, this setting is used preferably.

  The possible settings have the following meaning.

  – **Secure only**

    A connection is only set up if the communications system and the RTP terminal device can use encrypted RTP communication (SRTP with MIKEY or SDES).

    IMPORTANT:

    The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

  – **Insecure only**

    A connection is only set up if the communications system and the RTP terminal device can use an unencrypted RTP communication.

    In case encrypted and unencrypted RTP communication is offered, unencrypted RTP communication is selected. A connection is not set up only if the terminal device offers exclusively encrypted RTP communication.

– **Secure preferred**

If the communications system and the RTP terminal device can use encrypted RTP communication (SRTP with MIKEY or SDES), the OpenScape Media Server uses this type of communication.

If the communications system and the RTP terminal can only use an unencrypted RTP communication, the RTP connection is set up unencrypted.

IMPORTANT:

The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

– **Default (<current default value>)**

Activates for the terminal the setting for **Security mode** valid across the system as it is configured in the Streaming-IVR provider.

Default:	Secure preferred
Possible values:	– Secure only – Insecure only – Secure preferred

• **Security protocol**

Specifies the protocol via which the OpenScape Media Server can negotiate SRTP keys with terminals.

Default:	SDES and MIKEY
Possible values:	– MIKEY – SDES – SDES and MIKEY
Remark:	So that the selected security protocol is used, **Secure only** or **Secure preferred** must be selected under the **Security mode** of the relevant terminals.

- **SDES Authentication tag length**

  Defines the length of the authentication tag that the OpenScape Media Server uses for the cryptographic procedure HMAC-SHA1 used.

  The possible values have the following meaning:

  – 32-bit only

    The OpenScape Media Server itself offers only 32-bit authentication tags but can also use 80-bit authentication tags upon request.

  – 80-bit only

    The OpenScape Media Server itself offers only 80-bit authentication tags and can only use 80-bit authentication tags upon request.

  – 32- and 80-bit

    The OpenScape Media Server itself offers both authentication tag lengths and can use both lengths upon request.

Default:	32 and 80 bit
Possible values:	– 32-bit only – 80 bit only – 32- and 80-bit
Remark:	This setting is effective only if the security protocol SDES is used.

Streaming Route Bindings

In this section you define streaming route bindings valid across the system. A streaming route binding specifies which streaming route the OpenScape Media Server uses to transmit RTP data when the associated connection signaling is handled via a specific listening point.

> **NOTICE:** When you define individual streaming route bindings in a terminal, such settings specific to the terminal are used preferably.

- **<List of streaming route bindings >**

  Displays all streaming route bindings valid across the system and configured for the OpenScape Media Server.

  To select the relevant streaming route binding, enable the radio button that precedes the associated list entry. You can then edit the configuration of the selected streaming route binding or remove the selected binding.

- **Edit (under Streaming Route Binding)**

  Opens a dialog in which you can edit the settings of the selected streaming route bindings valid across the system.

- **Delete (under Streaming Route Binding)**

  Removes the selected streaming route binding valid across the system from the OpenScape Media Server configuration.

- **Add (under Streaming Route Binding)**

  Opens a configuration dialog in which you can create new streaming route bindings valid across the system.

Audio and Video Codecs

In this section you define which audio and video codecs the Streaming-IVR provider of the OpenScape Media Server can use for communications connections system-wide.

> **NOTICE:** If you specify individual codec settings in the data stream of a terminal, such terminal-specific settings are used preferably.

- **<List of audio or video codecs >**

  You see two tabs showing the audio or video codecs that can be used for transmitting RTP data. The codec display sequence determines the priority with which a codec is used. The codec with the highest priority appears as first entry in the respective codec list; the one with the lowest priority is the bottom entry in the list.

  To select the relevant codec, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected codec or remove the selected codec from the relevant codec list.

  The OpenScape Media Server can use the following codecs:

Media Type	Codec	Performance Factor [57]	Voice Quality	Use
Audio	G.711A	1	ISDN quality	Default PCM transmission with A-Law for volume compression. Mainly used in Europe.
	G.711µ	1	ISDN quality	Default PCM transmission with µ-Law for volume compression. Mainly used in North America and Japan.
	G.722	2	good	ISDN broadband codec with better voice quality than G.711
	G.729	3	reduced	Compressed voice transmission with speech pause suppression.
	G722.1 (Polycom Siren 7)[58]	-	high (mono)	All media-applications for a better user experience especially during Video-Conference Calls

57 The higher the performance factor, the more computing power the OpenScape Media Server needs to expend for the codec.

58 Royalty free offered by Polycom

Media Type	Codec	Performance Factor [57]	Voice Quality	Use
	G722.1 Appendix C (Polycom Siren 14)[59]	-	high (wideband)	All media-applications for a better user experience especially during Video-Conference Calls
	Telephone-event	low	–	Recognition of outband DTMF (RFC 2833)
Video	H.264	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4 / AVC.
Video	H.265	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4/AVC.

IMPORTANT:

If you do not configure the audio codec **Telephone-event** for a terminal, DTMF signals must be transmitted inband if the OpenScape Media Server is to recognize such DTMF signals. This inband-based recognition requires additional system capacity.

NOTICE:

Using a codec that requires increased computing power reduces the number of channels the OpenScape Media Server supports in parallel.

- **Move Up**

  Moves the selected codec up by one position in the codec list. This increases the priority with which the relevant codec is used.
- **Move Down**

  Moves the selected codec down by one position in the codec list. This decreases the priority with which the relevant codec is used.
- **Edit**

  Opens a dialog in which you can edit the settings of the selected codec type.
- **Remove**

  Removes the selected codec from the relevant codec list.

57 The higher the performance factor, the more computing power the OpenScape Media Server needs to expend for the codec.

59 Royalty free offered by Polycom

- **Add**

  Opens a configuration dialog in which you can add another codec to the relevant codec list.

15.2.5.2 TTS and ASR

Invocation in the Common Management Platform:
[Provider] Streaming-IVR (TTS, ASR, SDP) > **[tab] TTS and ASR**

On this tab you define the MRCP settings that the Streaming-IVR provider of the OpenScape Media Server uses for the MRCP communication with an external text-to-speech (TTS) or automatic speech recognition software (ASR).

NOTICE:

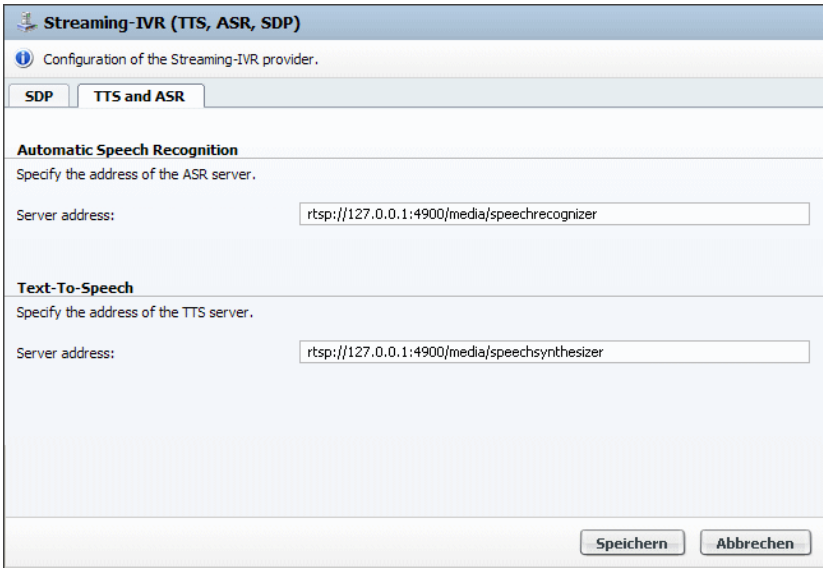
You need to consider the TTS and ASR settings only if you use the OpenScape Media Server under OpenScape UCApplication.

NOTICE:

The OpenScape Media Server has only been released with the ASR/TTS engine by Nuance. It must always be present on the OpenScape Media Server computer system.

NOTICE:

Using the OpenScape UCApplication TTS / ASR engine always requires at least one IPv4-based RTP streaming route to be configured in the OpenScape Media Server.



- **Server address (AutomaticSpeech Recognition)**

  Defines the URI under which the server can be reached for automatic speech recognition (ASR). If no URI is specified, the ASR connection is deactivated.

Default:	rtsp://<IP address Media Server >:4900/media/speechrecognizer
Possible values:	– <URI> – <Empty>

- **Server address (Text-To-Speech)**

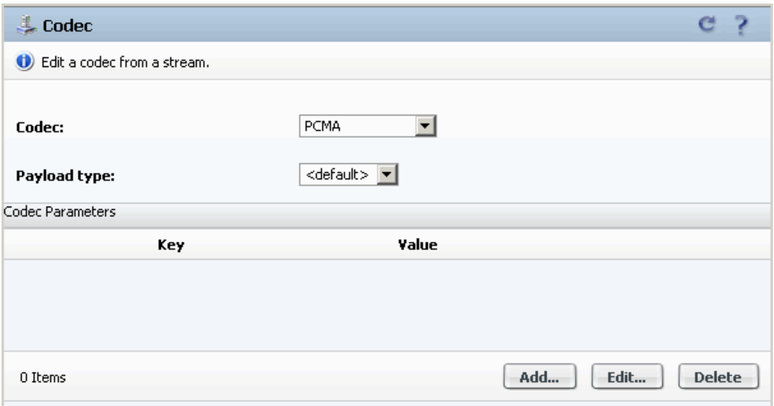
  Defines the URI under which the server can be reached for text-to-speech (TTS). If no URI is specified, the TTS connection is deactivated.

Default:	rtsp://127.0.0.1:4900/media/speechsynthesizer
Possible values:	– <URI> – <Empty>

15.2.5.3 Editing a Codec

Invocation in the Common Management Platform:
• **[Terminals] Add / Edit** > **Add / Edit (Streams)** > **Add / Edit (Codecs)** • **[Providers] Streaming-IVR (TTS, ASR, SDP)** > **[Tab] SDP** > **Add / Edit (Codecs)**

In this dialog you specify the settings of a codec.



- **Codec**

  Defines the codec name.

  The OpenScape Media Server can use the following codecs:

Media Type	Codec	Performance Factor [60]	Voice Quality	Use
Audio	G.711A	1	ISDN quality	Default PCM transmission with A-Law for volume compression. Mainly used in Europe.
	G.711µ	1	ISDN quality	Default PCM transmission with µ-Law for volume compression. Mainly used in North America and Japan.
	G.722	2	good	ISDN broadband codec with better voice quality than G.711
	G.729	3	reduced	Compressed voice transmission with speech pause suppression.
	G722.1 (Polycom Siren 7)[61]	-	high (mono)	All media-applications for a better user experience especially during Video-Conference Calls
	G722.1 Appendix C (Polycom Siren 14)[62]	-	high (wideband)	All media-applications for a better user experience especially during Video-Conference Calls
	Telephone-event	low	–	Recognition of outband DTMF (RFC 2833)
Video	H.264	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4 / AVC.
Video	H.265	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4/AVC.

- **Payload type**

  Defines the payload type that is transferred in the RTP header if the RTP data are coded with the relevant codec. As a rule, setting **<default>** is here the right choice.

60 The higher the performance factor, the more computing power the OpenScape Media Server needs to expend for the codec.

61 Royalty free offered by Polycom

62 Royalty free offered by Polycom

- **<List of codec parameters >**

  Shows all parameters that are assigned to the codec.

  To select the relevant parameter, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected parameter or remove the parameter.

  > **NOTICE:**
  >
  > For the time being, the codecs of the OpenScape Media Server support only codec parameters pre-configured by default.

- **Edit**

  Opens a dialog in which you can edit the properties of the selected codec parameter.
- **Remove**

  Removes the selected codec parameter from the OpenScape Media Server configuration.
- **Add (under Generic Properties)**

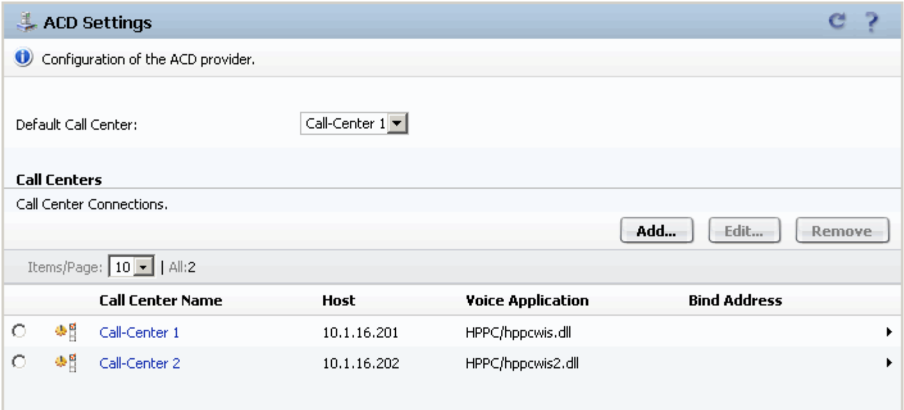
  Opens a configuration dialog in which you can define a new codec parameter.

15.2.6 ACD Provider

Invocation in the Common Management Platform:
[Provider] Automatic Call Distribution (ACD)

> **NOTICE:**
>
> The OpenScape Media Server does not yet use the ACD provider.

In this dialog you manage the ACD connections used for connecting external ACD systems to the OpenScape Media Server. If an external ACD system is connected to the OpenScape Media Server via such an ACD connection, applications of the OpenScape Media Server can hand calls over to the relevant ACD system for further distribution.



- **Default Call Center**
- **<List of all call center connections>**

  Shows all ACD connections that connect the OpenScape Media Server to external ACD systems.

  To select the relevant ACD connection, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected ACD connection or remove the selected ACD connection.
- **Edit**

  Opens a dialog in which you can edit the settings of the selected ACD connection.
- **Remove**

  Removes the selected ACD connection from the OpenScape Media Server configuration.
- **Add**

  Opens a configuration dialog in which you can create a new ACD connection.

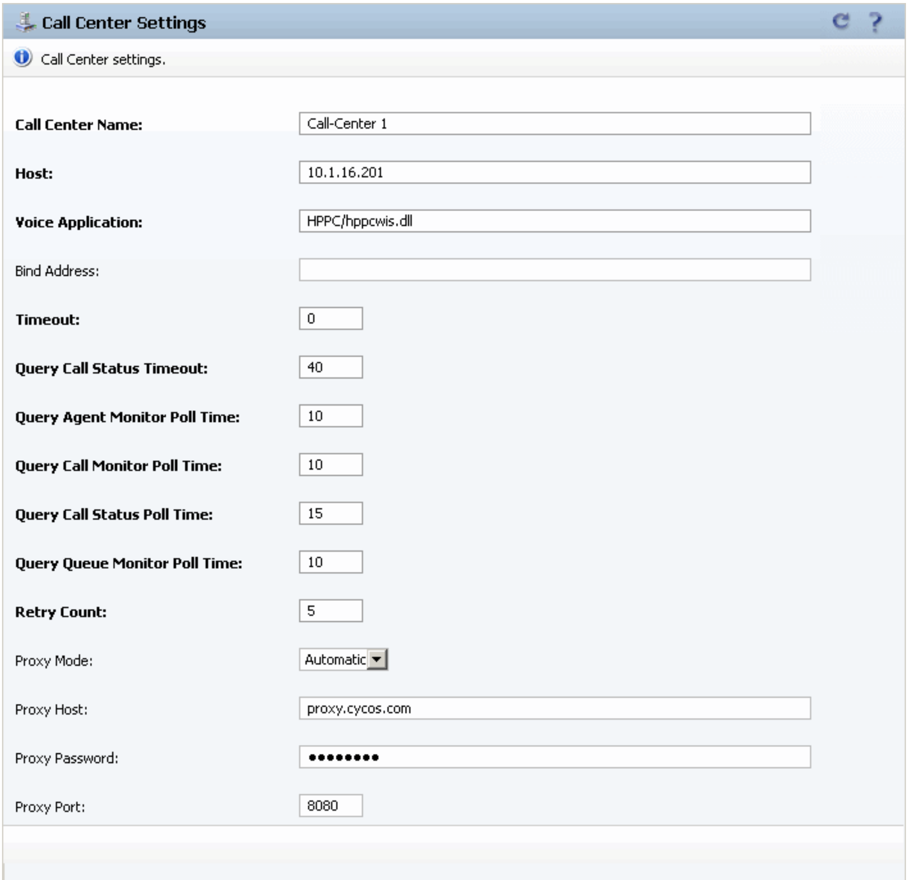
15.2.6.1 ACD Connection

Invocation in the Common Management Platform:
[Provider] Automatic Call Distribution (ACD) > **Adding / Editing**

NOTICE:

The OpenScape Media Server does not yet use ACD connections.

In this dialog you perform the settings of an ACD connection for an external ACD system to connect to the OpenScape Media Server.

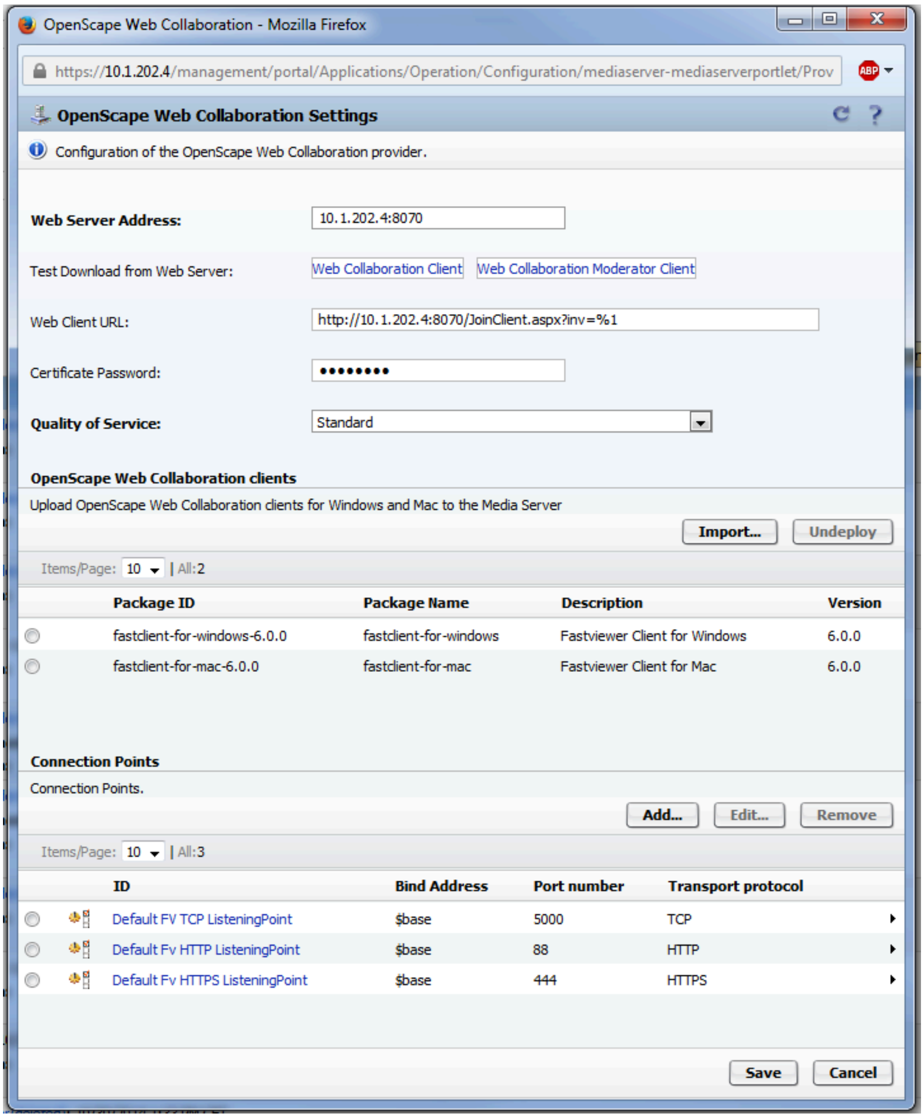


- **Call Center Name**
- **Host**
- **Voice Application**
- **Bind Address**
- **Timeout**
- **Query Call Status Timeout**
- **Query Agent Monitor Poll Time**
- **Query Call Monitor Poll Time**
- **Query Call Status Poll Time**
- **Query Queue Monitor Poll Time**
- **Retry Count**
- **Proxy Mode**
- **Proxy Host**
- **Proxy Password**
- **Proxy Port**
- **Proxy User**

15.2.7 OpenScape Web Collaboration Provider

Invocation in the Common Management Platform:
[Provider] OpenScape Web Collaboration

In this dialog you manage the settings for the OpenScape Web Collaboration provider.



- **Download Address for WebCollaboration clients**

  Specifies the IP address (IPv4, IPv6), under which the Web Collaboration services shall be accessible on the local computer system of the OpenScape Media Server.

  If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

  Port 8070 (http) and port 7443 (https) is always used for the Web Collaboration services.

Default:	auto$IPv4

Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name> – auto$IPv4 – auto$IPv6 – https addresses

For more details see the table below:

NOTICE:

It is also possible to use secure addresses with https.

Input	Download URL	remarks
auto$IPv4	http://<ipv4>:<port>/fvclient/ fastclient_i_<session_number>.exe	The IP address and the port will be taken from the configuration of the MS-internal tomcat provider. This is the default value
auto$IPv6	http://<ipv6>:<port>/fvclient/ fastclient_i_<session_number>.exe	The IP address and the port will be taken from the configuration of the MS-internal tomcat provider.
<ip>:<port>, e.g. 172.3.45.234:8080	http://<ip>:<port>/fvclient/ fastclient_i_<session_number>.exe	per default http is used
http://<ip>:<port>, e.g http://172.3.45.234:8080	http://<ip>:<port>/fvclient/ fastclient_i_<session_number>.exe	you have to give the right address and port here, as it is configured in the MS Tomcat configuration.
https://<ip>:<port>, e.g. https://172.3.45.234:3774	https://<ip>:<port>/fvclient/ fastclient_i_<session_number>.exe	you have to give the right address and port here, as it is configured in the MS Tomcat configuration.
https://myserver.mycompany:3774	https://myserver.mycompany:3774/ fvclient/ fastclient_i_<session_number>.exe	to make this work, a DNS entry must exist for the given FQDN that points to the MS-internal Tomcat. This format is necessary when signed certificates are used. Normally they are bound to a domain.

- **Web Client URL**

  Specifies the URL under which OpenScape Web Collaboration services of the OpenScape Media Server are accessible.

  This URL has the following general format.

  `http://`<FQDN of the Media Server>`:8070/JoinClient.aspx?inv=%1`

  For `<FQDN of the Media Server>` you need to enter the fully qualified host name under which OpenScape Web Collaboration clients can reach the OpenScape Media Server from outside.

- **Quality of Service**

  Defines the quality of service (DSCP) used for the RTP communication between OpenScape Media Server and RTP-based devices via the relevant RTP streaming route.

  The standardized and experimental service qualities can be selected.

Default:	Expedited Forwarding (EF)
Possible values:	– Assured Forwarding Class 1, Low Drop Precedence (AF11) – Assured Forwarding Class 1, Medium Drop Precedence (AF12) – Assured Forwarding Class 1, High Drop Precedence (AF13) – Assured Forwarding Class 2, Low Drop Precedence (AF21) – Assured Forwarding Class 2, Medium Drop Precedence (AF22) – Assured Forwarding Class 2, High Drop Precedence (AF23) – Assured Forwarding Class 3, Low Drop Precedence (AF31) – Assured Forwarding Class 3, Medium Drop Precedence (AF32) – Assured Forwarding Class 3, High Drop Precedence (AF33) – Assured Forwarding Class 4, Low Drop Precedence (AF41) – Assured Forwarding Class 4, Medium Drop Precedence (AF42) – Assured Forwarding Class 4, High Drop Precedence (AF43) – Expedited Forwarding (EF) – Precedence 1 (CS1) – Precedence 2 (CS2) – Precedence 3 (CS3) – Precedence 4 (CS4) – Precedence 5 (CS5) – Precedence 6 (CS6) – Precedence 7 (CS7) – Standard (CS0) – <further experimental DSCP code points in binary format>

- **OpenScape Web Collaboration clients> Import**

  Opens a dialog in which you can upload a new OpenScape Web Collaboration program module on the OpenScape Media Server. Users can download these files via permanently pre-set URLs for participating in web conferences with the relevant program module. Exactly one program module of each of the following types can be loaded on the OpenScape

Media Server. The file to be uploaded must have its associated defaulted file name.

  – Master module for Windows – `fastmaster.exe`
  – Master module for Mac – `fastmaster.app.zip`
  – Client module for Windows – `fastclient.exe`
  – Client module for Mac – `fastclient.app.zip`

- **OpenScape Web Collaboration clients> Undeploy**

  Uninstalls the selected program module from the OpenScape Media Server.

- **Connection points**

  Shows all Web Collaboration connection points via which users can download OpenScape Web Collaboration program modules from the OpenScape Media Server.

  To select the relevant connection point, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected connection point or remove it.

- **Connection points> Add**

  Opens a configuration dialog in which you can create a new Web Collaboration connection point for downloading OpenScape Web Collaboration program modules.

- **Connection points> Edit**

  Opens a dialog in which you can edit the settings of the selected Web Collaboration connection point.

- **Connection points> Remove**

  Removes the selected Web Collaboration connection point from the OpenScape Media Server configuration.

- **Listening points**

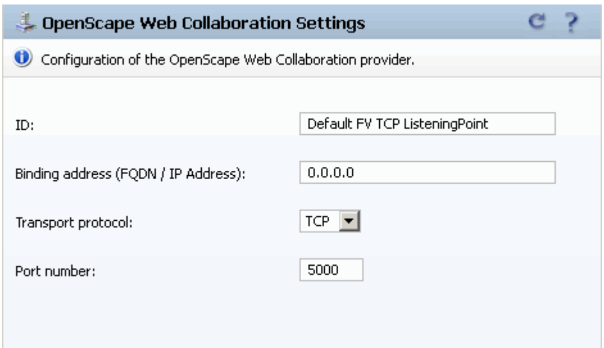
  Shows all default listening points that can be selected, as well as their transport protocols and the ports for Fastviewer:

Default FV	Port number
TCP ListeningPoint	5000
HTTP ListeningPoint	88
HTTPS ListeningPoint	444

15.2.7.1 Web Collaboration Connection Points

Invocation in the Common Management Platform:
[Provider] OpenScape Web Collaboration> Adding / Editing (connection points)

In this dialog you perform the settings of a OpenScape Web Collaboration connection points.



- **ID**

  Defines the unique name of the connection point. Under this name the connection point is administered in the CMP.

Default:	–
Possible values:	<unique name >

- **Bind address**

  Defines the IP address (IPv4, IPv6) that the OpenScape Media Server uses on the local computer system for the relevant connection point.

  If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

  If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

  If the value **0.0.0.0** is configured as bind address, all IP adresses are used that are available on the computer system of the OpenScape Media Server.

Default:	0.0.0.0
Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name> – auto$IPv4 – auto$IPv6

- **Transport protocol**

  Specifies the transport protocol that the OpenScape Media Server uses for the relevant listening point.

Default:	TCP
Possible values:	– TCP – HTTP – HTTPS

Remark:	If you create a connection point for the HTTPS transport protocol, you need to configure the settings **Certificate**, **Root Certificate** and **Certificate Password** in the settings of the OpenScape Web Collaboration provider.

- **Port number**

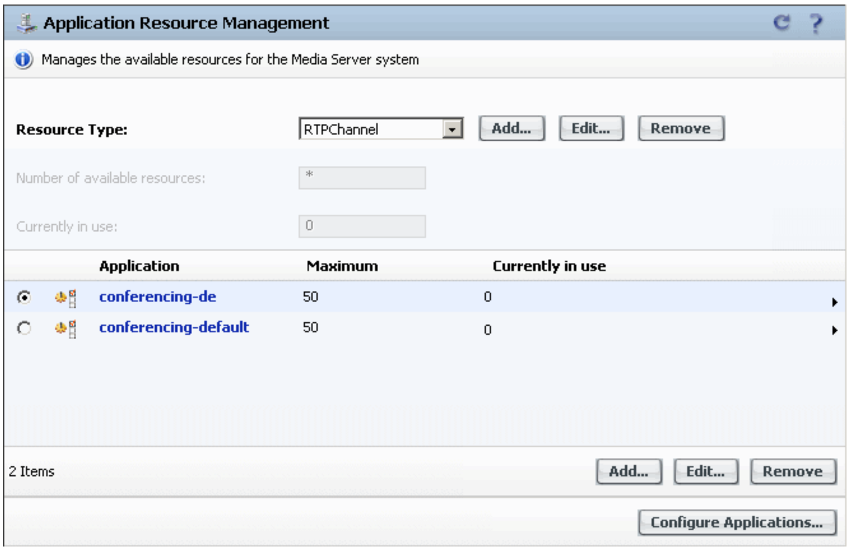
  Specifies the port that the OpenScape Media Server uses for the relevant connection point.

TCP	5000
HTTP	88
HTTPS	444
Possible values:	<port number>
Remark:	If the OpenScape Media Server is situated behind a firewall, you need to release the port configured here for the selected transport protocol in this firewall.

15.2.8 Application Partitioning

Invocation in the Common Management Platform:
[Providers] Application Partitioning

This dialog displays how the resources of the Media Server computer system distribute among the configured applications.



- **Resource Type**

  Specifies the name of the resource type the distribution of which is displayed. Furthermore, you can edit or remove the settings of the selected resource type.

Default:	–

Possible values:	– ConferenceMixingUnit – RTPChannel – Session – VideoComposer

- **Add**

  Opens a configuration dialog in which you can create a new resource type for administration.

  Creating a new resource type is useful if e.g. you program an individual application for the OpenScape Media Server that uses new resource types; or if you have inadvertently deleted one of the default types.
- **Edit**

  Opens a dialog in which you can edit the settings of the selected resource type.
- **Remove**

  Deletes the selected resource type. The associated resource assignments will then be deleted as well.
- **Number of available resources**

  Displays how many resources of the selected resource type are provided by the OpenScape Media Server in total.
- **Currently in use**

  Displays how many resources of the selected resource type are currently allocated by the different applications.
- **<Resource assignment list >**

  Displays all resource assignments configured for the selected resource type.

  To select the relevant resource assignment, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected resource assignment or remove the resource assignment.
- **Add**

  Opens a configuration dialog in which you can assign resources of the selected resource type to an installed application.
- **Edit**

  Opens a configuration dialog in which you can edit the settings of the selected resource assignment.
- **Remove**

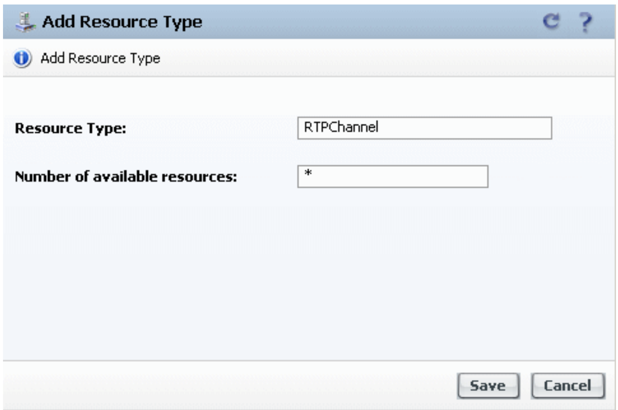
  Removes the selected resource assignment.
- **Configure Applications**

  Opens a configuration dialog in which you can control the resource management based on applications.

15.2.8.1 Resource Type

Invocation in the Common Management Platform:
[Providers] Application Partitioning> Add / Edit

In this dialog you define how many resources the OpenScape Media Server provides for a resource type of the application partitioning.



- **Resource Type**

  Defines the name of the resource type for which the available number of resources is defined.

Default:	–
Possible values:	– ConferenceMixingUnit – RTPChannel – Session – VideoComposer

- **Number of available resources**

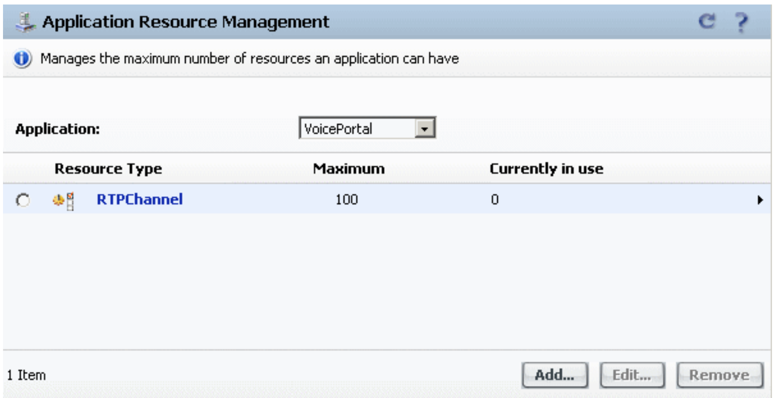
  Specifies how many resources of this resource type are available in the OpenScape Media Server. This total number can be distributed among the various OpenScape Media Server applications.

  The * wildcard defines an infinite number of resources.

15.2.8.2 Application-based Partitioning

Invocation in the Common Management Platform:
[Providers] Applications Partitioning> Configure Applications

This dialog shows which resources are assigned to a selected application.



- **Application**

  Specifies the name of the application the assignments of which are displayed. Only the applications configured in the OpenScape Media Server are offered for selection.
- **<Resource assignment list >**

  Displays all resource assignments configured for the selected application.

  To select the relevant resource assignment, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected resource assignment or remove the resource assignment.
- **Add**

  Opens a configuration dialog in which you assign resources of an available resource type to the selected application.
- **Edit**

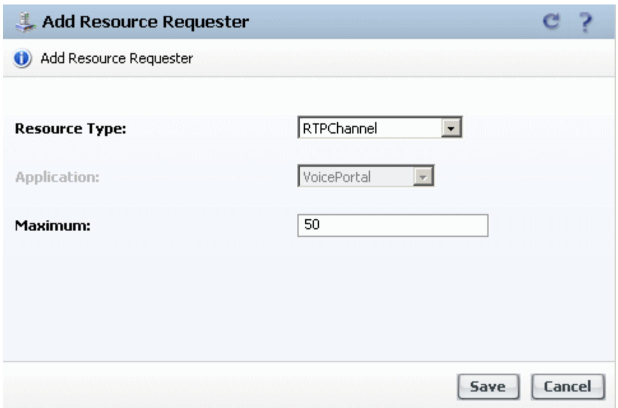
  Opens a configuration dialog in which you can edit the settings of the selected resource assignment.
- **Remove**

  Removes the selected resource assignment.

15.2.8.3 Adding a Resource Assignment

Invocation in the Common Management Platform:
• **[Providers] Application Partitioning> Add / Edit** • **[Providers] Application Partitioning> Configure Applications> Add / Edit**

In this dialog you assign a number of selected resources to an application.



- **Resource Type**

  Specifies the name of the resource type of which you want to assign resources to an application.

  This field is permanently allocated with the name of a resource type if you open the dialog from the resource-based application partitioning.

Default:	See description

Possible values:	– ConferenceMixingUnit – RTPChannel – Session – VideoComposer

- **Application**

  Specifies the name of the application that you want to assign a number of resources of the selected resource type.

  This field is permanently allocated with an application name if you open the dialog from the application-based application partitioning.
- **Maximum**

  Defines the maximum number of resources that the selected application may use of the selected resource type.

15.2.9 Nodes Replication

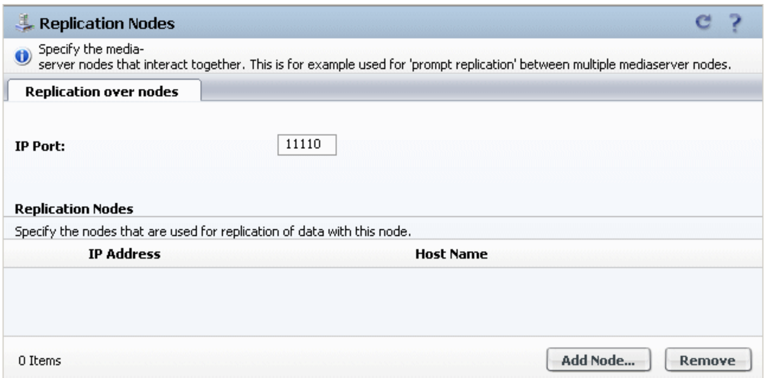
Invocation in the Common Management Platform:
[Providers] Nodes Replication

NOTICE:

You need to consider the node replication settings only if you use several OpenScape Media Servers as Media Server farm under OpenScape UCApplication.

If the OpenScape Media Server is used in a Media Server farm, it can automatically replicate customized voice portal welcome and name announcements to all other OpenScape Media Servers of the farm.

In this dialog you configure the settings for announcement replication.



- **IP Port**

  Specifies the port via which the OpenScape Media Servers exchange the control information of the replication mechanism.

Default:	11110
Possible values:	<port number>

- **<list of replication nodes >**

  Displays all OpenScape Media Servers of the OpenScape system to which the local OpenScape Media Server replicates customized welcome and name announcements.

  To select the relevant OpenScape Media Server, enable the radio button that precedes the associated list entry. You can then remove the OpenScape Media Server from the list. See **Remove**.

  NOTICE:

  If you use a Media Server farm you should configure each remote OpenScape Media Server on each OpenScape Media Server of the Media Server farm for node replication.

- **Add Node**

  Opens a dialog in which you can configure an OpenScape Media Server for node replication.
- **Remove**

  Removes the selected OpenScape Media Server from the list of nodes to which the local OpenScape Media Server replicates customized welcome and name announcements.

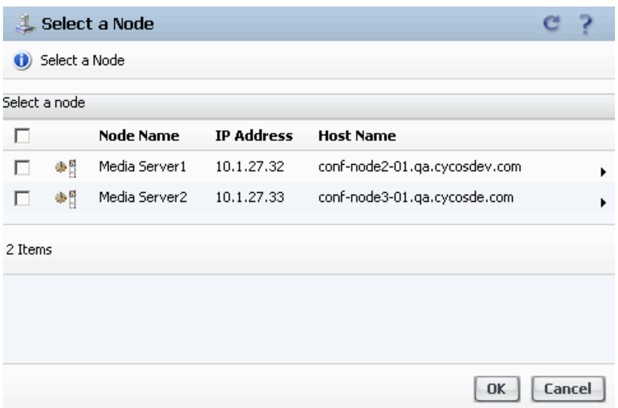
15.2.9.1 Node Selection for Node Replication

Invocation in the Common Management Platform:
[Providers] Nodes Replication> Add Node

NOTICE:

You need to consider the node replication settings only if you use several OpenScape Media Servers as Media Server farm under OpenScape UCApplication.

In this dialog you determine remote OpenScape Media Servers to which the local OpenScape Media Server is to replicate the welcome and name announcements of its voice portal.



- **<Node list >**

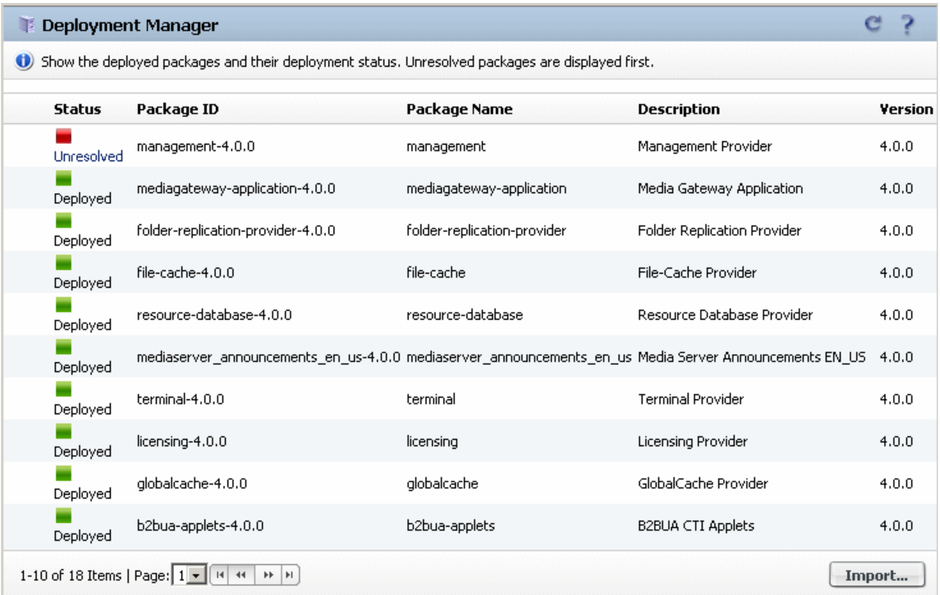
  To select the relevant OpenScape Media Server, enable the radio button that precedes the associated list entry. You can then click on **OK** to copy the selected OpenScape Media Servers to the replication list.

  > **NOTICE:**
  >
  > If you use a Media Server farm you should configure each remote OpenScape Media Server on each OpenScape Media Server of the Media Server farm for node replication.

15.2.10 Deployment Manager

Invocation in the Common Management Platform:
[Provider] Deployment Manager

The deployment manager shows which software components are installed for the OpenScape Media Server.



Deployment Manager

Show the deployed packages and their deployment status. Unresolved packages are displayed first.

Status	Package ID	Package Name	Description	Version
Unresolved	management-4.0.0	management	Management Provider	4.0.0
Deployed	mediagateway-application-4.0.0	mediagateway-application	Media Gateway Application	4.0.0
Deployed	folder-replication-provider-4.0.0	folder-replication-provider	Folder Replication Provider	4.0.0
Deployed	file-cache-4.0.0	file-cache	File-Cache Provider	4.0.0
Deployed	resource-database-4.0.0	resource-database	Resource Database Provider	4.0.0
Deployed	mediaserver_announcements_en_us-4.0.0	mediaserver_announcements_en_us	Media Server Announcements EN_US	4.0.0
Deployed	terminal-4.0.0	terminal	Terminal Provider	4.0.0
Deployed	licensing-4.0.0	licensing	Licensing Provider	4.0.0
Deployed	globalcache-4.0.0	globalcache	GlobalCache Provider	4.0.0
Deployed	b2bua-applets-4.0.0	b2bua-applets	B2BUA CTI Applets	4.0.0

1-10 of 18 Items | Page: 1

Import...

- **<List of all software components >**

  Shows all software components that are installed for the OpenScape Media Server.

  The **ID**, **Name**, a short **Description** and the provided **Version** is listed for each component made available. Furthermore, the **Status** indicates whether the OpenScape Media Server was able to start the relevant component trouble-free.

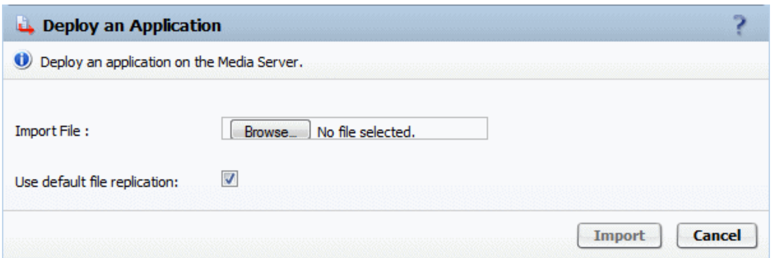
- **Import**

  Opens a dialog in which you can provide deployment packages of a Media Server component for the OpenScape Media Server.

15.2.10.1 Deploying an Application

Invocation in the Common Management Platform:
[Provider] Deployment Manager > Import

In this dialog you provide the OpenScape Media Server with a new component by a deployment package. You can create the deployment package of such a component with the Application Builder of OpenScape UCApplication, for example.



- **Import File**

  Specifies the deployment package to be provided in the OpenScape Media Server.

  NOTICE:

  A deployment package must have the extension `.mdp.zip`. If you attempt to provide a file with a differing extension, the deployment process is aborted with an error message.

  NOTICE:

  Due to Tomcat max upload size limitations it is currently only supported to upload zip files that do not exceed 100MB in size.

- **Import**

  Provides the deployment package in the OpenScape Media Server that is specified under **Import File**. After the deployment package has been provided, the OpenScape Media Server starts the relevant component independently.

- **Use default file replication**

  Determines whether the individual deployment package shall be automatically replicated to all other OpenScape Media Servers of a Media Server farm.

15.2.11 Announcements and Resources

Invocation in the Common Management Platform:
[Providers] Announcements and Resources

In this dialog you manage files that depend on applications and are stored on the OpenScape Media Server computer system.

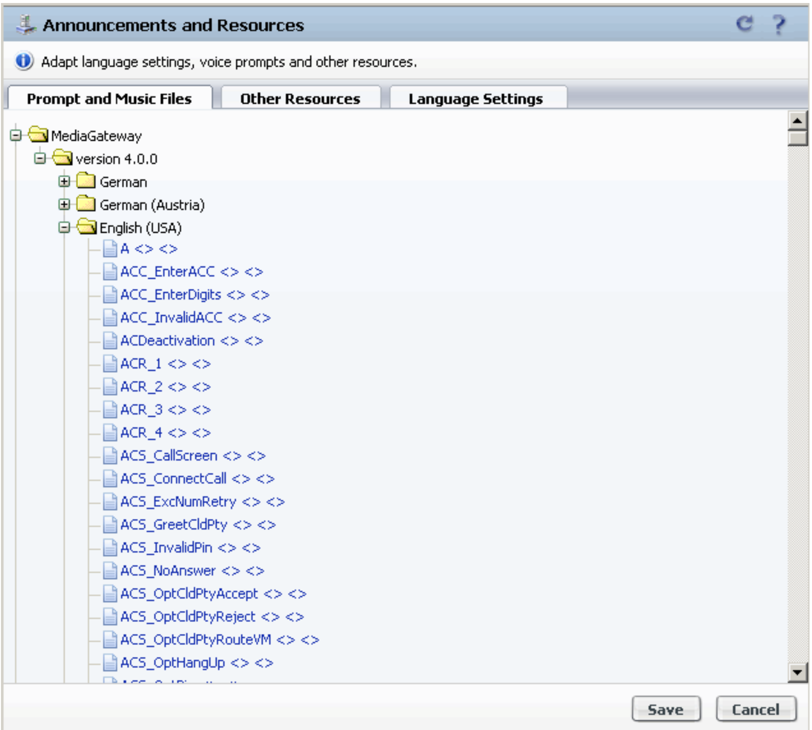
The settings in this dialog are grouped as follows:

- Prompt and Music Files
- Other Resources
- Language Settings

15.2.11.1 Prompt and Music Files

Invocation in the Common Management Platform:
[Provider] Announcements and Resources > **Prompt and Music Files**

In this dialog you administer files that depend on applications, containing prompts and music. These prompts are e.g. the announcements of OpenScape Voice assigned to the Media Gateway application and the voice portal announcements.



The files that depend on applications are administered in the OpenScape Media Server in a default directory structure. In this dialog you see the files in this structure. Where applicable, each file name is followed by the below information in pointed brackets and in the given sequence:

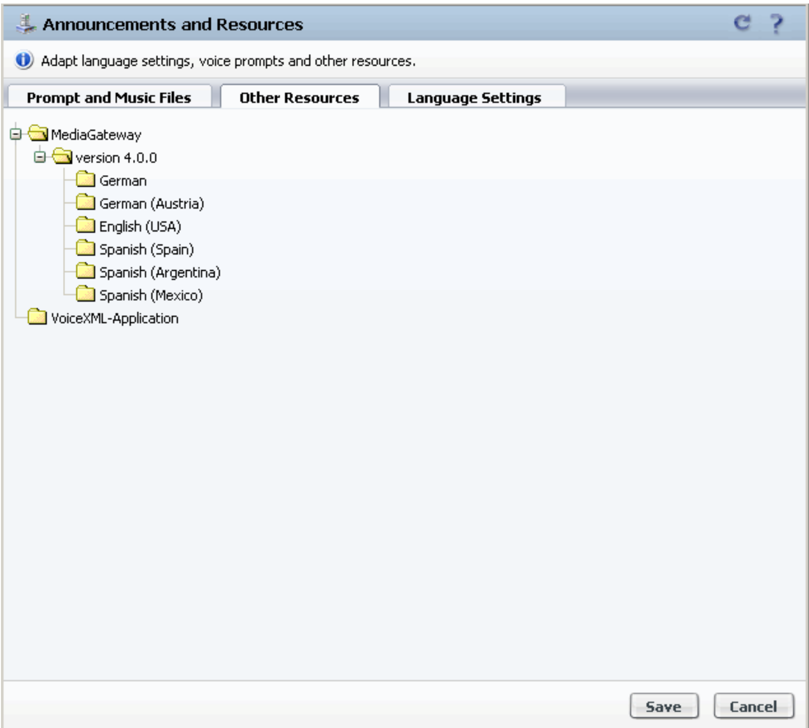
- Short file description
- Alternate text

When you click a file's name you reach a configuration dialog in which you can edit the relevant file.

15.2.11.2 Other Resources

Invocation in the Common Management Platform:
[Provider] Announcements and Resources > **Other Resources**

In this dialog you administer additional application-specific files. Such files are e.g. the grammar files for the voice-controlled voice portal application.



The files that depend on applications are administered in the OpenScape Media Server in a default directory structure. In this dialog you see the files in this structure. Where applicable, each file name is followed by the below information in pointed brackets and in the given sequence:

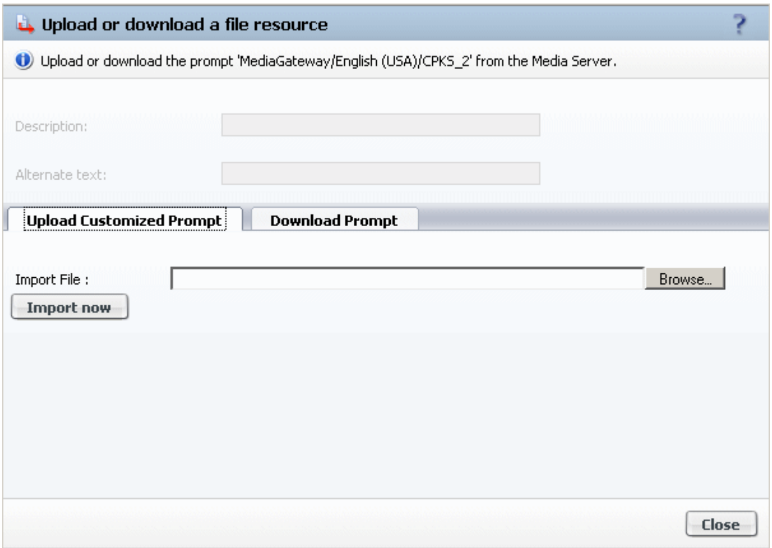
- Short file description
- Alternate text

When you click a file's name you reach a configuration dialog in which you can edit the relevant file.

15.2.11.3 Editing Prompts and Resources

Invocation in the Common Management Platform:
• **[Providers] Announcements and Resources** > **Prompt and Music Files** > **<File >** • **[Providers] Announcements and Resources** > **Other Resources** > **<File >**

In this dialog you edit a prompt or music file that depends on an application or the file of another resource.



- **Description**

  Shows a short description of the relevant file as far as such information has been defined.
- **Alternate text**

  Shows an alternative text of the relevant file as far as this text has been defined.
- **Upload Customized Prompt / Resource**

  On this tab you can load an additional, individual version for the relevant file on the OpenScape Media Server. The original file is maintained on the OpenScape Media Server.

  Subsequently, you can delete the individual version of the file again.

  When you load an individual file version on the OpenScape Media Server the individual file is played from then on in place of the original file.
- **Download Prompt / Resource**

  On this tab you can download the relevant file from the OpenScape Media Server to the local computer system.

  If an individual version is available on the OpenScape Media Server for the relevant file, you can download this file to the local computer system also, or remove it from the OpenScape Media Server.

  When you remove the individual file version from the OpenScape Media Server the original file is played again.

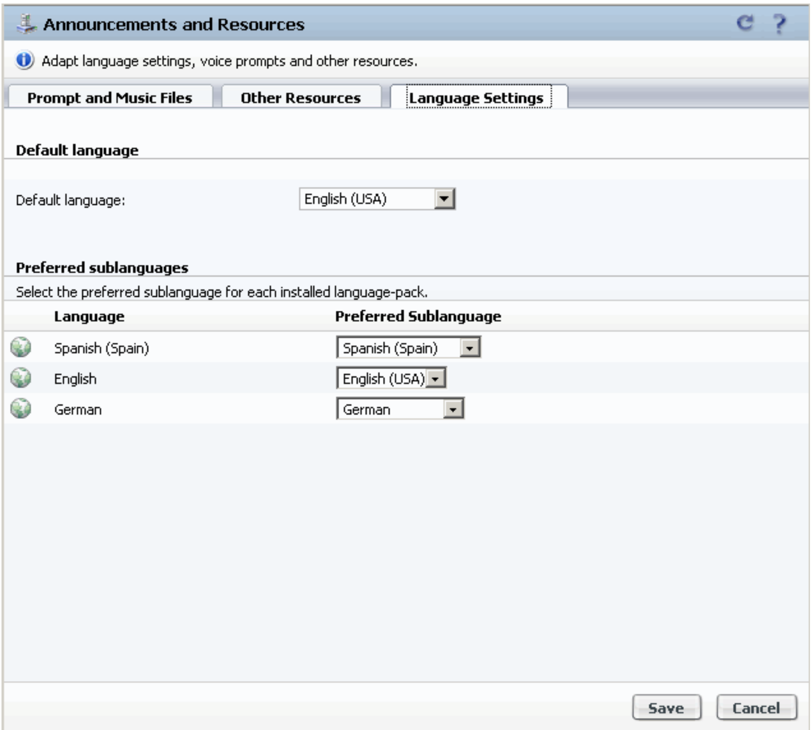
15.2.11.4 Language Settings

Invocation in the Common Management Platform:
[Provider] Announcements and Resources > **Language Settings**

NOTICE:

You need to consider the language settings only if you use the OpenScape Media Server at OpenScape Voice.

In this dialog you determine the voice settings for OpenScape Voice prompts if the OpenScape Media Server is used at OpenScape Voice.



- **Default language**

  Defines the language the announcements and tones of which the OpenScape Media Server uses if no language has been specified with a play-back prompt by OpenScape Voice.
- **<List of preferred sublanguages >**

  Shows all language packs of the basic language that are installed on the OpenScape Media Server. Several sublanguages can be installed on the OpenScape Media Server for one basic language. For example, the sublanguages for India and the US for the basic language English.

  In this case you can determine under **Preferred Sublanguage** which sublanguage to use for the associated basic language.

15.2.12 Internet Radio Streaming

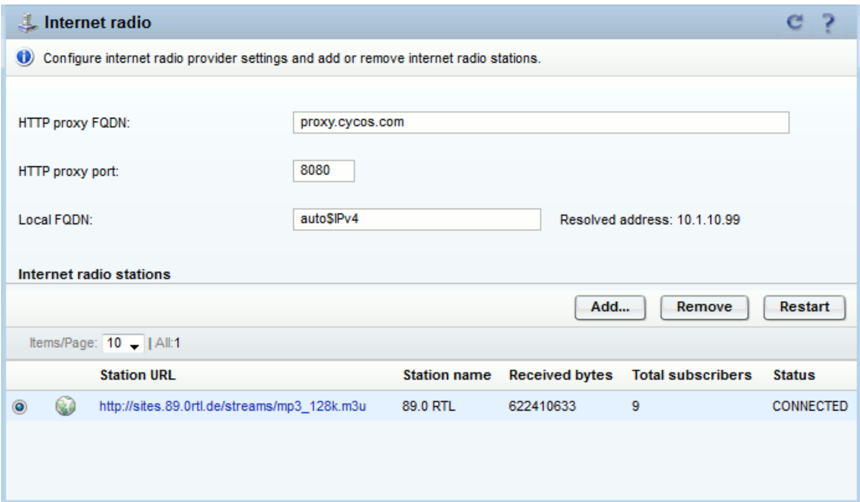
Invocation in the CMP:
[Providers] Internet Radio Streaming

NOTICE:

You need to consider the Internet radio streaming settings only if you use the OpenScape Media Server at OpenScape Voice.

In this dialog you perform the settings the Internet Radio Streaming Provider of the OpenScape Media Server uses for playing music-on-hold.

If you wish to use the Internet Radio Streaming Provider, you need to configure at least one Internet radio station.



- **HTTP proxy FQDN**

  If the Internet Radio Streaming Provider is to connect to the configured Internet radio stations via a proxy, specify under **HTTP proxy FQDN** the proxy's IP address (IPv4, IPv6).

  If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.
- **HTTP proxy port**

  If the Internet Radio Streaming Provider is to connect to the configured Internet radio stations via a proxy, specify under **HTTP proxy port** the port number to which the Internet Radio Streaming Provider is to broadcast.
- **Local FQDN**

  Specifies the IP address (IPv4, IPv6) the Internet Radio Streaming Provider is to use on the local computer system of the OpenScape Media Server.

  If the OpenScape Media Server is to automatically select an IPv4 or IPv6 address from the available IP addresses, you can enter the variables **auto $IPv4** or **auto$IPv6**. In this case you see next to the field the selected real IP address.

- **<List of all station URLs >**

  Displays all configured Internet radio stations. You can select all Internet radio stations displayed here in the MGCP provider for music-on-hold.

  The following information is displayed for every Internet radio station:

  – **Station name**

    Indicates the name of the Internet radio station. This information is broadcasted by the Internet radio station in the stream.

  – **Received bytes**

    Indicates the amount of data received by the Internet radio station since the last connection start.

  – **Total subscribers**

    Indicates the number of subscribers to whom music from an Internet radio station is currently played.

  – **Status**

    Indicates the current status of the connection to the Internet radio station.

  To select the relevant Internet radio station, enable the radio button that precedes the associated list entry. You can then remove or restart the selected Internet radio station.

- **Restart**

  Closes the current connection to the selected Internet radio station and establishes the connection anew.

  IMPORTANT:

  A new start will interrupt the playback of Internet radio station music for some seconds.

- **Remove**

  Deletes the settings performed for the selected Internet radio station.

- **Add**

  Opens a configuration dialog in which you can perform the settings for a new Internet radio station.

15.2.12.1 Internet Radio Station

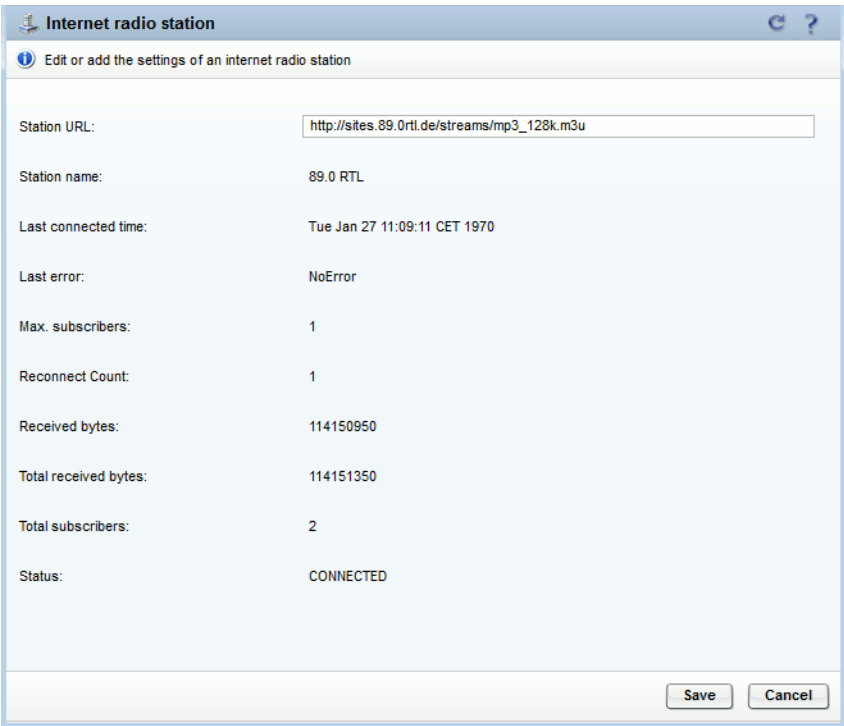
Invocation in the CMP:
[Providers] Internet Radio Streaming > **Add**

NOTICE:

You need to consider the settings for Internet radio stations only if you use the OpenScape Media Server at OpenScape Voice.

In this dialog you specify the Internet radio station that the Internet Radio Streaming Provider of the OpenScape Media Server connects to play the broadcasted music as music-on-hold.

If you wish to use the Internet Radio Streaming Provider, you need to configure at least one Internet radio station.



- **Station URL**

  Specifies the URL under which the Internet radio station can be reached.
- **Station name**

  Indicates the name of the Internet radio station. This information is broadcasted by the Internet radio station in the stream.
- **Last connected time**

  Indicates when the Internet Radio Streaming Provider set up the last connection to the Internet radio station.
- **Last error**

  Indicates the last occurred error.
- **Max. subscribers**

  Indicates the maximum number of subscribers to whom music from an Internet radio station was broadcasted simultaneously.
- **Reconnect Count**

  Indicates how often the connection to an Internet radio station was reestablished.
- **Received bytes**

  Indicates the amount of data received by the Internet radio station since the last connection start.
- **Total received bytes**

  Indicates the amount of data received by the Internet radio station since the last start of the Internet Radio Streaming Provider.

- **Total subscribers**

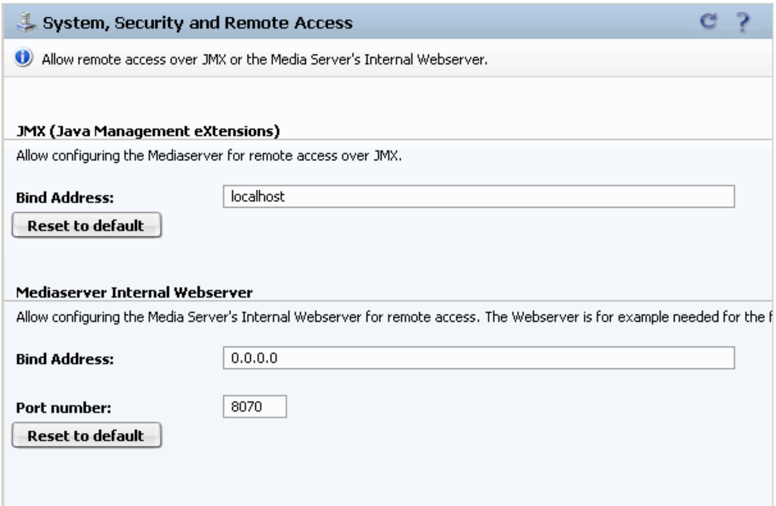
  Indicates the number of subscribers to whom music from an Internet radio station is currently played.
- **Status**

  Indicates the current status of the connection to the Internet radio station.

15.2.13 System, Security and Remote Access

Invocation in the Common Management Platform:
[Providers] System, Security and Remote Access

In this dialog you manage the settings which define how systems can access the OpenScape Media Server. For example how the OpenScape System Monitor can access the statistics framework of the OpenScape Media Server via JMX (Java Management eXtensions).



JMX (Java Management eXtensions)

Defines how the Java Management eXtensions of the OpenScape Media Server can be accessed.

- **Bind Address**

  Defines the IP address that the OpenScape Media Server uses to give access to the Java Management eXtensions.

  If `localhost` is configured, the Java Management eXtensions can only be accessed from the local computer system.
- **Reset to default**

  Reset the value of **Bind Address** to `localhost`.

Mediaserver Internal Webserver

Defines how the internal Tomcat web server of the OpenScape Media Server can be accessed.

- **Bind Address**

  Defines the IP address that the OpenScape Media Server uses to give access to the internal Tomcat web server. The connection to the Tomcat web server is only used for internal communication of the OpenScape Media Server.

  If the value `0.0.0.0` is configured, the internal Tomcat web server can be accessed via every IP address that is available on the OpenScape Media Server´s computer system.
- **Port number**

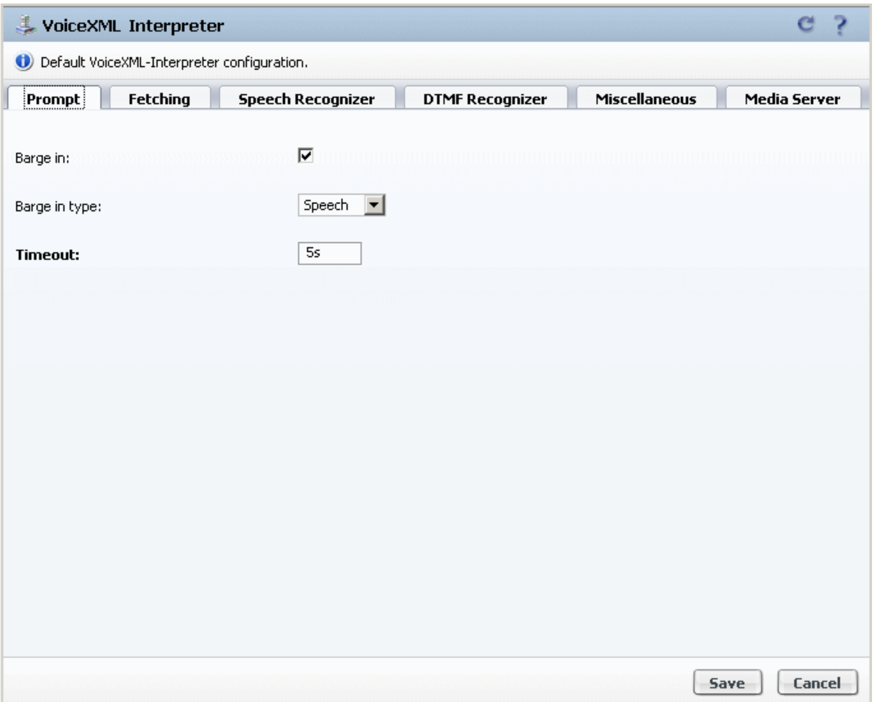
  Defines the port that the OpenScape Media Server uses to give access to the internal Tomcat web server.
- **Reset to default**

  Reset the value of **Bind Address** to `0.0.0.0` and the value of **Portnummer** to `8070`.

15.2.14 VoiceXML-Interpreter

Invocation in the Common Management Platform:
[Providers] VoiceXML-Interpreter

In this dialog you manage the default settings for VoiceXML document attributes that are valid in the VoiceXML-Interpreter context. The VoiceXML-Interpreter uses these settings if a VoiceXML document does not define an individual value for one of these VoiceXML attributes.



The following document attributes and their default settings are available for the VoiceXML-Interpreter:

- **Prompt Settings**

Barge in	Barge in type	Timeout

- **Fetching**

Fetchtimeout		
Audiofetchhint	Audiomaxage	Audiomaxstale
Datafetchhint	Datamaxage	Datamaxstale
Documentfetchhint	Documentmaxage	Documentmaxstale
Grammarfetchhint	Grammarmaxage	Grammarmaxstale
Objectfetchhint	Objectmaxage	Objectmaxstale
Scriptfetchhint	Scriptmaxage	Scriptmaxstale
Fetchaudio		
Fetchaudiodelay		
Fetchaudiominimum		

- **Speech Recognizer Settings**

Confidencelevel		
Sensitivity		
Speed vs accuracy		
Completetimeout	Incompletetimeout	Maxspeechtimeout
Timeout		

- **DTMF Recognizer Settings**

Interdigittimeout	Termtimeout	Timeout
Termchar		

- **Miscellaneous**

Inputmodes	Universals	Maxn#best

- **Media Server Settings**

Transferoriginator	Billingnumber	
SSMLwithnamespace		
Localaudio		

15.2.14.1 Prompt Settings of the VoiceXML-Interpreter

Invocation in the Common Management Platform:
[Provider] VoiceXML-Interpreter > Prompt tab

NOTICE:

You find further information about these settings in the W3C standard with the title Voice Extensible Markup Language (VoiceXML) Version 2.0 or Voice Extensible Markup Language (VoiceXML) Version 2.1.

These settings control the default behavior of the VoiceXML-Interpreter when playing announcements.

Barge in

Default:	<activated >

Defines whether a user must listen to an announcement until the end or whether the system allows a voice or DTMF entry before the announcement playback is complete.

Barge in type

Default:	Speech
Possible values:	• Speech – Announcement stops after any entry • Hotword – Announcement stops after valid command only
Remark:	Is used in combination with the **Barge-in** setting.

Defines the circumstances under which an announcement is stopped when a user makes a voice or DTMF entry in the frame of barge in.

In case of the **Speech** setting the announcement playback is stopped as soon as the system recognizes a voice or DTMF entry. It is irrelevant whether or not the voice or DTMF entry represents a valid command.

In case of the **Hotword** setting the announcement playback is only stopped if the system recognizes a valid command.

Timeout

Default:	5 [Seconds]
Possible values:	<Time> [seconds]

Defines the period after the end of the announcement playback in which a user has to make a voice or DTMF entry. If the system fails to recognize a voice or DTMF entry within this period, it signals internally that the user has not made an entry.

15.2.14.2 Fetching Settings of the VoiceXML-Interpreter

Invocation in the Common Management Platform:
[Provider] VoiceXML-Interpreter > Fetching tab

NOTICE:

You find further information about these settings in the W3C standard with the title Voice Extensible Markup Language (VoiceXML) Version 2.0 or Voice Extensible Markup Language (VoiceXML) Version 2.1.

These settings control the default behavior of the VoiceXML-Interpreter when loading referenced resources. The following resource types are distinguished:

- Sound file (e. g. file for a announcement)
- Data (e. g. requested calendar data for a user)
- Document (e. g. further referenced VoiceXML documents)
- Grammar (e. g. grammars for recognizing voice commands)
- Object (is currently not used by the OpenScape Media Server)
- Script (e. g. external Java scripts)

Fetchtimeout

Default:	5 000 [milliseconds]
Possible values:	<time> [milliseconds]

Defines the maximum period the VoiceXML-Interpreter waits for receiving a requested resource. If the VoiceXML-Interpreter does not receive a requested resource within this period, it signals internally that the requested resource could not be received.

Audiofetchhint

Default:	Prefetch
Possible values:	• Prefetch – sound files are loaded with document • Save – sound files are loaded if required

Defines when the VoiceXML-Interpreter loads a sound file that is referenced in the just interpreted VoiceXML document.

In case of the **Prefetch** setting the VoiceXML-Interpreter loads all sound files of a VoiceXML document as soon as it starts to interpret the relevant document. It is irrelevant here whether some of these sound files will possibly not be played at all.

In case of the **Save** setting the VoiceXML-Interpreter loads the single sound files of a VoiceXML document precisely at the time when the relevant sound file is to be played.

Audiomaxage

Default:	500 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Audiomaxstale** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Audiomaxage defines the maximum permissible age of a sound file for the server still to be allowed to send it to the VoiceXML-Interpreter.

Audiomaxage = 43200 seconds (12 hours)

A sound file is created by a server at 00:00. The VoiceXML-Interpreter retrieves this sound file from the server at 15:00.

Since the age of the sound file exceeds the period specified in **Audiomaxage**, the server needs to recreate the sound file before it may send it to the VoiceXML-Interpreter.

Audiomaxstale

Default:	1 000 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Audiomaxage** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Audiomaxstale defines the maximum period that may exceed the maximum age of a sound file (**Audiomaxage**) for the sound file still to be sent to the VoiceXML-Interpreter. Only when the age of the sound file exceeds the sum of **Audiomaxstale** and **Audiomaxage**, the server needs to recreate the sound file before sending it to the VoiceXML-Interpreter.

Audiomaxage = 43 200 seconds (12 hours)

Audiomaxstale= 21 600 seconds (6 hours)

A sound file is created by a server at 00:00. The VoiceXML-Interpreter retrieves this sound file from the server at 15:00.

The age of the sound file exceeds the maximum permissible age from **Audiomaxage** by 5 hours. According to **Audiomaxstale** the age may exceed the setting from **Audiomaxage** by up to 6 hours. The server may thus send the sound file to the VoiceXML-Interpreter and need not recreate it.

Datafetchhint

Default:	Prefetch
Possible values:	• Prefetch – data resources are loaded with document • Save – data resources are loaded if required

Defines when the VoiceXML-Interpreter loads a data resource that is referenced in the just interpreted VoiceXML document.

In case of the **Prefetch** setting the VoiceXML-Interpreter loads all data resources of a VoiceXML document as soon as it starts to interpret the relevant document. It is irrelevant here whether some of these data resources will possibly not be used at all.

In case of the **Save** setting the VoiceXML-Interpreter loads the single data resources of a VoiceXML document precisely at the time when the relevant data resource is to be used.

Datamaxage

Default:	500 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Datamaxstale** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Datamaxage defines the maximum permissible age of a data resource for the server still to be allowed to send it to the VoiceXML-Interpreter.

Datamaxage = 43200 seconds (12 hours)

A data resource is created by a server at 00:00. The VoiceXML-Interpreter retrieves this data resource from the server at 15:00.

Since the age of the data resource exceeds the period specified in **Datamaxage**, the server needs to recreate the data resource before it may send it to the VoiceXML-Interpreter.

Datamaxstale

Default:	1 000 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Datamaxage** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Datamaxstale defines the maximum period that may exceed the maximum age of a data resource (**Datamaxage**) for the data resource still to be sent to the VoiceXML-Interpreter. Only when the age of the data resource exceeds the sum of **Datamaxstale** and **Datamaxage**, the server needs to recreate the data resource before sending it to the VoiceXML-Interpreter.

Datamaxage = 43 200 seconds (12 hours)

Datamaxstale = 21 600 seconds (6 hours)

A data resource is created by a server at 00:00. The VoiceXML-Interpreter retrieves this data resource from the server at 15:00.

The age of the data resource exceeds the maximum permissible age from **Datamaxage** by 5 hours. According to **Datamaxstale** the age may exceed the setting from **Datamaxage** by up to 6 hours. The server may thus send the data resource to the VoiceXML-Interpreter and need not recreate it.

Documentfetchhint

Default:	Prefetch

Possible values:	• Prefetch – documents are loaded with document • Save – documents are loaded if required

Defines when the VoiceXML-Interpreter loads a VoiceXML document that is referenced in the just interpreted VoiceXML document.

In case of the **Prefetch** setting the VoiceXML-Interpreter loads all VoiceXML documents of a VoiceXML document as soon as it starts to interpret the relevant document. It is irrelevant here whether some of these VoiceXML documents will possibly not be used at all.

In case of the **Save** setting the VoiceXML-Interpreter loads the single VoiceXML documents of a VoiceXML document precisely at the time when the relevant VoiceXML document is to be interpreted.

Documentmaxage

Default:	500 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Documentmaxstale** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Documentmaxage defines the maximum permissible age of a VoiceXML document for the server still to be allowed to send it to the VoiceXML-Interpreter.

Documentmaxage = 43200 seconds (12 hours)

A VoiceXML document is created by a server at 00:00. The VoiceXML-Interpreter retrieves this VoiceXML document from the server at 15:00.

Since the age of the VoiceXML document exceeds the period specified in **Documentmaxage**, the server needs to recreate the VoiceXML document before it may send it to the VoiceXML-Interpreter.

Documentmaxstale

Default:	1 000 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Documentmaxage** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Documentmaxstale defines the maximum period that may exceed the maximum age of a VoiceXML document (**Documentmaxage**) for the VoiceXML document still to be sent to the VoiceXML-Interpreter. Only when the age of the VoiceXML document exceeds the sum of **Documentmaxstale** and **Documentmaxage**, the server needs to recreate the VoiceXML document before it sends it to the VoiceXML-Interpreter.

Documentmaxage = 43 200 seconds (12 hours)

Documentmaxstale = 21 600 seconds (6 hours)

A VoiceXML document is created by a server at 00:00. The VoiceXML-Interpreter retrieves this VoiceXML document from the server at 15:00.

The age of the VoiceXML document exceeds the maximum permissible age from **Documentmaxage** by 5 hours. According to **Documentmaxstale** the age may exceed the setting from **Documentmaxage** by up to 6 hours. The server may thus send the VoiceXML document to the VoiceXML-Interpreter and need not recreate it.

Grammarfetchhint

Default:	Prefetch
Possible values:	• Prefetch – grammars are loaded with document • Save – grammars are loaded if required

Defines when the VoiceXML-Interpreter loads a grammar that is referenced in the just interpreted VoiceXML document.

In case of the **Prefetch** setting the VoiceXML-Interpreter loads all grammars of a VoiceXML document as soon as it starts to interpret the relevant document. It is irrelevant here whether some of these grammars will possibly not be used at all.

In case of the **Save** setting the VoiceXML-Interpreter loads the single grammars of a VoiceXML document precisely at the time when the relevant grammar is to be used.

Grammarmaxage

Default:	500 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Grammarmaxstale** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Grammarmaxage defines the maximum permissible age of a grammar for the server still to be allowed to send it to the VoiceXML-Interpreter.

Grammarmaxage = 43200 seconds (12 hours)

A grammar is created by a server at 00:00. The VoiceXML-Interpreter retrieves this grammar from the server at 15:00.

Since the age of the grammar exceeds the period specified in **Grammarmaxage**, the server needs to recreate the grammar before it may send it to the VoiceXML-Interpreter.

Grammarmaxstale

Default:	1 000 [Seconds]
Possible values:	<Time> [seconds]

Remark:	Is used in combination with the **Grammarmaxage** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Grammarmaxstale defines the maximum period that may exceed the maximum age of a grammar (**Grammarmaxage**) for the grammar still to be sent to the VoiceXML-Interpreter. Only when the age of the grammar exceeds the sum of **Grammarmaxstale** and **Grammarmaxage**, the server needs to recreate the grammar before sending it to the VoiceXML-Interpreter.

Grammarmaxage = 43 200 seconds (12 hours)

Grammarmaxstale = 21 600 seconds (6 hours)

A grammar is created by a server at 00:00. The VoiceXML-Interpreter retrieves this grammar from the server at 15:00.

The age of the grammar exceeds the maximum permissible age from **Grammarmaxage** by 5 hours. According to **Grammarmaxstale** the age may exceed the setting from **Grammarmaxage** by up to 6 hours. The server may thus send the grammar to the VoiceXML-Interpreter and need not recreate it.

Objectfetchhint

Default:	Prefetch
Possible values:	• Prefetch – objects are loaded with document • Save – objects are loaded if required

Defines when the VoiceXML-Interpreter loads a VoiceXML object that is referenced in the just interpreted VoiceXML document.

In case of the **Prefetch** setting the VoiceXML-Interpreter loads all VoiceXML objects of a VoiceXML document as soon as it starts to interpret the relevant document. It is irrelevant here whether some of these VoiceXML objects will possibly not be used at all.

In case of the **Save** setting the VoiceXML-Interpreter loads the single VoiceXML objects of a VoiceXML document precisely at the time when the relevant VoiceXML object is to be interpreted.

Objectmaxage

Default:	500 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Objectmaxstale** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Objectmaxage defines the maximum permissible age of a VoiceXML object for the server still to be allowed to send it to the VoiceXML-Interpreter.

Objectmaxage = 43200 seconds (12 hours)

A VoiceXML object is created by a server at 00:00. The VoiceXML-Interpreter retrieves this VoiceXML object from the server at 15:00.

Since the age of the VoiceXML object exceeds the period specified in **Objectmaxage**, the server needs to recreate the VoiceXML object before it may send it to the VoiceXML-Interpreter.

Objectmaxstale

Default:	1 000 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Objectmaxage** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Objectmaxstale defines the maximum period that may exceed the maximum age of a VoiceXML object (**Objectmaxage**) for the VoiceXML object still to be sent to the VoiceXML-Interpreter. Only when the age of the VoiceXML object exceeds the sum of **Objectmaxstale** and **Objectmaxage**, the server needs to recreate the VoiceXML object before sending it to the VoiceXML-Interpreter.

Objectmaxage = 43 200 seconds (12 hours)

Objectmaxstale = 21 600 seconds (6 hours)

A VoiceXML object is created by a server at 00:00. The VoiceXML-Interpreter retrieves this VoiceXML object from the server at 15:00.

The age of the VoiceXML object exceeds the maximum permissible age from **Objectmaxage** by 5 hours. According to **Objectmaxstale** the age may exceed the setting from **Objectmaxage** by up to 6 hours. The server may thus send the VoiceXML object to the VoiceXML-Interpreter and need not recreate it.

Scriptfetchhint

Default:	Prefetch
Possible values:	• Prefetch – scripts are loaded with document • Save – scripts are loaded if required

Defines when the VoiceXML-Interpreter loads a Java script that is referenced in the just interpreted VoiceXML document.

In case of the **Prefetch** setting the VoiceXML-Interpreter loads all Java scripts of a VoiceXML document as soon as it starts to interpret the relevant document. It is irrelevant here whether some of these Java scripts will possibly not be used at all.

In case of the **Save** setting the VoiceXML-Interpreter loads the single Java scripts of a VoiceXML document precisely at the time when the relevant Java script is to be interpreted.

Scriptmaxage

Default:	500 [Seconds]
Possible values:	<Time> [seconds]

Remark:	Is used in combination with the **Scriptmaxstale** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Scriptmaxage defines the maximum permissible age of a Java script for the server still to be allowed to send it to the VoiceXML-Interpreter.

Scriptmaxage = 43200 seconds (12 hours)

A Java script is created by a server at 00:00. The VoiceXML-Interpreter retrieves this Java script from the server at 15:00.

Since the age of the Java script exceeds the period specified in **Scriptmaxage**, the server needs to recreate the Java script before it may send it to the VoiceXML-Interpreter.

Scriptmaxstale

Default:	1 000 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Scriptmaxage** setting.

When the VoiceXML-Interpreter loads a resource from a server, this resource on the relevant server may probably not be older than is specified. If the resource age exceeds the specified period, the server needs to recreate the resource before it may send it to the VoiceXML-Interpreter.

Scriptmaxstale defines the maximum period that may exceed the maximum age of a Java script (**Scriptmaxage**) for the Java script still to be sent to the VoiceXML-Interpreter. Only when the age of the Java script exceeds the sum of **Scriptmaxstale** and **Scriptmaxage**, the server needs to recreate the Java script before sending it to the VoiceXML-Interpreter.

Scriptmaxage = 43 200 seconds (12 hours)

Scriptmaxstale = 21 600 seconds (6 hours)

A Java script is created by a server at 00:00. The VoiceXML-Interpreter retrieves this Java script from the server at 15:00.

The age of the Java script exceeds the maximum permissible age from **Scriptmaxage** by 5 hours. According to **Scriptmaxstale** the age may exceed the setting from **Scriptmaxage** by up to 6 hours. The server may thus send the Java script to the VoiceXML-Interpreter and need not recreate it.

Fetchaudio

Default:	–
Possible values:	<URI of a sound file>
Remark:	Is used in connection with the following settings: • **Fetchaudiodelay** • **Fetchaudiominimum**

Defines the URI of a sound file. This sound file is played as announcement of music-on-hold while the VoiceXML-Interpreter loads resources and the user waits for further system outputs.

If no URI is specified, no announcement or music-on-hold is played during the loading process.

Fetchaudiodelay

Default:	2 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in connection with the following settings: • **Fetchaudio** • **Fetchaudiominimum**

Defines a period for delaying the start of the announcement or music-on-hold playback. This prevents announcements or music-on-hold from being started and immediately stopped again in case of short loading periods.

Fetchaudiominimum

Default:	5 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in connection with the following settings: • **Fetchaudio** • **Fetchaudiodelay**

Defines the minimum playback time for the announcement or music-on-hold once it has been started. This time also applies even if all required resources have been loaded in the meantime.

15.2.14.3 Speech Recognizer Settings of the VoiceXML-Interpreter

Invocation in the Common Management Platform:
[Provider] VoiceXML-Interpreter > Speech Recognizer tab

NOTICE:

You find further information about these settings in the W3C standard with the title Voice Extensible Markup Language (VoiceXML) Version 2.0 or Voice Extensible Markup Language (VoiceXML) Version 2.1.

These settings control the default behavior of the VoiceXML-Interpreter for speech recognition. The speech recognition as such is executed by an ASR system, which needs to be connected to the OpenScape Media Server for this purpose.

In addition to these settings, the **Timeout** prompt setting controls the speech recognition default behavior.

Confidencelevel

Default:	0,5
Possible values:	<0…1>

Defines the threshold for the recognition reliability of a voice prompt. If the recoginition reliability of the ASR system falls short of this threshold, the voice prompt is considered not recognized.

Setting **1** corresponds to a recognition reliability of 100 %.

Sensitivity

Default:	0,5
Possible values:	<0…1>

Defines the sensitivity with which the ASR system reacts to voice entries.

In case of setting **1** the ASR system is most sensitive and reacts to entries made in a low voice also.

Speed vs accuracy

Default:	0,5
Possible values:	<0…1>

Recognizing a voice prompt is always a matter of balancing speed and accuracy. If a prompt must be recognized fast, the recognition may be relatively inaccurate; if more time is available, a more precise result may be achieved.

Speed vs accuracy defines the ratio of the speed and accuracy parameters applied by the ASR system to speech recognition.

In case of setting **0** the ASR system puts the emphasis on speed, with setting **1**, accuracy is more important.

Completetimeout

Default:	0,3 [Seconds]
Possible values:	<Time> [seconds]
Remark:	The value for **Incompletetimeout** should be greater than the one for **Completetimeout**. This gives the user time for short pauses and breathing space.

Defines the period that the ASR system waits after a voice entry before it internally transfers the result of the speech recognition. The ASR system only starts this period if it recognizes the voice entry as valid prompt and any further voice entry does not match other commands.

A great value for **Completetimeout** delays the internal result transfer by the ASR system, thus slowing down the system reaction to voice prompts.

Incompletetimeout

Default:	1 [Seconds]
Possible values:	<Time> [seconds]

Remark:	The value for **Incompletetimeout** should be greater than the one for **Completetimeout**. This gives the user time for short pauses and breathing space.

Defines the period that the ASR system waits after a voice entry before it internally transfers the result of the speech recognition. The ASR system starts this period in two cases:

- The ASR system has not yet recognized a valid command in the voice entry
- The ASR system has recognized a valid command in the voice entry, but further voice entries may match another command.

A great value for **Incompletetimeout** delays the internal result transfer by the ASR system, thus slowing down the system reaction to voice prompts. A small value, however, may lead to voice prompts not being recognized completely.

Maxspeechtimeout

Default:	30 [seconds]
Possible values:	<Time> [seconds]

Defines the maximum permissible length of a voice entry.

15.2.14.4 DTMF Recognizer Settings of the VoiceXML-Interpreter

Invocation in the Common Management Platform:
[Provider] VoiceXML-Interpreter > DTMF Recognizer tab

NOTICE:

You find further information about these settings in the W3C standard with the title Voice Extensible Markup Language (VoiceXML) Version 2.0 or Voice Extensible Markup Language (VoiceXML) Version 2.1.

These settings control the default behavior of the VoiceXML-Interpreter for DTMF recognition. The DTMF recognition as such is executed by other components of the OpenScape Media Server.

In addition to these settings, the **Timeout** prompt setting controls the DTMF recognition default behavior.

Interdigittimeout

Default:	2 [Seconds]
Possible values:	<Time> [seconds]

Defines the period in which the user needs to enter the next digit. If the DTMF recognition of the OpenScape Media Server does not receive the next DTMF signal within this period, it aborts the entry process and transfers the result of the DTMF recognition internally.

Termtimeout

Default:	0 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in combination with the **Termchar** setting.

Defines the period that the DTMF recognition of the OpenScape Media Server waits for the entry that signals the prompt end (cf. **Termchar**). This period is only started if a valid command was recognized in the DTMF entry of the user and any further DTMF entry does not match another command.

If the DTMF recognition of the OpenScape Media Server does not receive the entry that signals the prompt end within this period, it aborts the entry process and transfers the result of the DTMF recognition internally.

Termchar

Default:	#
Possible values:	<character on a telephone key>
Remark:	Is used in combination with the **Termtimeout** setting.

Defines the entry that signals the prompt end. Users can deploy the corresponding character to accelerate the completion of a DTMF entry if a value greater than zero is configured for **Termtimeout**.

If the DTMF recognition of the OpenScape Media Server receives this character, it aborts the entry process and transfers the result of the DTMF recognition internally.

15.2.14.5 Miscellaneous Settings of the VoiceXML-Interpreter

Invocation in the Common Management Platform:
[Provider] VoiceXML-Interpreter > Miscellaneous tab

NOTICE:

You find further information about these settings in the W3C standard with the title Voice Extensible Markup Language (VoiceXML) Version 2.0 or Voice Extensible Markup Language (VoiceXML) Version 2.1.

A variety of further VoiceXML-Interpreter settings exists in this area.

Inputmodes

Default:	DTMF and voice
Possible values:	• Only DTMF • Only voice • DTMF and voice

Remark:	The set input modes must be supported by the recognition software used.

Defines the input modes to be allowed by the VoiceXML-Interpreter.

Universals

Default:	None
Possible values:	<blank-separated list of grammar names>
Remark:	Do not change this setting.

Defines the names of default grammars provided by the ASR system used. They should always also be deployed for evaluating voice entries.

When integrating default grammars of the ASR system, ensure that the application can process hits of this type.

Maxn#best

Default:	1
Possible values:	<whole number>
Remark:	Do not change this setting.

A voice entry may lead to several valid commands based on different grammars.

Maxn-best defines how many of such hits are returned by the ASR system. If a number greater than one is set, ensure that the application can process multiple hits.

15.2.14.6 Media Server Settings of the VoiceXML-Interpreter

Invocation in the Common Management Platform:
[Provider] VoiceXML-Interpreter > Media Server tab

This area contains various VoiceXML-Interpreter settings that individually concern the OpenScape Media Server.

Transferoriginator

Default:	–
Possible values:	<subscriber number in the connected PBX>
Remark:	In this field only digits and a leading + character are permitted.

Applications can forward communication connections via the VoiceXML browser of the OpenScape Media Server.

Transferoriginator defines a phone number used as originator number for such a forwarding. If no phone number has been specified in **Transferoriginator**, the originator number of the forwarded call is used as originator number.

Billingnumber

Default:	–
Possible values:	<Calling number>
Remark:	In this field only digits and a leading + character are permitted.

Applications can forward communication connections via the VoiceXML browser of the OpenScape Media Server.

Billingnumber defines the phone number of an OpenScape Voice subscriber who is assigned the incurred connection charges in OpenScape Voice.

SSMLwithnamespace

Default:	<deactivated>
Possible values:	<activated> – tags contain namespace identifiers <deactivated> – tags do not contain namespace identifiers

Defines whether SSML tags contain the complete namespace identifier when the VoiceXML-Interpreter sends them to the TTS engine.

Localaudio

Default:	<deactivated>
Possible values:	<activated> – Media Server plays announcement files <deactivated> – TTS system plays announcement files

The TTS system plays announcement files as well as TTS announcements by default. Alternatively, TTS announcements can be played by the TTS system and announcement files can be played by the OpenScape Media Server.

Localaudio defines, which component plays announcement files.

This setting is particularly important if only prerecorded and no TTS announcements are played with the OpenScape Media Server. If **Localaudio** is active in this case, the OpenScape Media Server does not need a TTS system for playing announcement files.

15.3 Terminal Settings in the Common Management Platform

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Terminals tab**

The **Terminals** tab displays all terminals configured in the OpenScape Media Server. For each terminal the following associated information is displayed:

- **Terminal**

  Shows the ID of the relevant terminal. When you click on a terminal's ID you reach a dialog for configuring the relevant terminal.
- **Applet**

  Displays the application assigned to the terminal. In case of voice portal applications the associated application profile of the voice portal is displayed.

Furthermore, the **Terminals** tab contains the following buttons:

- **Edit**

  Opens a dialog in which you can edit the settings of the terminal selected in the terminal list.
- **Remove**

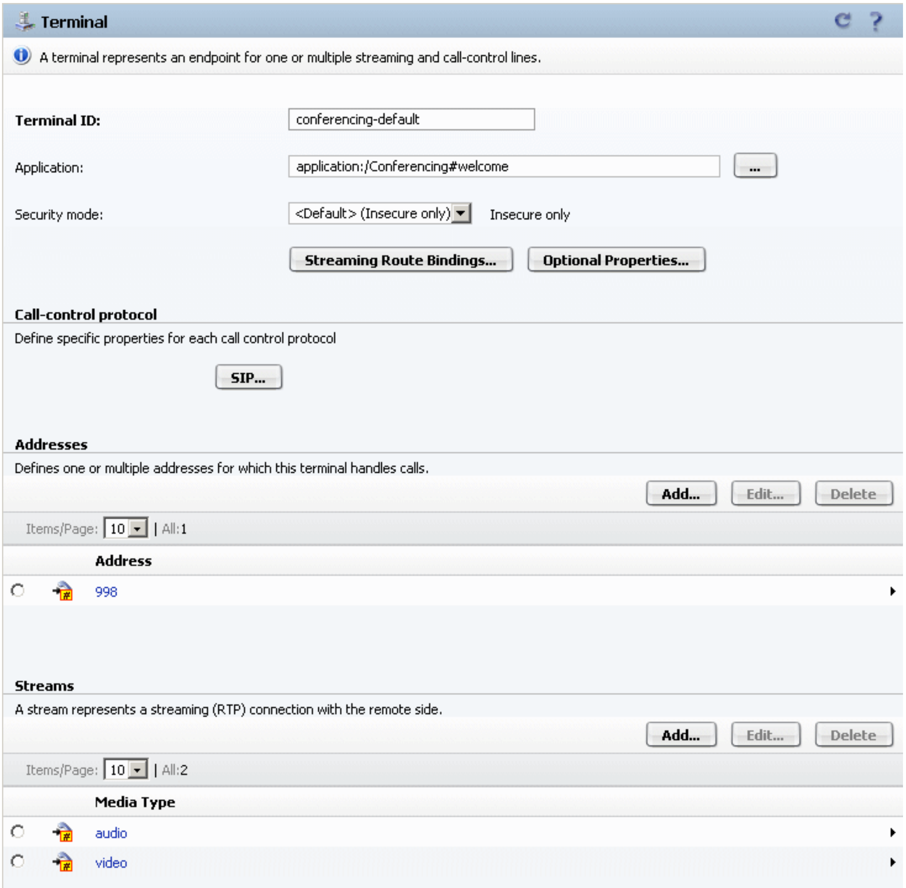
  Deletes the terminal selected in the terminal list.
- **Add**

  Opens a configuration dialog in which you can create a new terminal.

15.3.1 Editing a Terminal

Invocation in the Common Management Platform:
[Terminals] Add/ Edit

In this dialog you specify the settings of a terminal.



- **Terminal ID**

  Specifies the unique terminal name.

  Under this name the terminal is administered in the Common Management Platform.
- **Application**

  Defines the application connected to the relevant terminal. In case of voice portal applications this is a voice portal application profile.
- **Security mode**

  Specifies which security settings the relevant terminal uses respectively prefers for the communication.

IMPORTANT:

Using SRTP with MIKEY requires the system time of all systems involved in the SRTP communication to be synchronized – OpenScape Media Server, RTP-based devices (e. g. phone), VoIP gateway etc. The Network Time Protocol (NTP) may be used for this purpose.

The possible settings have the following meaning.

– **Secure only**

  A connection is only set up if the communications system and the RTP terminal device can use encrypted RTP communication (SRTP with MIKEY or SDES).

  IMPORTANT:

  The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

– **Insecure only**

  A connection is only set up if the communications system and the RTP terminal device can use an unencrypted RTP communication.

  In case encrypted and unencrypted RTP communication is offered, unencrypted RTP communication is selected. A connection is not set up only if the terminal device offers exclusively encrypted RTP communication.

– **Secure preferred**

  If the communications system and the RTP terminal device can use encrypted RTP communication (SRTP with MIKEY or SDES), the OpenScape Media Server uses this type of communication.

  If the communications system and the RTP terminal can only use an unencrypted RTP communication, the RTP connection is set up unencrypted.

  IMPORTANT:

  The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

– **Default (<current default value>)**

  Activates for the terminal the setting for **Security mode** valid across the system as it is configured in the Streaming-IVR provider.

Default:	Applying system-wide setting
Possible values:	– Secure only – Insecure only – Secure preferred – Default (<current default value>)

- **Call-control protocol**

  In this section you can perform terminal settings for protocols that the terminal can use for signalling communication connections. For the time being, the following SIP protocol settings are available:

  – **Billing address**

    Applications can establish outgoing communication connections via the OpenScape Media Server. Under **Billing address** you can specify for the terminal the phone number of an OpenScape Voice subscriber who is assigned the incurred connection charges in OpenScape Voice.

    In this field only digits and a leading + character are permitted.

    NOTICE:

    This setting refers to SIP-based communication connections only and is not effective for an MGCP-related terminal.

  – **Outbound line**

    Specifies the SIP server line used by the relevant terminal for connection signaling.

    NOTICE:

    This setting refers to SIP-based communication connections only and is not effective for an MGCP-related terminal.

- **Streaming Route Bindings...**

  Opens a dialog in which you can configure streaming route bindings specific to a terminal.

  A streaming route binding specifies which streaming route the OpenScape Media Server uses to transmit connection payloads when the associated connection signaling is handled via a specific listening point.

  NOTICE: Terminal-specific streaming route bindings have a higher priority than those valid across the system that you may have configured in the Streaming-IVR provider.

- **Optional Properties**

  Opens a dialog in which you can edit the generic properties that are transferred to the assigned **Application** for the individual terminal. You can use the **Add**, **Edit** and **Delete** buttons for this purpose.

  NOTICE:

  The expert parameters of the conference portal can be used as generic properties, for example.

  You find information about the expert parameters of the conference portal in the manual *OpenScape UCApplication, Configuration and Administration*.

- **<Addresses list >**

  Shows all addresses for which the terminal processes incoming connection requests and transfers to the associated application.

  To select the relevant address, enable the radio button that precedes the associated list entry. You can then edit the settings of the selected address or remove the address.
- **Edit (under Addresses)**

  Opens a dialog in which you can edit the settings of the selected address.
- **Delete (under Addresses)**

  Removes the selected address from the OpenScape Media Server configuration.
- **Add (under Addresses)**

  Opens a configuration dialog in which you can create a new address under which the terminal and thus the associated application is to be available.
- **<list of data streams >**

  Displays all RTP data streams configured for the terminal.

  To select the relevant RTP data stream, enable the radio button that precedes the associated list entry. You can then edit the configuration of the selected RTP data stream or remove the selected RTP data stream.
- **Edit (under Streams)**

  Opens a dialog in which you can edit the settings of the selected RTP stream configuration.
- **Delete (under Streams)**

  Removes the selected RTP data stream from the OpenScape Media Server configuration.
- **Add (under Streams)**

  Opens a configuration dialog in which you can configure a new RTP data stream.

NOTICE:

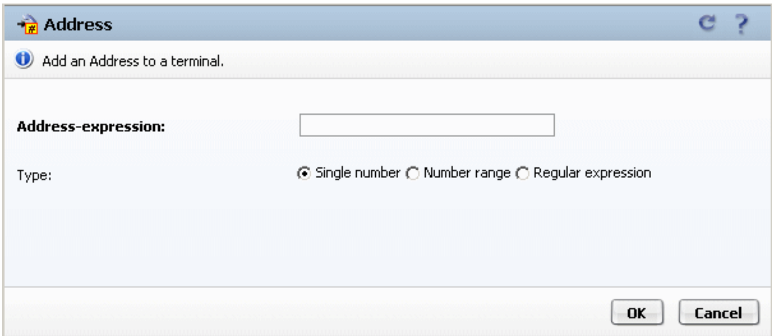
Not more than one RTP data stream per media type can be configured in each terminal.

15.3.2 Address Settings

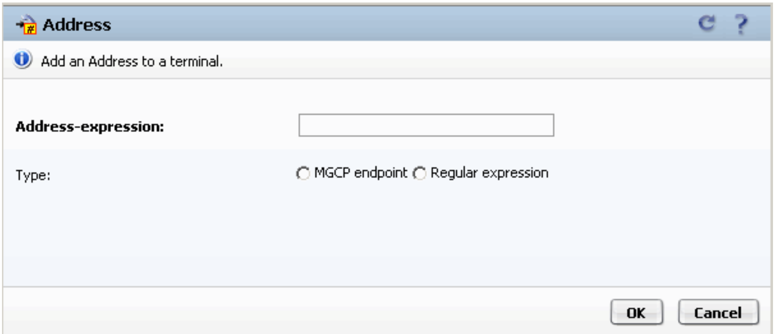
Invocation in the Common Management Platform:
[Terminals] Add / Edit > **Add / Edit (Address)**

In this dialog you define the setting of an address under which you can reach the associated terminal for inbound SIP connections.

Address dialog for SIP-based terminals:



Address dialog for MGCP-based terminals:



- **Address-expression**

  Defines the address under which you can reach the relevant terminal.

  Depending on the setting in the **Type** field the address expression may have various formats.

  If you want to specify several phone numbers that cannot be constituted in the form of a single phone number expression, you need to create at least one more address binding with the same terminal ID.

  NOTICE:

  Always specify the phone numbers in the normalized phone number format – e. g. +492404901100.

  NOTICE:

  You need to ensure that the phone numbers configured here are routed on the SIP trunk to the OpenScape Media Server in the communications system.

- **Type**

Default:	Single number (SIP) MGCP endpoint (MGCP)

Possible values:	Single number (SIP) Number range (SIP) Regular expression (SIP, MGCP) MGCP endpoint (MGCP)

Defines in which format the address specified in **Address-expression** is to be interpreted by the OpenScape Media Server.

1) Single number

Example: +492404901100

With this type the address expression may only contain a single address. The address expression may consist of:

– A fully qualified address URI
– The complete user portion of an address URI.

Consequently, the following address expressions, for example, are not allowed.

– wrong: +4924049011*
– wrong: SIP : +492404901100

If you want to assign several single phone numbers to an application, you need to create an individual address binding for each phone number. You cannot line up in a row several phone number expressions.

NOTICE:

An address expression of this type is not prefixed with a binding schema in the address binding list.

NOTICE:

This address type exists for addresses of SIP-based terminals only.

2) Number range

Example: +492404901 – +492404909

With this type you can specify the address expression as coherent address range. The addresses that you specify as start and end of the range may only consist of the complete user portion of an address URI.

Consequently, the following address expressions, for example, are not allowed.

– wrong: SIP : +492404901@.* – SIP:+492404909@.*
– wrong: SIP : +4924049010@comp.com – SIP: +4924049019@comp.com

The correct example expression comprises the phone numbers +4924049010 to +4924049019 independent from the phone number schema used or from the domain.

If you want to assign several incoherent phone number ranges to an application, you need to create an individual address binding for each coherent phone number range. You cannot line up several address expressions in a row.

NOTICE:

An address expression of this type is prefixed with the **range:** binding schema in the address binding list.

NOTICE:

This address type exists for addresses of SIP-based terminals only.

3) Regular expression

SIP example: SIP : +4924049010.@company.*

MGCP example: mgcp:ann/[1,30]

With this type you can define the address expression as regular expression.

The SIP example expression comprises the phone numbers +49240490100 to +49240490109 with the calling number schema SIP and all domains that begin with string company.

The MGCP example expression comprises the MGCP announcement addresses 1 to 30.

If you want to assign addresses to an application by several regular expressions, you need to create an individual address binding for each regular expression. You cannot line up several address expressions in a row.

NOTICE:

An address expression of this type is prefixed with the **regexp:** binding schema in the address binding list.

4) MGCP endpoint

Example: ann/*@*

NOTICE:

An address expression of this type is prefixed with the **mgcp:** binding schema in the address binding list.

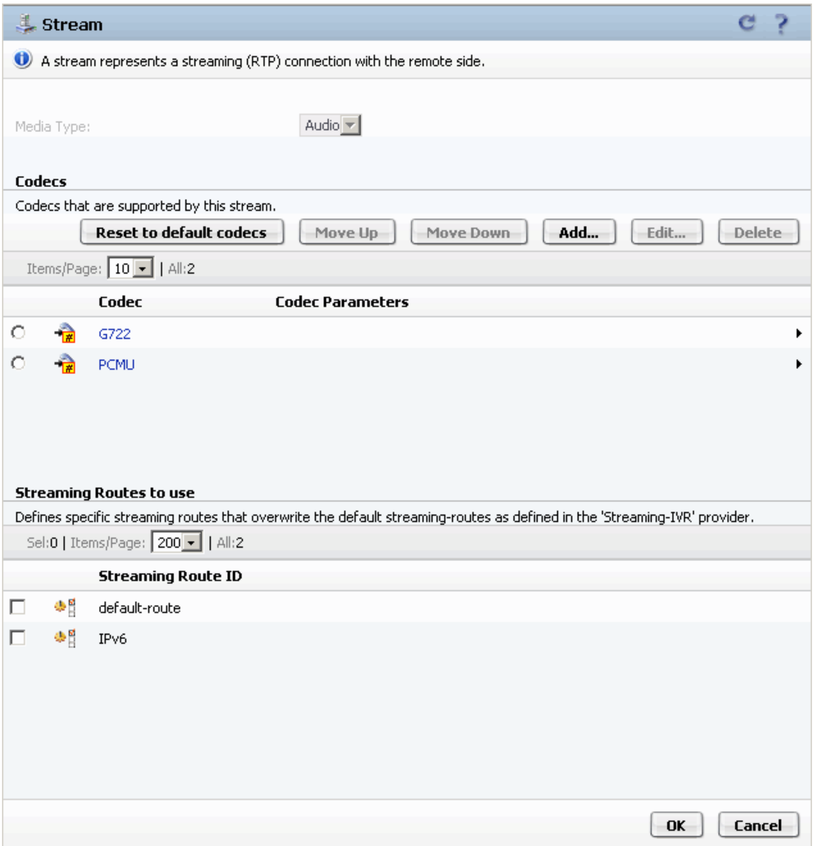
NOTICE:

This address type exists for addresses of MGCP-based terminals only.

15.3.3 Editing an RTP Data Stream

Invocation in the Common Management Platform:
[Terminals] Add / Edit > **Add / Edit (Streams)**

In this dialog you specify the settings of an RTP data stream.



- **Media Type**

  Specifies the media type for which the relevant RTP data stream is to be used.

  NOTICE:

  Only one RTP data stream can be configured for each media type.

- **<Codecs list >**

  Displays all codecs that can be used for the relevant RTP data stream. The display order conforms with the priority with which a codec is to be used. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

If you do not have configured any individual codec settings for a data stream, the codec settings valid across the system are displayed here. You administer settings valid across the system in the Streaming-IVR provider.

If you have performed individual codec settings, you can mark one of the list entries by selecting the radio button that precedes the respective list entry. You can then edit the settings of the relevant codec or delete the selected codec for the relevant data stream.

You can assign only those codecs to a data stream that correspond to the media type of the data stream. For example, only audio codecs can be assigned to an audio data stream.

The OpenScape Media Server can use the following codecs:

Media Type	Codec	Performance Factor [63]	Voice Quality	Use
Audio	G.711A	1	ISDN quality	Default PCM transmission with A-Law for volume compression. Mainly used in Europe.
	G.711µ	1	ISDN quality	Default PCM transmission with µ-Law for volume compression. Mainly used in North America and Japan.
	G.722	2	good	ISDN broadband codec with better voice quality than G.711
	G.729	3	rather poor	Compressed voice transmission with speech pause suppression.
	G722.1 (Polycom Siren 7)[64]	-	high (mono)	All media-applications for a better user experience especially during Video-Conference Calls
	G722.1 Appendix C (Polycom Siren 14)[65]	-	high (wideband)	All media-applications for a better user experience especially during Video-Conference Calls
	Telephone-event	low	–	Recognition of outband DTMF (RFC 2833)

63 The higher the performance factor, the more computing power the OpenScape Media Server needs to expend for the codec.

64 Royalty free offered by Polycom

65 Royalty free offered by Polycom

Media Type	Codec	Performance Factor [63]	Voice Quality	Use
Video	H.264	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4 / AVC.
Video	H.265	Playback: 4 Transcoding: up to 80	–	General video codec with high compression. Corresponds to MPEG-4/AVC.

NOTICE:

Using a codec that requires increased computing power reduces the number of channels the OpenScape Media Server supports in parallel.

- **Define terminal specific codecs**

  If no individual codec settings have been performed for the data stream, you can deactivate codec settings valid across the system via **Reset to default codecs** and configure individual ones.

  NOTICE:

  This button is only active if no individual codec settings have been configured for the data stream.

- **Reset to default codecs**

  If you have configured individual codec settings for the data stream, you can delete them via **Reset to default codecs**. In this case, codec settings valid across the system are displayed and activated for the data stream again.

  NOTICE:

  This button is only active if individual codec settings have been configured for the data stream.

- **Move Up**

  Moves the selected codec up by one row in the codec list. This increases the priority with which the relevant codec is used.

  NOTICE:

  This button is only active if individual codec settings have been configured for the data stream.

63 The higher the performance factor, the more computing power the OpenScape Media Server needs to expend for the codec.

- **Move Down**

  Moves the selected codec down by one row in the codec list. This decreases the priority with which the relevant codec is used.

  > **NOTICE:**
  >
  > This button is only active if individual codec settings have been configured for the data stream.

- **Edit**

  Opens a dialog in which you can edit the settings of the selected codec type.

  > **NOTICE:**
  >
  > This button is only active if individual codec settings have been configured for the data stream.

- **Remove**

  Deletes the selected codec for the relevant RTP data stream.

  > **NOTICE:**
  >
  > This button is only active if individual codec settings have been configured for the data stream.

- **Add**

  Opens a configuration dialog in which you can add another codec for the relevant RTP data stream.

  > **NOTICE:**
  >
  > This button is only active if individual codec settings have been configured for the data stream.

- **<List of the RTP streaming routes >**

  Displays all RTP streaming routes configured for the OpenScape Media Server.

  You assign the relevant RTP streaming route to the RTP data stream by selecting the corresponding checkbox that precedes the list entry. The OpenScape Media Server then uses the relevant RTP streaming route to exchange RTP data of the selected media type with RTP devices. You can also assign several RTP streaming routes to one RTP data stream.

  > **NOTICE:**
  >
  > You can only see the RTP streaming routes list if more than one RTP streaming route is configured in the OpenScape Media Server.

If you do not assign an RTP streaming route to an RTP data stream, the OpenScape Media Server uses an RTP streaming route defined by streaming route bindings. In this process the OpenScape Media Server prefers the definitions of terminal-specific streaming route bindings to those of global streaming route bindings configured in the Streaming-IVR provider.

15.3.4 Editing Optional Settings

Invocation in the Common Management Platform:
[Terminals] Add/Edit > **Optional Properties** > **Add/ Edit**

In this dialog you define generic properties that are transferred to a application of the OpenScape Media Server when the application is being invoked. Generic properties influence only the behavior of the application and do not serve any other purpose in the OpenScape Media Server.

NOTICE:

The expert parameters of the conference portal can be used as generic properties, for example.

You find information about the expert parameters of the conference portal in the manual *OpenScape UCApplication, Configuration and Administration*.

- **Key**

  Specifies the key of the generic property to be transferred to the application when being invoked.

  The key specifies which generic property is concerned.

  IMPORTANT:

  The OpenScape Media Server does not check a specified key for plausibility. Therefore, please be sure to write the key correctly.

- **Value**

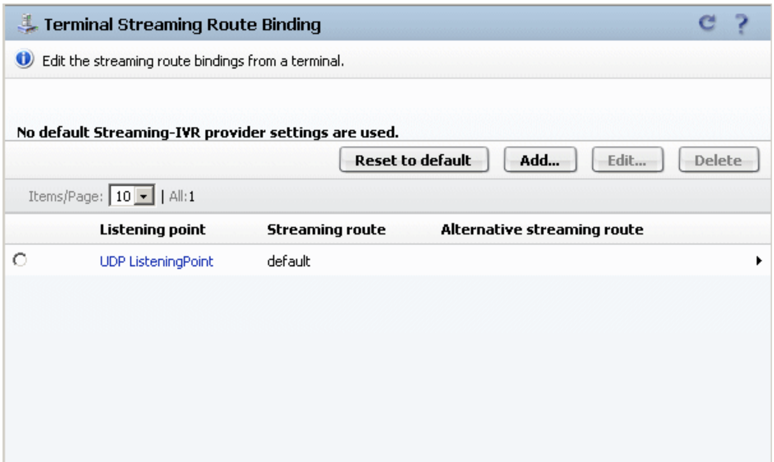
  Defines the value to be transferred to the application for the specified key.

  IMPORTANT:

  The OpenScape Media Server does not check a specified value for plausibility. Therefore, please verify that the specified value stays within the permitted value range, insofar as restrictions exist on this.

15.4 Streaming Route Binding Settings

Invocation in the Common Management Platform:
[Terminals] Add / Edit > **Streaming Route Bindings**



In this dialog you see all RTP streaming route bindings configured in the OpenScape Media Server. For each binding the following associated information is displayed:

- **Listening point**

  Defines the listening point from which the individual routing of RTP data is to depend.

  If signaling data is transmitted via this listening point, the associated RTP data is routed via the streaming route defined under **Streaming route**.

  The **(SIP) *** setting makes routing dependent from all configured SIP listening points.
- **Streaming route**

  Defines the streaming route to be used for RTP data if the associated signaling data is routed via the specified listening point.
- **Alternative streaming route**

  Defines a streaming route that the OpenScape Media Server uses as alternative streaming route for the selected listening point.

> **NOTICE:**
>
> You need to specify an alternative streaming route if the OpenScape Media Server is simultaneously connected to an IPv4- and IPv6-based network. In this case, select under **Streaming route** e. g. a route into the IPv4-based network and under **Alternative streaming route** a route into the IPv6-based network.

Furthermore, the dialog contains the following buttons:

- **Define terminal specific binding**

  If no individual streaming route bindings have been configured for the terminal, you can use the **Define terminal specific binding** button to deactivate the binding settings valid across the system and configure individual ones.

  > **NOTICE:**
  >
  > You see this button only if no individual streaming route bindings have been configured for the terminal.

- **Reset to default**

  If you have configured individual streaming route bindings for a terminal, you can delete them via **Reset to default**. In this case, streaming route bindings valid across the system are displayed and activated for the terminal again.

  > **NOTICE:**
  >
  > You see this button only if individual streaming route bindings have been configured for the terminal.

- **Edit**

  Opens a dialog in which you can edit the settings of the streaming route binding selected in the bindings list.
- **Remove**

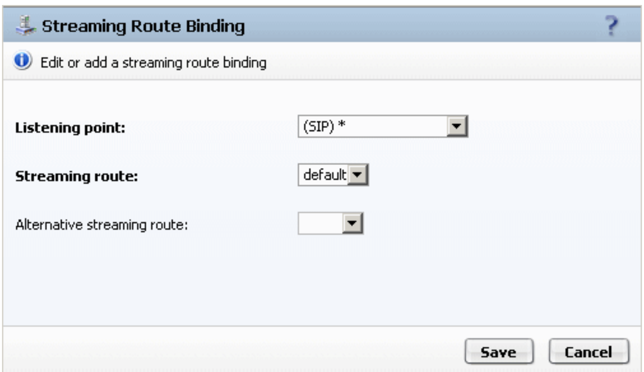
  Deletes the streaming route binding selected in the bindings list.
- **Add**

  Opens a configuration dialog in which you can create a new streaming route binding.

15.4.1 Editing a Streaming Route Binding

Invocation in the Common Management Platform:
• **[Terminals] Add / Edit** > **Streaming Route Bindings** • **[Providers] Streaming-IVR (TTS, ASR, SDP)** > **[tab] SDP** > **Add / Edit (Streaming Route Binding)**

In this dialog you specify the settings of a streaming route binding.



For each streaming route binding the following associated information is displayed:

- **Listening point**

  Defines the listening point from which the individual routing of RTP data is to depend.

  If signaling data is transmitted via this listening point, the associated RTP data is routed via the streaming route selected under **Streaming route**.

  The **(SIP) *** setting makes routing dependent from all configured SIP listening points.
- **Streaming Route**

  Defines the streaming route to be used for RTP data if the associated signaling data is routed via the specified listening point.
- **Alternative streaming route**

  Defines a streaming route that the OpenScape Media Server uses as alternative streaming route for the selected listening point.

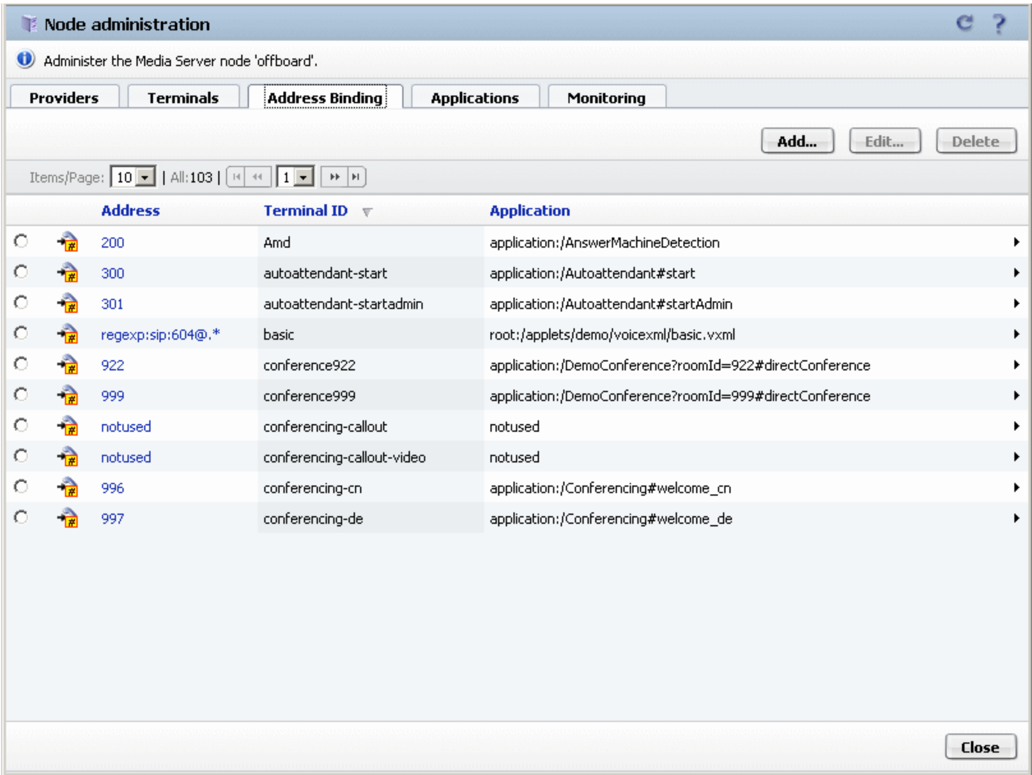
> **NOTICE:**
>
> You need to specify an alternative streaming route if the OpenScape Media Server is simultaneously connected to an IPv4- and IPv6-based network. In this case, select under **Streaming route** e. g. a route into the IPv4-based network and under **Alternative streaming route** a route into the IPv6-based network.

15.5 Address Binding Settings in the Common Management Platform

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Address Binding tab**

On the **Address Binding** tab you specify under which addresses an OpenScape Media Server application shall be available. The address bindings are solely an address-centered view of the configured terminals and their assigned application.

> **NOTICE:**
>
> Despite the address-centered view of the address bindings, addresses are always assigned to a terminal. The address bindings view is to provide a quick overview of all configured phone numbers, find an unused address and assign this address to an application.



For each address binding the following associated information is displayed:

- **Address**

  Shows the address expression that specifies the addresses of the address binding. When you click on the address of an address binding you reach a dialog for configuring the relevant address binding.
- **Terminal ID**

  Shows the ID of the terminal assigned to the address binding.
- **Application**

  Shows the applet of the application assigned to the address binding.

Furthermore, the **Address Binding** tab contains the following buttons:

- **Edit**

  Opens a dialog in which you can edit the properties of the address binding selected in the address binding list.
- **Remove**

  Deletes the address binding selected in the address binding list.
- **Add**

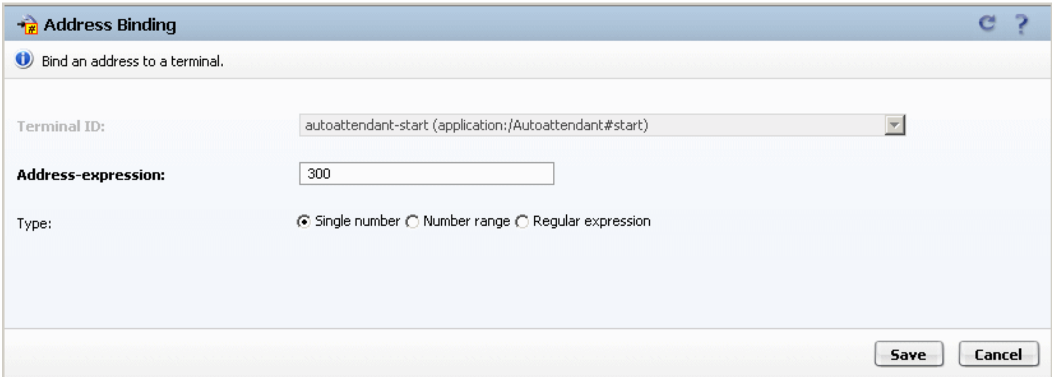
  Opens a configuration dialog in which you can create a new address binding.

15.5.1 Editing an Address Binding

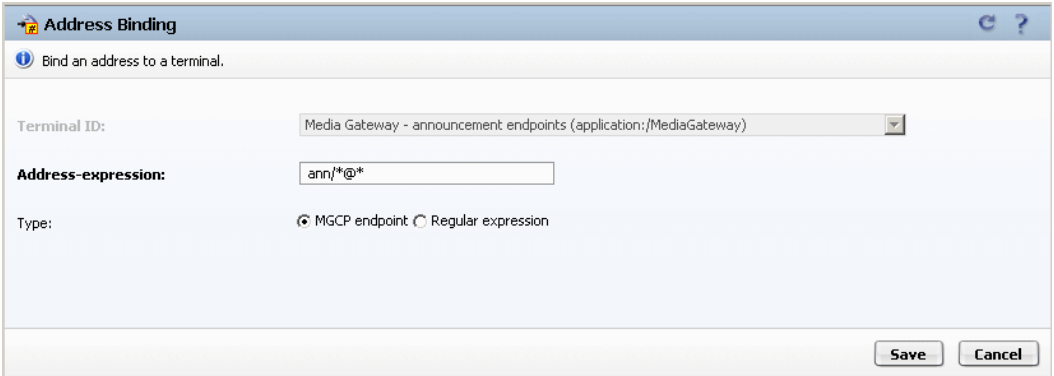
Invocation in the Common Management Platform:
• **[Address Bindings] Add/ Edit** • **[Terminals] Add/ Edit> Add / Edit (Addresses)**

In this dialog you specify the settings of an address binding.

Address binding dialog for SIP-based address bindings:



Address binding dialog for MGCP-based address bindings:



- **Terminal ID**

  Specifies the terminal of the relevant address binding.
- **Address-expression**

  Defines the address under which the application of the specified terminal is available.

  Depending on the setting in the **Type** field the address expression may have various formats.

  If you want to specify several phone numbers that cannot be constituted in the form of a single phone number expression, you need to create at least one more address binding with the same terminal ID.

  NOTICE:

  Always specify the phone numbers in the normalized phone number format – e. g. +492404901100.

  NOTICE:

  You need to ensure that the phone numbers configured here are routed on the SIP trunk to the OpenScape Media Server in the communications system.

- **Type**

Default:	Single number (SIP) MGCP endpoint (MGCP)

Possible values:	Single number (SIP) Number range (SIP) Regular expression (SIP, MGCP) MGCP endpoint (MGCP)

Defines in which format the address specified in **Address-expression** is to be interpreted by the OpenScape Media Server.

1) Single number

Example: +492404901100

With this type the address expression may only contain a single address. The address expression may consist of:

– A fully qualified address URI
– The complete user portion of an address URI.

Consequently, the following address expressions, for example, are not allowed.

– wrong: +4924049011*
– wrong: SIP : +492404901100

If you want to assign several single phone numbers to an application, you need to create an individual address binding for each phone number. You cannot line up in a row several phone number expressions.

NOTICE:

An address expression of this type is not prefixed with a binding schema in the address binding list.

NOTICE:

This address type exists for addresses of SIP-based terminals only.

2) Number range

Example: +4924049010 – +4924049019

With this type you can specify the address expression as coherent address range. The addresses that you specify as start and end of the range may only consist of the complete user portion of an address URI.

Consequently, the following address expressions, for example, are not allowed.

– wrong: SIP : +4924049010@.* – SIP:+4924049019@.*
– wrong: SIP : +4924049010@comp.com – SIP: +4924049019@comp.com

The correct example expression comprises the phone numbers +4924049010 to +4924049019 independent from the phone number schema used or from the domain.

If you want to assign several incoherent phone number ranges to an application, you need to create an individual address binding for each coherent phone number range. You cannot line up several address expressions in a row.

> **NOTICE:**
>
> An address expression of this type is prefixed with the **range:** binding schema in the address binding list.

> **NOTICE:**
>
> This address type exists for addresses of SIP-based terminals only.

3) Regular expression

SIP example: SIP : +4924049010.@company.*

MGCP example: mgcp:ann/[1,30]

With this type you can define the address expression as regular expression.

The SIP example expression comprises the phone numbers +49240490100 to +49240490109 with the calling number schema SIP and all domains that begin with string company.

The MGCP example expression comprises the MGCP announcement addresses 1 to 30.

If you want to assign addresses to an application by several regular expressions, you need to create an individual address binding for each regular expression. You cannot line up several address expressions in a row.

> **NOTICE:**
>
> An address expression of this type is prefixed with the **regexp:** binding schema in the address binding list.

4) MGCP endpoint

Example: ann/*@*

> **NOTICE:**
>
> An address expression of this type is prefixed with the **mgcp:** binding schema in the address binding list.

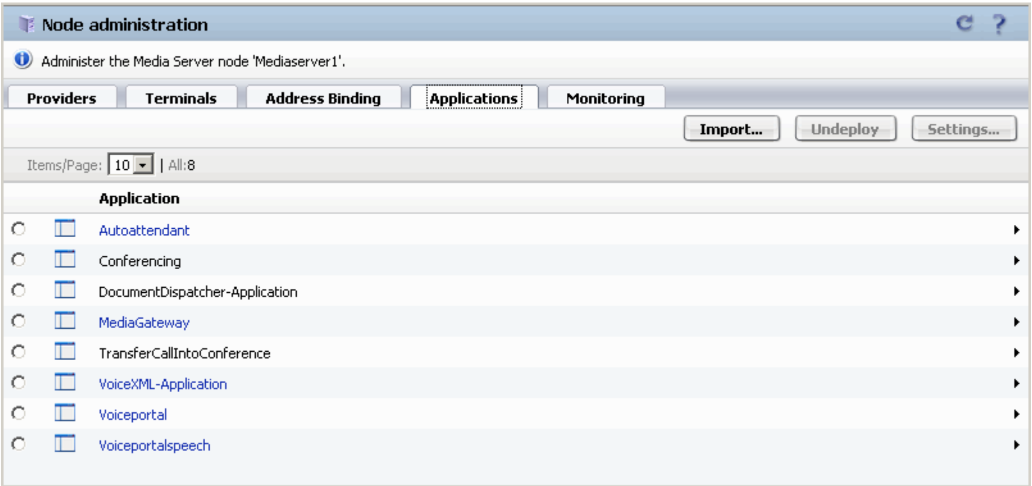
> **NOTICE:**
>
> This address type exists for addresses of MGCP-based terminals only.

15.6 Application Settings in the Common Management Platform

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Applications tab**

The **Applications** tab shows a list of all applications used by the OpenScape Media Server.

When you click on the name of an application you reach a dialog for configuring individual application settings. The structure of this configuration dialog depends on whether or not the application in question provides an individual configuration module. If the application does not provide an individual configuration module, the OpenScape Media Server displays a generic configuration dialog.



Furthermore, the **Applications** tab contains the following buttons:

- **Import**

  Opens a dialog in which you can provide deployment packages of Media Server applications for the OpenScape Media Server. For example applications created with the Application Builder.
- **Settings**

  Opens a dialog in which you can edit settings for the selected application.

  If the application does not provide an individual configuration module, the OpenScape Media Server displays a generic configuration dialog. In this dialog application settings are configured much in the same manner as the generic properties of a terminal.

15.7 Expert Settings for SIP

NOTICE:

You need to consider the SIP expert settings only if you use the OpenScape Media Server under OpenScape UCApplication.

The expert settings for the SIP are administered in the configuration file of the SIP provider.

Configuration file:	`sip-connectivity.xml`
Storage location:	/<host >`/providers/sip#connectivity.component.xml`

<host > corresponds to one of the following paths:

- `/enterprise/mediaserver/application_host`
- `/opt/siemens/mediaserver/application_host`

You can divide the settings in the configuration file of the SIP provider in two areas:

- Settings individual for SIP server lines

  Settings that apply for an individual SIP server line.
- Universal settings

  Settings that are universal and apply for all configured SIP server lines.

15.7.1 SIP Expert Settings Specific to SIP Server Lines

The configured SIP server lines are combined in the configuration file of the SIP provider by the **sipServers** tag. Every single SIP server line is labeled by the **sipServer** tab. The **id** attribute of the respective **sipServer** tag defines the ID of the associated SIP server line.

```
<sipServers>
  <sipServer id="H8K">
    <connectionPoint address='1.2.3.4' port=':5060' Transport=''UDP'/>
    <domainName>domain.org</domainName>
    <listeningPointId>UDP ListeningPoint</listeningPointId>
    <keepAliveRequestInterval>60</keepAliveRequestInterval>
    <serverAddressAlternatives>
      <connectionPoint address='1.2.3.5' port=':5060' Transport=''UDP'/
      >
      <connectionPoint address='1.2.3.6' port=':5060' Transport=''UDP'/
      >
    </serverAddressAlternatives>
    <sendByeRtpStatistics>true</sendByeRtpStatistics>
    <fallbackToMasterSipServerTime>3600</
    fallbackToMasterSipServerTime>
    <sipServerAutoDetectionEnabled>false</
    sipServerAutoDetectionEnabled>
```

```
    </sipServer>
    <sipServer id="Asterisk">
        <connectionPoint address='fdbd:ae65:79cc::31' port=':5060'
        Transport=''UDP'/>
        <listeningPointId>UDP V6 ListeningPoint</listeningPointId>
    </sipServer>
</sipServers>
```

Each of the configured SIP server lines contains the following line-individual SIP settings:

- **addressTranslationContext**

  Defines the ID of an address translation context configured in the CMP. The SIP provider uses this context to normalize and localize phone numbers for the relevant SIP server line.

Default:	–
Possible values:	<ID of a configured address translation context>
Remark:	Is configured via the Common Management Platform.

- **connectionPoint**

  Defines the connection data of an SIP server that the OpenScape Media Server uses for outbound SIP connections. The following information is given for an SIP server:

  – IP address (IPv4, IPv6) of the SIP server

    If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

  – Port to which the OpenScape Media Server sends the data for the relevant SIP server.

  – Transport protocol that the OpenScape Media Server uses for the relevant SIP server.

  The single connection data items are specified as attributes **address**, **port** and **transport** or the **connectionPoint** tag.

  The connection data specified directly within the **sipServer** tag concern the preferred SIP server (Master SIP server) of an SIP server line. Connection data specified within the **serverAddressAlternatives** tag describes the associated alternative servers.

Default:	–
Possible values:	<IPv4 address / IPv6 address / hostname> : <Port number> / <Transport protocol>
Remark:	Is configured via the Common Management Platform.

Note:	If a firewall exists between the OpenScape Media Server and OpenScape Voice, you need to activate the port configured here in this firewall.

- **domainName**

  Defines a domain name used when creating SIP addresses. If no domain name is defined, the IP address of the SIP server is used for the domain portion of SIP addresses.

Default:	–
Possible values:	<domain name >
Remark:	Optional

- **fallbackToMasterSipServerTime**

  If the Master SIP server is not operable any more, the SIP provider uses an alternative SIP server (if configured).

  fallbackToMasterSipServerTime defines a period after which the SIP provider switches back to the Master SIP server; no matter whether or not the Master SIP server is available at this time. Start time for the timer is the switch-back to the alternative SIP server.

Default:	0 [Seconds]
Possible values:	– <Time> [seconds] – 0 – deactivates the fallback mechanism

- **keepAliveRequestInterval**

  The SIP provider uses a keep-alive mechanism to check whether the preferred SIP server (Master SIP server) is still operable.

  keepAliveRequestInterval defines in which intervals the SIP provider sends keep-alive requests to the Master SIP server.

Default:	180 [Seconds]
Possible values:	– <Time> [seconds] – 0 – deactivates the Keep-Alive mechanism
Remark:	If the keep-alive mechanism is inactive, the consistency check does not test the availability of the connected SIP servers.

- **listeningPointId**

  Defines the SIP listening point the communication settings of which the OpenScape Media Server uses when it deploys the relevant SIP server line for an outgoing call.

Default:	–
Possible values:	<ID of a configured SIP listening point >
Remark:	Is configured via the Common Management Platform.

- **receiveKeypadEvents**

  Defines whether the SIP provider processes keypad events.

  When this switch is inactive, multiple recognition of a key entry can be prevented if a keystroke is simultaneously received e. g. by DTMF (RFC 2833) and keypad event.

Default:	false
Possible values:	– true – SIP provider processes keypad events – false – SIP provider does not process keypad events

- **sendByeRtpStatistics**

  Using the X-Siemens-RTP-stats-list-Header specific to the manufacturer, the OpenScape Media Server can transmit RTP statistics information within SIP-BYE messages or replies.

  sendByeRtpStatistics specifies whether RTP statistics information is transferred within SIP-BYE messages.

Default:	true
Possible values:	– true – activates the transfer specific to the manufacturer – false – deactivates the transfer specific to the manufacturer

- **serverAdressAlternatives**

  Structures the alternative SIP servers of an SIP server line.

Remark:	Exclusive structure element

- **sipServerAutoDetectionEnabled**

  The SIP provider can automatically detect SIP servers that are available in the OpenScape Media Server network environment. To do this the SIP provider uses SIP connection requests it receives from SIP servers.

  If the SIP server detection is active and the OpenScape Media Server receives a connection request from an SIP server it has not known so far, the SIP provider creates automatically a new SIP server line. The originator address of the received SIP-INVITE message is used as SIP server address; the port on which the SIP-INVITE message arrives is used as SIP listening point.

  sipServerAutoDetectionEnabled defines whether the automatic SIP server detection is active.

Default:	false
Possible values:	– true – activates the automatic SIP server detection – false – deactivates the automatic SIP server detection
Important:	If this feature is activated, unauthorized persons may access the system. Therefore SIP servers should always be statically provisioned!

15.7.2 Universal SIP Expert Settings

The configuration file of the SIP provider contains the following universal SIP settings. They apply for all configured SIP server lines.

- **connectionSupervisionTimer**

  The OpenScape Media Server can monitor the setup, clearing and duration of SIP-based connections.

  – Monitoring the connection setup

    If a connection does not reach status CONNECTED within 200 seconds after an SIP-INVITE message, the connection setup is abandoned and the connection attempt has failed.

  – Monitoring the connection clearing

    If a connection does not reach status DISCONNECTED within 60 seconds after its clearing has been initiated, it is closed automatically.

  – Monitoring the connection duration

    Every connection is cleared automatically after it existed for a fixed period.

  connectionSupervisionTimer defines the maximum duration for SIP connections. If a connection exists for this duration, it is cleared automatically.

Default:	90 000 [seconds] (corresponds to 25 hours)
Possible values:	– <Time> [seconds] – 0 – deactivates all monitoring features
Important:	Only trained service personnel may change this setting!

- **floodingCallLimit**

  The SIP provider monitors how many INVITE messages it processes at any time. Therefore it uses the respective counting mechanism.

  floodingCallLimit defines an upper threshold for this counter. When this threshold is reached, all ensuing INVITE messages are rejected until the threshold is gone below again.

Default:	20
Possible values:	– <number > – 0– deactivates the counting mechanism

- **inboundConnectionAcceptanceTimeout**

  Specifies the period within which the SIP provider expects a reply to inbound calls from internal applications. If an internal application does not answer within this period, the SIP provider transfers the incoming call to other internal, available processes or rejects it as impossible to route (SIP response “Not found”).

Default:	4 000 [ms]
Possible values:	– <Time> [ms] – 0 – deactivates the time-out mechanism

Important:	Only trained service personnel may change this setting!

- **inboundConnectionOfferTimeout**

  Defines the period within which a correct address binding must be determined for incoming calls. If no correct address binding can be determined within this period, the SIP provider transfers the incoming call to other internal, available processes or rejects it as impossible to route (SIP response “Not found”).

Default:	600 [ms]
Possible values:	– <Time> [ms] – 0 – deactivates the time-out mechanism
Important:	Only trained service personnel may change this setting!

- **keyStore**

  Specifies the name of the keystore the certificate of which is used by the OpenScape Media Server for the TLS communication.

  The specified keystore must contain a valid certificate for the OpenScape Media Server, which is signed by a root CA. The specified keystore must contain also the certificate of the used root CA.

  The keystore used must be stored in the following directory:

  `osgi/config-beans/host/providers/sip-connectivity`

Default:	tls-keystore.jks
Possible values:	<Path and file name of the keystore>
Remark:	The reference path for the setting is: osgi\config-beans\host\providers\sip-connectivity

- **keyStorePassword**

  To access the keystore configured under **keyStore**, the OpenScape Media Server uses the password *password* by default.

  If the configured keystore uses another password, you need to add the setting **keyStorePassword** in the configuration file and in it configure the password of the keystore used.

Default:	–
Possible values:	<passwort>
Remark:	Optional

- **keyStoreType**

  To access the keystore specified under **keyStore**, the OpenScape Media Server uses the keystore type *jks*.

  If the configured keystore uses another keystore type, you need to add the setting **keyStoreType** in the configuration file and in it configure the keystore type of the keystore used.

Default:	–

Possible values:	<File suffix>
Important:	Only trained service personnel may change this setting!

- **listeningPoint**

  Specifies the communication settings for the inbound OpenScape Media Server SIP connections in the form of so-called SIP listening points.

  Each SIP listening point consists of the following settings:

  – ID via which an SIP listening point can be referenced. An SIP listening point is also managed under this ID in the Common Management Platform.
  – IP address (IPv4, IPv6), via which the OpenScape Media Server communicates for the SIP listening point.

    If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.
  – Port on which the OpenScape Media Server receives the data for the relevant SIP listening point.
  – Transport protocol the OpenScape Media Server uses for the SIP listening point.

  These single settings are combined in the form of an SIP listening point:

Default:	<listeningPoint id="UDP ListeningPoint" address="auto $IPv4" port="5060" transport="UDP"/> <listeningPoint id="TCP ListeningPoint" address="auto $IPv4" port="5060" transport="TCP"/> <listeningPoint id="TLS ListeningPoint" address="auto $IPv4" port="5061" transport="TLS"/>
Possible values:	<List of single listening points>
Remark:	Is configured via the Common Management Platform. If a firewall exists between the OpenScape Media Server and OpenScape Voice, you need to activate the ports configured here in this firewall.

- **listeningPoints**

  Defines the configured SIP listening points.

Remark:	Exclusive structure element

- **maxConnectionThreads**

  Defines the maximum number of simultaneous threads that the SIP provider uses for SIP connection requests.

Default:	10
Possible values:	> 0
Important:	Only trained service personnel may change this setting!

- **mediaCallControlEnabled**

  Controls the internal manager module Media-Call-Control.

Default:	true
Possible values:	– true – false
Important:	Only trained service personnel may change this setting!

- **registrarServerEnabled**

  Controls the internal manager module that realizes an internal SIP registrar server.

Default:	false
Possible values:	– true – false
Important:	Only trained service personnel may change this setting!

- **registrationClientEnabled**

  Controls the internal manager module for registering at external SIP servers.

Default:	true
Possible values:	– true – false
Important:	Only trained service personnel may change this setting!

- **sipServerAutoDetectionEnabled**

  The SIP provider can automatically detect SIP servers that are available in the OpenScape Media Server network environment. To do this the SIP provider uses SIP connection requests it receives from SIP servers.

  If the SIP server detection is active and the OpenScape Media Server receives a connection request from an SIP server it has not known so far, the SIP provider creates automatically a new SIP server line. The originator address of the received SIP-INVITE message is used as SIP server address; the port on which the SIP-INVITE message arrives is used as SIP listening point.

  sipServerAutoDetectionEnabled defines whether the automatic SIP server detection is active.

Default:	false
Possible values:	– true – activates the automatic SIP server detection – false – deactivates the automatic SIP server detection
Important:	If this feature is activated, unauthorized persons may access the system. Therefore SIP servers should always be statically provisioned!

- **sipSessionTimerExpiration**

  Using SIP session update requests SIP user agents and SIP proxy servers can check whether their status matches for an individual connection.

Such a check is useful if an above-average number of data is lost during transmission in a transport network, so that, for example, SIP connections are preserved in the OpenScape Media Server though the communication partner has already cleared them.

Default:	0
Possible values:	– <Time> [ms] – 0 – deactivates the update mechanism
Important:	Only trained service personnel may change this setting!

- **sipStackProperties**

  Defines internal SIP stack settings.

Remark:	Exclusive structure element
Important:	Only trained service personnel may change the contained property entries!

15.8 Expert Settings for Streaming

The expert settings for streaming MFW are administered in the MFW configuration file.

Configuration file:	`mfw.component.xml`
Storage location:	/<host >`/providers/streaming-mps`

<host > corresponds to one of the following paths:

- `/enterprise/mediaserver/application_host`
- `/opt/siemens/mediaserver/application_host`

You can divide the configuration file for streaming MFW in two areas:

- Route-individual settings

  Settings that apply for an individual RTP streaming route.
- Universal settings

  Settings that are universal and apply for all configured RTP streaming routes.

15.8.1 Streaming Expert Settings Specific to Routes

The configured RTP streaming routes are combined in the configuration file of the Streaming provider by the **streamingRoutes** tag. In this process, each single RTP streaming route is labeled by the **streamingRoute** tag. The **id** attribute of the respective **streamingRoute** tag defines the ID of the associated RTP streaming route.

```
<streamingRoutes>

    <streamingRoute id="route 1">
```

```
        <ipAddress>196.178.10.17</ipAddress>
        <rtpPortRangeStart>20000</rtpPortRangeStart>
        <numRtpPorts>20000</numRtpPorts>
        <rtpTypeOfService></ rtpTypeOfService>
        <rtcpSenderreportEnabled>false</rtcpSenderreportEnabled>
        <rtcpSenderreportInterval>5</rtcpSenderreportInterval>
        <icmpMonitoringEnabled>true</icmpMonitoringEnabled>
        <icmpUnreachableCount>200</icmpUnreachableCount>
    </streamingRoute>
</streamingRoutes>
```

Each of the configured RTP streaming routes contains the following route-individual settings:

- **icmpMonitoringEnabled**

  Network components use the Internet Control Message Protocol (ICMP) to exchange diagnostics data via the internet protocol. A router may return e.g. ICMP messages to a data source if it needs to dismiss packets of this data source.

  icmpMonitoringEnabled specifies whether or not the ICMP monitoring of the OpenScape Media Server is active.

  When the ICMP monitoring of the OpenScape Media Server is active, the OpenScape Media Server reacts to ICMP messages that it receives from the network. If the number of received ICMP messages exceeds a threshold, the Media Server sends appropriate messages to its applications. The applications can react to this by temporarily stopping or reducing the send activities.

  The described threshold is determined by **icmpUnreachableCount**.

Default:	false
Possible values:	– true – activates the ICMP monitoring – false – deactivates the ICMP monitoring
Remark:	Is used in connection with the following setting: – **icmpUnreachableCount** – **icmpRecoveryTime**

- **icmpUnreachableCount**

  When the ICMP monitoring of the OpenScape Media Server is active (**icmpMonitoringEnabled** = true), the OpenScape Media Server reacts to ICMP messages that it receives from the network. If the number of received ICMP messages exceeds a threshold, the Media Server sends appropriate messages to its applications. The applications can react to this by temporarily stopping or reducing the send activities.

icmpUnreachableCount defines the amount of the described threshold. The counter for this threshold is reset after a period defined by **icmpRecoveryTime**.

Default:	200
Possible values:	<Number>
Remark:	Is used in connection with the following setting: – **icmpMonitoringEnabled** – **icmpRecoveryTime**

- **ipAddress**

  Defines the IP address (IPv4, IPv6) that the OpenScape Media Server uses on the local computer system for the RTP communication via the relevant RTP streaming route.

  If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

Remark	Is configured via the Common Management Platform.

- **numRtpPorts**

  Defines the maximum number of UDP ports that the OpenScape Media Server uses for the RTP-based communication via the relevant RTP streaming route.

Remark:	Is configured via the Common Management Platform.

- **rtpPortRangeStart**

  Defines the first UDP port of the port range that the OpenScape Media Server uses for the RTP-based communication via the relevant RTP streaming route.

Remark:	Is configured via the Common Management Platform.

- **rtcpSenderreportEnabled**

  Defines whether the Media Server sends RTCP originator reports in specific intervals via the relevant RTP streaming route and receives RTCP originator / receiver reports.

  The interval for sending RTCP originator reports is defined by **rtcpSenderreportInterval**.

Remark:	Is configured via the Common Management Platform. Is used in connection with the **rtcpSenderreportInterval** setting.

- **rtcpSenderreportInterval**

  Defines the interval in which the OpenScape Media Server sends RTCP originator reports via the relevant RTP streaming route.

  Before the interval becomes effective, RTCP must be activated for the relevant RTP streaming route via **rtcpSenderreportEnabled**.

Default:	5 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in connection with the **rtcpSenderreportEnabled** setting.

- **rtpTypeOfService**

  Defines the quality of service (DSCP) used for the RTP communication between OpenScape Media Server and RTP-based devices via the relevant RTP streaming route.

Remark:	Is configured via the Common Management Platform.

Table 10: Assignment of codepoint setting and quality of service

Setting	Quality of service according to Common Management Platform
0	Standard (CS0)
1 – 7	Experimental code points
8	Precedence 1 (CS1)
9	Experimental code point
10	Assured Forwarding Class 1, Low Drop Precedence (AF11)
11	Experimental code point
12	Assured Forwarding Class 1, Medium Drop Precedence (AF12)
13	Experimental code point
14	Assured Forwarding Class 1, High Drop Precedence (AF13)
15	Experimental code point
16	Precedence 2 (CS2)
17	Experimental code point
18	Assured Forwarding Class 2, Low Drop Precedence (AF21)
19	Experimental code point

Setting	Quality of service according to Common Management Platform
20	Assured Forwarding Class 2, Medium Drop Precedence (AF22)
21	Experimental code point
22	Assured Forwarding Class 2, High Drop Precedence (AF23)
23	Experimental code point
24	Precedence 3 (CS3)
25	Experimental code point
26	Assured Forwarding Class 3, Low Drop Precedence (AF31)
27	Experimental code point
28	Assured Forwarding Class 3, Medium Drop Precedence (AF32)
29	Experimental code point
30	Assured Forwarding Class 3, High Drop Precedence (AF33)
31	Experimental code point
32	Precedence 4 (CS4)
33	Experimental code point
34	Assured Forwarding Class 4, Low Drop Precedence (AF41)
35	Experimental code point
36	Assured Forwarding Class 4, Medium Drop Precedence (AF42)
37	Experimental code point
38	Assured Forwarding Class 4, High Drop Precedence (AF43)
39	Experimental code point
40	Precedence 5 (CS5)
41 – 45	Experimental code points
46	Expedited Forwarding (EF)
47	Experimental code point
48	Precedence 6 (CS6)

Setting	Quality of service according to Common Management Platform
49 – 55	Experimental code points
56	Precedence 7 (CS7)
57 – 63	Experimental code points

- **videoEncoderIFrameCreationInterval**

  A video encoder inserts regulary single key frames or intra frames in a video stream to group the ensuing video images up to the next key frame for processing.

  A key frame is a fully described still and serves as reference for the assigned video images in which only reference specifications and motion vectors are then stored with reference to the key frame.

  The more often a key frame is inserted in the video stream, the more the playback quality of the video improves. However, key frames contain considerably more data than the other video images, thus increasing bandwidth requirements for video streaming.

  videoEncoderIFrameCreationInterval specifies the interval after which the video encoder inserts a key frame in the video stream if it has not been inserted in another way until then.

Default:	30 [seconds]
Possible values:	– <Time> [seconds] – 0 – Deactivates the insertion mechanism of the video encoder
Remark:	Is used in connection with the **rtcpSenderreportEnabled** setting.

- **videoEncoderPerformance**

  Specifies whether the video encoder of the OpenScape Media Server is to optimize its coding in terms of the resulting transmission bandwidth or the resulting image quality.

Default:	6
Possible values:	0 … 9 – 0 – Optimized for low bandwidth – 9 – Optimized for high image quality
Remark:	Is used in connection with the **rtcpSenderreportEnabled** setting.

15.8.2 Universal Streaming Expert Settings

The configuration file of the Streaming provider contains the following universal settings. They apply for all configured RTP streaming routes.

- **aliveTimeout**

  Controls the watchdog process with which the Java media framework monitors the process of the native RTP unit.

  aliveTimeout specifies a period in which the native RTP unit process has to answer. If it does not, it is automatically rebooted.

Default:	60 [Seconds]
Possible values:	<Time> [seconds]

- **eventThreadpoolSize**

  Defines the size of the event thread pool for the Java media framework. This pool processes all events sent to the Java Media Framework by the native RTP unit.

Default:	5
Possible values:	<number >

- **icmpRecoveryTime**

  When the ICMP monitoring of the OpenScape Media Server is active (**icmpMonitoringEnabled** = true), the OpenScape Media Server reacts to ICMP messages that it receives from the network. If the number of received ICMP messages exceeds a threshold, the Media Server sends appropriate messages to its applications. The applications can react to this by temporarily stopping or reducing the send activities.

  The counter for the described threshold is reset after a period defined by **icmpRecoveryTime**.

Default:	200 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in connection with the following setting: – **icmpMonitoringEnabled** – **icmpUnreachableCount**

- **ipAddrMediaServer**

  Defines the IP address (IPv4, IPv6) under which the Java portion of the OpenScape Media Server communicates with the component NativeRtpUnit.

Default:	127.0.0.1
Possible values:	– <IPv4 address / IPv6 address> – <fully qualified host name> – *
Remark:	Is only required if the computer system of the OpenScape Media Server uses several network boards.

- **maxNumRtpPorts**

  Specifies the maximum permissible number of RTP channels that may be configured for the total number of RTP streaming routes.

  The value set here is thus the upper limit for the sum of the **numRtpPorts** settings of all RTP streaming routes.

  If an individual traffic measurement shows that not all RTP streaming routes use their maximum number of RTP ports at the same time, you may individually “overbook” the maximum permissible number of RTP channels of the RTP streaming routes. However, in this case you should regularly verify that the configured overbooking matches the RTP traffic behavior.

Default:	2500
Possible values:	>= **numRtpPorts** Depends on the hardware you use for the OpenScape Media Server.

- **mfwCommandString**

  Defines a text string that is transferred to the Media-Server-internal native RTP unit as command line command.

  The command interface of the native RTP unit defines which commands can be transferred here.

Default:	-k (close all other active entities of the native RTP unit)
Possible values:	– <command for the command interface of the native RTP unit > – <Blank> deactivates the default **-k**
Important:	Only trained service personnel may change this setting!

- **nativeRtpUnitUse10msSched**

  Specifies the RTP packet size used by the OpenScape Media Server.

Default:	false
Possible values:	– true – 10ms – false – 20ms.

- **nativeRtpUnitUseLowPrioScheduling**

  Defines which process / thread priority is used for the auxiliary process nativeRTPUnit.

Default:	false
Possible values:	– false – REALTIME_PRIORITY_CLASS – true – HIGH_PRIORITY_CLASS

- **nativeRtpUnitUseRtcClock**

  Specifies how the OpenScape Media Server synchronizes the RTP communication.

Default:	true

Possible values:	– true – Linux RealTimeClock – false – SystemClock
IMPORTANT:	Productive systems must be operated with the default.

- **numberOfProxyObjects**

  Defines the maximum size of the MFW-Object-Request-Brocker.

Default:	5000

- **rtpBlacklistedTime**

  The OpenScape Media Server uses an RTP port scanner to detect and fend off Denial-of-Service attacks. Using this scanner the OpenScape Media Server searches all officially free RTP ports for suspicious communication in a round-robin process. The suspicious communication may be caused by a client with unusual communication behavior or a Denial-of-Service attacker.

  If the RTP port scanner could not detect any suspicious communication on a checked RTP channel, it marks this port as safe and the OpenScape Media Server can use it for its communication. If the RTP port scanner detects suspicious communication on a checked RTP channel, this port is integrated in a black list and not be used by the OpenScape Media Server for a specific period.

  rtpBlacklistedTime specifies how long an individual RTP port is not used by the OpenScape Media Server when the RTP port scanner has detected suspicious communication on this port. After expiration of this period, the port can be used by the OpenScape Media Server again.

Default:	30 [seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in connection with the following setting: – **rtpScanDuration** – **rtpScanWindowSize**.

- **rtpScanDuration**

  The OpenScape Media Server uses an RTP port scanner to detect and fend off Denial-of-Service attacks. Using this scanner the OpenScape Media Server searches all officially free RTP ports for suspicious communication in a round-robin process. This involves groups of RTP ports.

  If the RTP port scanner could not detect any suspicious communication on a checked RTP channel, it marks this port as safe and the OpenScape Media Server can use it for its communication.

  rtpScanDuration specifies how long the RTP port scanner searches a group of RTP channels for suspicious communication per round-robin cycle.

Default:	500 [milliseconds]
Possible values:	<100 … 2000> [milliseconds]

Remark:	Is used in connection with the following setting: – **rtpBlacklistedTime** – **rtpScanWindowSize**.

- **rtpScanWindowSize**

  The OpenScape Media Server uses an RTP port scanner to detect and fend off Denial-of-Service attacks. Using this scanner the OpenScape Media Server searches all officially free RTP ports for suspicious communication in a round-robin process. This involves groups of RTP ports. If the RTP port scanner could not detect any suspicious communication on a checked RTP channel, it marks this port as safe and the OpenScape Media Server can use it for its communication.

  rtpScanWindowSize specifies how many RTP ports the OpenScape Media Server simultaneously checks for a specific period. Setting **0** deactivates the RTP port scanner.

  The period length is determined by **rtpScanDuration**.

  NOTICE:

  While a group of RTP ports is being searched by the RTP port scanner, the relevant ports are not available for the RTP communication. A larger total number of RTP ports used should therefore be configured.

Default:	20
Possible values:	– 0 – deactivates the RTP port scanner – <1 … 100>
Remark:	Is used in connection with the following setting: – **rtpBlacklistedTime** – **rtpScanDuration**.

- **socketManagerRxPort**

  Specifies the receiving port via which the Java portion of the Media Framework receives information from the native portion.

Default:	7000
Possible values:	<port number>

- **socketManagerTxPort**

  Specifies the send port via which the Java portion of the Media Framework sends information to the native portion.

Default:	7001
Possible values:	<port number>

- **supportedAudioFormats**

  Defines the audio formats that the OpenScape Media Server can use.

Default:	audio/PCMU audio/PCMA audio/G729 audio/G729;annexb=no
Possible values:	Blank-separated list of settings in the form of <supportedAudioFormats></supportedAudioFormats> – audio/G722 – audio/G7221;rate=16000;bitrate=24000 – audio/G7221;rate=16000;bitrate=32000 – audio/G7221;rate=32000;bitrate=24000 audio/G7221;rate=32000;bitrate=32000 – audio/G7221;rate=32000;bitrate=48000 – audio/G729 – audio/G729;annexb=no – audio/opus – audio/PCMA – audio/PCMU – audio/telephone-event

- **supportedFaxFormats**

  Defines the fax formats that the OpenScape Media Server can use.

Default:	audio/L16 image/t38
Possible values:	Blank-separated list of settings of the following list in the form `audio/<format setting>` or `image/<format setting>`: – L16 – T.30-Fax – t38 – T.38-Fax

- **supportedVideoFormats**

  Defines the video formats that the OpenScape Media Server can use.

Default:	video/H264 video/H264;profile-level-id=428014 video/H264;packetization-mode=1
Possible values:	Blank-separated list of settings in the form of <supportedVideoFormats></supportedVideoFormats>: – video/H264;profile-level-id=640028 – video/H264;profile-level-id=640028;packetization-mode=1 – video/H264;profile-level-id=428033 video/H264;profile-level-id=428033;packetization-mode=1 – video/VP8

- **zombiObjectTimeout**

  The Media Framework uses a so-called “zombie” scanner that checks in 60-second intervals all assigned / active MFW objects for their topicality. If the scanner finds an object in this search the age of which exceeds a specified period, it is removed from the internal assignment table as so-called “zombie”.

zombiObjectTimeout defines the length of this period.

Whether or not the “zombie” scanner finds outdated MFW objects becomes visible when you configure the log level `FINEST` for the following log category:`com.siemens.media.mfw.native.MfwNativeObjectManager`

Search the log for a line of the following format:

```
start scanning for possible outdated MFW zombi-objects
(zombis detected till now: '<xxx>' - items in alloc-list
'<zzz>'
```

In smooth operation, value `0` should always be displayed for <xxx>.

If the “zombie” scanner finds outdated MFW objects, an error message of the following format is put out:

```
15:02:43,365 INFO native.MfwNativeObjectManager[]! MFW
object zombi detected .. will be freed!
```

Default:	36030 [Seconds]
Possible values:	<1 … 604800> [seconds]

15.9 Expert Settings for Streaming IVR

The expert settings for streaming IVR are administered in the streaming configuration file.

Configuration file:	`streaming.component.xml`
Storage location:	/<host >`/providers/streaming-mps`

<host > corresponds to one of the following paths:

- `/enterprise/mediaserver/application_host`
- `/opt/siemens/mediaserver/application_host`

You can divide the configuration file for streaming IVR in two areas:

- Settings specific to MRCP connections

  Settings that apply individually for each configured MRCP connection to a TTS or ASR system.
- Universal settings

  Settings that are universally valid and independent from the configured MRCP connections.

15.9.1 Streaming IVR Expert Settings Specific to MRCP Connections

All MRCP-based connections to a TTS and / or ASR system are labeled in the configuration file by the **mrcp** tag. The **uri** attribute of the **mrcp** tag defines the complete or partial address under which the TTS or ASR system can be reached. If no value has been specified for **uri**, communication via MRCP is inactive.

```
<mrcp uri="rtsp://10.1.210.100:554">
    <keep-session-open>false</keep-session-open>
    <multipart-support>false</multipart-support>
    <recognizer uri="media/recognizer">
        <preferred-format>G711u</preferred-format>
        <preferred-format>G711a</preferred-format>
    <recognizer uri="media/recognizer">
    <synthesizer uri="media/synthesizer">
        <additional-sdp-attributes>modul:guaranteed</additional-sdp-
        attributes>
    </synthesizer>
</mrcp>
```

Each of the configured MRCP-based connections contains the following settings:

- **additional-sdp-attributes**

  Defines SDP attributes that the OpenScape Media Server sends to the connected TTS / ASR system.

Default:	–
Possible values:	<list of SDP attributes>
Remark:	Optionally admitted under the following elements: – **mrcp** – **recognizer** – **synthesizer**

- **keep-session-open**

  Specifies whether the OpenScape Media Server

  – closes a connection to the ASR / TTS system, after the requested announcement was played via the ASR / TTS system
  – keeps a connection to the ASR / TTS system open until the communication connection that the OpenScape Media Server has opened for the relevant ASR / TTS connection is closed down.

Default:	false
Possible values:	– true – ASR / TTS session will stay open during the connection – false – ASR / TTS session will be closed after the TTS playback.

Remark:	Optionally admitted under the following elements: – **mrcp** – **recognizer** – **synthesizer** The false option should be set here. This reduces the number of ASR / TTS licenses the system requires for operation.

- **multipart support**

  Specifies whether the OpenScape Media Server can send multipart MIME messages to the ASR or TTS system used.

Default:	false
Possible values:	– true – Send multipart MIME messages – false – do not send multipart MIME messages.
Remark:	Optionally admitted under the following elements: – **mrcp** – **recognizer** – **synthesizer**

- **preferred-format**

  Specifies the RTP streaming format that OpenScape Media Server announces to the MRCP server as preferred format.

Default:	–
Possible values:	– G711u – G711a – G729
Remark:	Optionally admitted under the following elements: – **mrcp** – **recognizer** – **synthesizer** Each preferred-format setting can always only define one format. If you want to use various formats preferably, specify preferred-format several times.

- **recognizer**

Remark:	Optional structure element

Structures the settings for a connected ASR system. The **uri** attribute of **recognizer** defines the address under which the ASR system can be reached. With this applies:

– If no address has yet been specified in the **uri** attribute of the superordinate **mrcp** tag, the complete address of the ASR system must be defined in the **uri** attribute of **recognizer**.

```
<mrcp>
```

```
        <keep-session-open>false</keep-session-open>
        <recognizer uri="rtsp://10.1.210.100:557/media/recognizer">
        <recognizer uri="media/recognizer">
        <synthesizer uri="rtsp://10.1.211.46:4900/media/
        speechsynthesizer">
            <multipart-support>false</multipart-support>
        </synthesizer>
</mrcp>
```

– If an address has already been specified in the **uri** attribute of the superordinate **mrcp** tag, only a possibly required address extension must be specified in the **uri** attribute of **recognizer**.

```
<mrcp uri="rtsp://10.1.210.100:554">
        <keep-session-open>false</keep-session-open>
        <multipart-support>false</multipart-support>
        <recognizer uri="media/recognizer">
            <preferred-format>G711u</preferred-format>
            <preferred-format>G711a</preferred-format>
        <recognizer uri="media/recognizer">
        <synthesizer uri="media/synthesizer">
            <additional-sdp-attributes>modul:guaranteed</additional-
            sdp-attributes>
        </synthesizer>
</mrcp>
```

- **rfc2833-payload-type**

  Defines the payload type used by the Streaming provider for sending RFC 2833 events to the ASR system.

Default:	–
Possible values:	<Encoding according to RFC 2833>
Remark:	Optionally admitted under **recognizer**.

- **streamingRouteId**

  Defines the ID of the RTP streaming route via which RTP data is to be exchanged with the TTS / ASR system.

  The **streamingRouteId** setting is admitted only directly under the **mrcp** tag.

Default:	–
Possible values:	<ID of an RTP streaming route>

Remark:	Optional. Only admitted directly under the **mrcp** tag. Must only be used if RTP data is not to be exchanged with the TTS / ASR system via the RTP streaming route **Standard**.

- **synthesizer**

Remark:	Optional structure element

Structures the settings for a connected TTS system. The **uri** attribute of **synthesizer** defines the address under which the TTS system can be reached. With this applies:

– If no address has yet been specified in the **uri** attribute of the superordinate **mrcp** tag, the complete address of the ASR system must be defined in the **uri** attribute of **synthesizer**.

```
<mrcp>
    <keep-session-open>false</keep-session-open>
    <recognizer uri="rtsp://10.1.210.100:557/media/recognizer">
    <recognizer uri="media/recognizer">
    <synthesizer uri="rtsp://10.1.211.46:4900/media/
    speechsynthesizer">
        <multipart-support>false</multipart-support>
    </synthesizer>
</mrcp>
```

– If an address has already been specified in the **uri** attribute of the superordinate **mrcp** tag, only a possibly required address extension must be specified in the **uri** attribute of **synthesizer**.

```
<mrcp uri="rtsp://10.1.210.100:554">
    <keep-session-open>false</keep-session-open>
    <multipart-support>false</multipart-support>
    <recognizer uri="media/recognizer">
        <preferred-format>G711u</preferred-format>
        <preferred-format>G711a</preferred-format>
    <recognizer uri="media/recognizer">
    <synthesizer uri="media/synthesizer">
        <additional-sdp-attributes>modul:guaranteed</additional-
        sdp-attributes>
    </synthesizer>
</mrcp>
```

15.9.2 Universal Streaming IVR Expert Settings

The configuration file for streaming IVR contains the following universal settings.

- **noRtpStreamTimeout**

  Defines a period in which the Streaming provider expects an RTP packet for and RTP connection. If the Streaming provider does not register an RTP packet in this period, it may send RTP-Stream-Absent messages to the application layer.

  Sending the above RTP-Stream-Absent messages is activated by the **rtpStreamMonitoringEnabled** setting.

Default:	15 [Seconds]
Possible values:	<Time> [seconds]
Remark:	Is used in connection with the **rtpStreamMonitoringEnabled** setting:

- **recordingSensitivity**

  The OpenScape Media Server uses a voice recorder for voice recordings.

  If this voice recorder operates in the automatic recording mode, **recordingSensitivity** specifies the sensitivity for realizing the end of the recording.

Default:	50 [%]
Possible values:	<0 … 100> [%]

- **rtpStreamMonitoringEnabled**

  Defines whether the Streaming provider sends RTP-Stream-Absent messages to the application layer if no RTP packets have been registered for an RTP connection within a specific period.

Default:	false
Possible values:	– true – Activates RTP packet monitoring – false – Deactivates RTP packet monitoring.
Remark:	Is used in connection with the **noRtpStreamTimeout** setting:

SDP Settings

The universal streaming IVR settings contain the following SDP settings. These settings are enclosed in the **sdp** tag.

- **audioFormats**

  Specifies system-wide which audio codecs the OpenScape Media Server can use for transmitting RTP data. The codec sequence in this list defines the individual priority with which the OpenScape Media Server is to use the relevant codec. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

The entire codec list is enclosed by the **audioFormats** tag. The single list entries are enclosed by the **format** tag.

Example:	<audioFormats><format>audio/opus</format><format>audio/G7221; bitrate=48000; rate=32000</format><!-- enable G.722.1 32 kHz 24 kbit/s for Lifesize VHD 100 / VHD 400 --><!--format>audio/G7221;rate=32000;bitrate=24000</format --><format>audio/opus; maxplaybackrate=24000; sprop-maxcapturerate=24000</format><format>audio/G7221; bitrate=32000</format><format>audio/G722</format><format>audio/PCMU</format><format>audio/PCMA</format><format>audio/G729</format><format>audio/G729; annexb=no</format><format payloadType="101">audio/telephone-event</format></audioFormats>

Possible values:	– audio/opus – audio/opus; maxplaybackrate=24000; sprop-maxcapturerate=24000 – audio/G7221; bitrate=48000; rate=32000 – audio/G7221;rate=32000;bitrate=24000 – audio/G711A – audio/G711U – audio/G729 – audio/G722 – audio/PCMA – audio/PCMU – audio/G729; annexb=no – audio/telephone-event
Remark:	This setting is used for a connection only if no audio codec list specific to the data stream has been configured for the terminal used.

- **anatEnabled**

  You can connect the OpenScape Media Server to the network via IPv4 and IPv6 addresses simultaneously. In this case **anatEnabled** specifies system-wide whether the OpenScape Media Server uses the ANAT protocol for informing communication partners about the alternatively available IP addresses.

Remark:	Is configured via the Common Management Platform.

- **faxFormats**

  Specifies system-wide which fax codecs the OpenScape Media Server can use for transmitting RTP data. The codec sequence in this list defines the individual priority with which the OpenScape Media Server is to use the relevant codec. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

The entire codec list is enclosed by the **faxFormats** tag. The single list entries are enclosed by the **format** tag.

Example:	<audioFormats> <format>image/t38</format> </audioFormats>

Possible values:	image/t38
Remark:	This setting is used for a connection only if no fax codec list specific to the data stream has been configured for the terminal used.

- **forceLocalCodecPreference**

  Each RTP terminal uses an individual codec list to negotiate for RTP connections with its counterpart which codec is to be used for transmitting the RTP data. The codec sequence in this list defines the individual priority with which the relevant terminal wants to use a listed codec.

  Because the codec lists of different RTP terminal devices vary as a rule, you need to specify, which codec list shall define the priority of an available codec.

  forceLocalCodecPreference specifies whether the relevant codec list of the OpenScape Media Server or the codec list of the communication partner defines the priority of an available codec for inbound connections. According to RFC 3264, the codec list of the communication partner should do this as a rule.

Default:	false
Possible values:	– true – Codec list of the OpenScape Media Server – false – Codec list of the communication partner

- **iceEnabled**

  You can connect the OpenScape Media Server to the network via IPv4 and IPv6 addresses simultaneously. In this case **iceEnabled** specifies system-wide whether the OpenScape Media Server uses the ICE protocol for informing communication partners about the alternatively available IP addresses.

  You can configure the **microlite** attribute for **iceEnabled** in addition. If ICE is active, this attribute specifies whether the OpenScape Media Server uses ICE in version lite or microlite. You can configure the settings **true** or **false** for the **microlite** attribute. If you configure setting **true**, the OpenScape Media Server uses version ICE microlite, and it uses version ICE lite if you configure setting **false**.

Example:	<iceEnabled microlite="false">true</iceEnabled>

Remark:	Is configured via the Common Management Platform.

- **offeredSdesRTPAuthTag**

  Defines the length of the authentication tag that the OpenScape Media Server uses for the cryptographic procedure HMAC-SHA1 used.

Remark:	Is configured via the Common Management Platform.

- **offeredSecurityProtocol**

  Specifies the protocol via which the OpenScape Media Server can negotiate SRTP keys with terminals.

Remark:	Is configured via the Common Management Platform.

- **secureMode**

  Specifies system-wide, which type of security the OpenScape Media Server uses for inbound and outbound connections.

  The possible settings have the following meaning.

  – secure_only

    A connection is only set up if the communications system and the RTP terminal use SRTP with MIKEY or SDES for the RTP communication.

    IMPORTANT:

    The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

  – insecure_only

    A connection is only set up if the communications system and the RTP terminal use an unencrypted RTP communication.

  – secure_preferred

    If the communications system and the RTP terminal can use SRTP with MIKEY or SDES for the RTP communication, the OpenScape Media Server uses this type of communication.

    If the communications system and the RTP terminal can only use an unencrypted RTP communication, the RTP connection is set up unencrypted.

    IMPORTANT:

    The keys for encrypting the RTP communication are exchanged via SIP. In case of this setting it is therefore important to configure the TLS transport protocol in the SIP configuration also.

  You can additionally configure the **securityLineMode** attribute for the security type setting **secure_preferred**. This attribute specifies whether the relevant security type is signalled via a single or two so-called m-line(s). The associated attribute settings are called **SingleLine** or **DualLine** accordingly. If the attribute is not specified, the **DualLine** setting is defaulted.

Example:	<secureMode securityLineMode="SingleLine">secure_preferred</secureMode>

Default:	secure_preferred
Possible values:	– secure_only – insecure_only – secure_preferred (with attribute **securityLineMode** if required)
Remark:	This setting is used for a connection only if no security setting specific to the terminal has been configured for the terminal used.

- **videoFormats**

  Specifies system-wide which video codecs the OpenScape Media Server can use for transmitting RTP data. The codec sequence in this list defines the individual priority with which the OpenScape Media Server is to use the relevant codec. The codec with the highest priority appears as first entry in the codec list; the one with the lowest priority is the bottom entry in the list.

  The entire codec list is enclosed by the **videoFormats** tag. The single list entries are enclosed by the **format** tag.

Example:	<videoFormats><format>video/H264; profile-level-id=640028; max-mbps=250000; max-fs=10000</format><format>video/H264; profile-level-id=640028; max-mbps=250000; max-fs=10000; packetization-mode=1</format><format>video/H264; profile-level-id=428028; max-mbps=250000; max-fs=10000</format><format>video/H264; profile-level-id=428028; max-mbps=250000; max-fs=10000; packetization-mode=1</format><format payloadType="100">video/VP8</format></videoFormats>

Possible values:	– video/VP8 – video/H264
Remark:	This setting is used for a connection only if no video codec list specific to the data stream has been configured for the terminal used.

15.10 Expert Settings for the Resource Database

The expert settings for the resource database are administered in the resource database configuration file.

Configuration file:	`resource-database.component.xml`
Storage location:	/<host >`/providers/resource-database`

<host > corresponds to one of the following paths:

- `/enterprise/mediaserver/application_host`
- `/opt/siemens/mediaserver/application_host`

In this configuration file of the resource database the following settings are available:

- **defaultLanguage**

  Defines the language the announcements and tones of which the OpenScape Media Server uses if no language has been specified with a play-back prompt by OpenScape Voice.

Default:	en
Possible values:	<Language code >

- **fallbackLanguages**

  If a language package does not contain all country-specific announcements of the relevant country, **fallbackLanguages** determines from which alternative language package the OpenScape Media Server plays the missing announcements.

  Example: <**fallbackLanguages**>`zh_hk=en_us`</**fallbackLanguages**>

  Defines that the OpenScape Media Server uses English (US) as alternative language package for the sublanguage Hongkong.

Default:	ms=en_us,id=en_us,th=en_us,fr_ma=fr,bs=sr,lt=en, en_ph=en_us,zh_hk=en_us,zh_tw=en_us,zh_sg=en_us, ko=en_us,vi=en_us,ja=en_us,es_ve=es_mx,es_ec=es_mx, es_pe=es_mx,es_co=es_mx
Possible values:	Comma-separated list of the format: <language code language package > = <language code altern.language package >

- **preferredLanguages**

  Several language packages may be installed on the OpenScape Media Server for an OpenScape Voice language ID (basic language). For example, for the OpenScape Voice language ID en the language packages for India (en_in) and for the US (en_us).

  In this case you can define in the **preferredLanguages** setting which of these language packages is used for the associated OpenScape Voice language ID.

Default:	–
Possible values:	Comma-separated list <four-digit language codes >
Remark:	Optional

15.11 Settings for Applications based on the Application Builder (Applications Plug#in)

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Applications tab** > **<Application Builder application>**

If an application has been created using the Application Builder, you can configure your settings via a generic application plug-in.

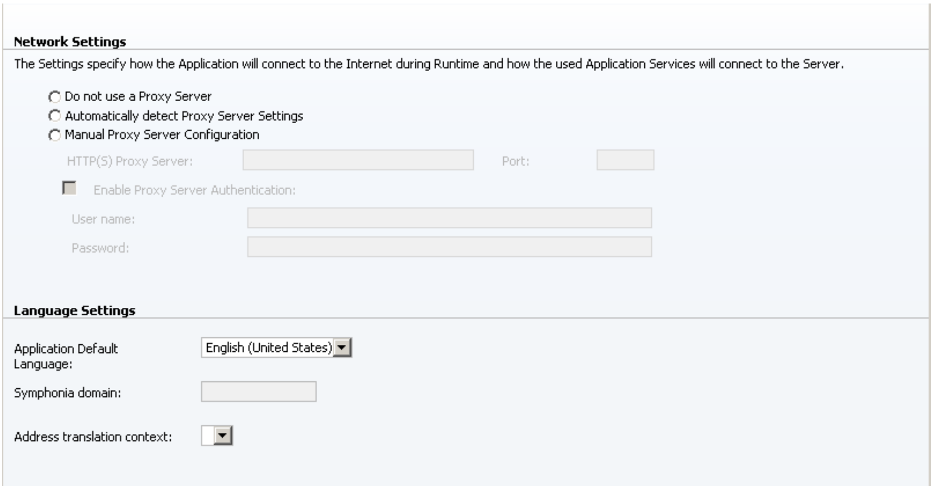
The settings of this application plug-in are grouped in the following areas:

- Application configuration
- Deployment
- Application webservices
- Databases

15.11.1 Application Configuration

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Applications tab** > **<Application Builder application>** > **Application configuration**

On this tab you perform the general configuration settings for the application.



- **Network Settings**

  Defines whether the application is to connect to the internet via a proxy server.

  You can choose from:

  – **Do not use a Proxy Server**

    The application attempts to connect to the internet directly.

  – **Automatically detect Proxy Server Settings**

    If possible, the settings of a configured proxy server are automatically determined via the Web Proxy Autodiscovery protocol (WPAD).

  – **Manual Proxy Server Configuration**

    You can manually specify the connection settings of a proxy server under **HTTP(S) Proxy Server** and **Port**.

    If the proxy server used demands authentication, you need to activate the **Enable Proxy Server Authentication** option. In this case you need to specify the details for a successful authentication under **User name** and **Password**.

- **Application Default Language**

  The application always plays the first announcements in a language that is independent form the calling user– this is the so-called default language.

  The application does not attempt to determine the user-individual language setting until the calling user has logged in at the system. In this attempt the application uses the specified log-in data to look for the individual user settings in the OpenScape user database. If the determined, user-individual language setting differs from the default language, the application can switch the TUI to this determined language.

  Guests can hear the application announcements in the default language only.

  Default language defines the default language for the application.

Default:	English (US)
Possible values:	– German – English (UK) – English (US) – Spanish – French – Italian – Portuguese (Brazil) – Portuguese (Portugal) – Chinese
Remark:	Only those languages are offered for selection that have been installed for the language package.

- **Symphonia domain**

Default:	system
Remark:	Cannot be modified.

- **Address translation context**

  If, for example, a user needs to specify a phone number in the application, he/she will do this always with reference to the respective location. For example, as pure extension or as phone number with area code but without international prefix. This leads to problems, though, if the application and the user are e. g. situated in different countries.

  To evade such phone number problems, the OpenScape system transforms all phone numbers before the actual processing into a normalized phone number format – e. g. +492404901100. The thus normalized phone numbers then contain all information that the phone number uniquely identifies or localizes.

  The OpenScape system uses for the phone number normalization so-called address conversion contexts.

  If an OpenScape user enters a phone number via TUI, the application uses the information of the relevant OpenScape user as address translation context. If this is not possible, the voice portal uses address translation contexts that can be configured in the CMP instead.

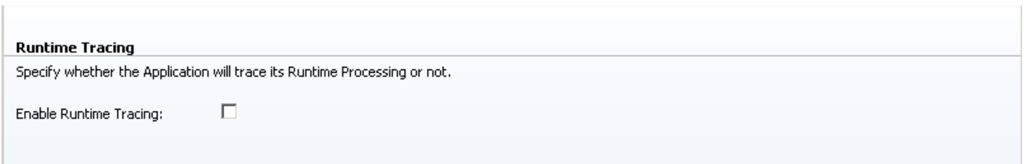
  Address translation context defines the ID of an address translation context configured in the CMP. The application can use this context for phone number normalization, if no OpenScape user is available as address translation context.

Default:	–
Remark:	<ID of an address translation context>

15.11.2 Deployment

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Applications tab** > **<Application Builder application>** > **Deployment**

On this tab you define whether tracing is active for the application.



- **Enable Runtime Tracing**

  Activates application tracing as soon as the application is started.

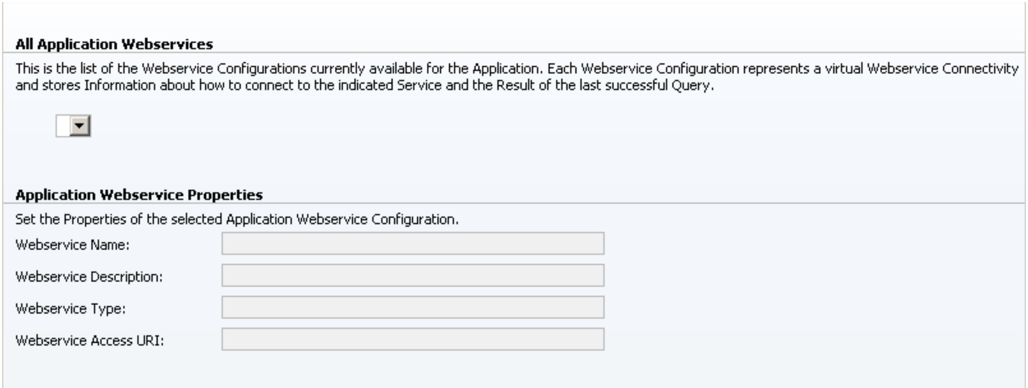
15.11.3 Application Webservices

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Applications tab** > **<Application Builder application>** > **Application Webservices**

This tab displays the settings of all webservice connections that the Application Builder application uses.

NOTICE:

The displayed properties were configured when the application was created in the Application Builder. On this tab you can merely see but not change the properties.



- **All Application Webservices**

  Shows a list of all webservice connections that the Application Builder application uses. The following properties are displayed for the selected webservice connection:

  – **Webservice Name**

    Defines the name of the connected webservice.

  – **Webservice Description**

    Gives a short description of the connected webservice.

  – **Webservice Type**

    Defines the type of the connected webservice.

  – **Webservice Access URI**

    Defines the URI under which the connected webservice can be reached.

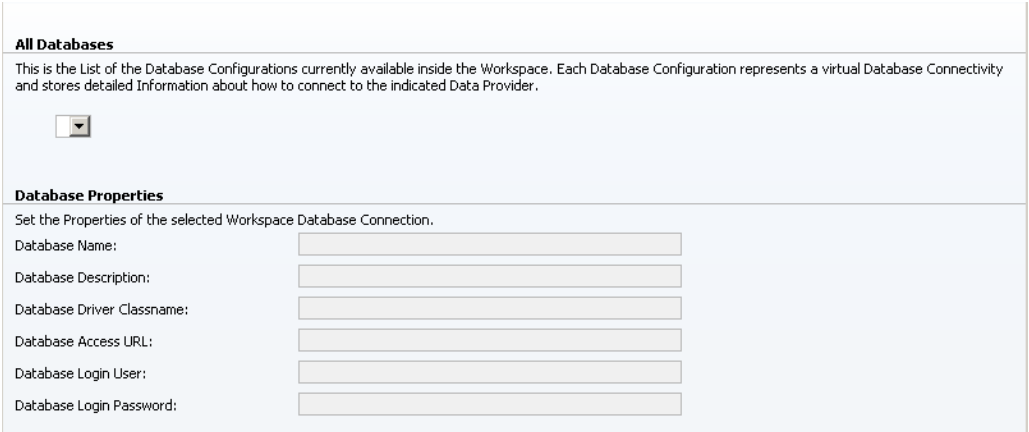
15.11.4 Databases

Invocation in the Common Management Platform:
Operation & Maintenance > **Unified Communications** > **Configuration** > **Media Server** > **Applications tab** > **<Application Builder application>** > **Databases**

This tab displays the settings of all database connections that the Application Builder application uses.

NOTICE:

The displayed properties were configured when the application was created in the Application Builder. On this tab you can merely see but not change the properties.



- **All Databases**

  Shows a list of all database connections that the Application Builder application uses. The following properties are displayed for the selected database connection:

  – **Database Name**

    Defines the name of the connected database.

  – **Database Description**

    Gives a short description of the connected database.

  – **Database Driver Classname**

    Defines the type of the connected database.

  – **Database Access URL**

    Defines the URL under which the connected database can be reached.

  – **Database Login User**

    Defines the name of the database user account with which the application accesses the database.

  – **Database Login Password**

    Defines the password for the database user account specified under **Database Login User**.

Index

W