



A MITEL
PRODUCT
GUIDE

Mitel CX

OpenScape Contact Media Service Integration Guide

Release Number 1.0

July 2025

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel”), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 About this guide	5
1.1 Who should use this guide	5
1.2 Formatting conventions	5
1.3 Documentation feedback	6
2 Installing the OpenScape Contact Media Service	7
2.1 Virtualization requirements	7
2.2 System requirements	7
2.3 Installation	8
2.4 Optional post-installation optimization parameters	14
3 Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX	17
3.1 Prerequisites	17
3.2 Logging in the OpenScape Contact Media Service	17
3.3 Configuring the OpenScape Contact Media Service for SIP Platforms	18
3.3.1 VoIP Configuration	18
3.3.2 Users Configuration	21
3.3.3 Networking Configuration	21
3.3.4 Security Configuration	22
3.3.5 SDK Configuration	25
3.3.6 Recorder Configuration	26
3.3.7 IVR Configuration	29
3.3.8 System	30
3.3.9 System Messages	30
3.4 Configuring the OpenScape Contact Media Service for MiVB Platform	31
3.4.1 Integration with GCP for TTS and ASR	31
3.4.1.1 uniMRCP Configuration	31
3.4.1.2 GCP Authentication	32
3.4.1.3 Speech Recognition Configuration	33
4 Quality of Service in OpenScape Contact Media Service	35
4.1 RTP	35
4.2 SIP	35
4.3 TOS/DSCP Values	36
Index	38

1 About this guide

This guide describes the integration between Contact Media Service (CMS) and Mitel CX. The purpose of this integration document is to ensure a unified communication experience, optimized resource utilization, and improved customer engagement.

1.1 Who should use this guide

This guide is intended for installation technicians or anyone else in the organization who is responsible with the integration between Contact Media Service (CMS) and Mitel CX.

1.2 Formatting conventions

The following formatting conventions are used in this guide:

Bold

This font identifies OpenScape Contact Media Service components, window and dialog box titles, and item names.

Italic

This font identifies references to related documentation.

`Monospace Font`

This font distinguishes text that you should type, or that the computer displays in a message.

NOTE: Notes emphasize information that is useful but not essential, such as tips or alternative methods for performing a task.

IMPORTANT: Important notes draw special attention to actions that could adversely affect the operation of the application or result in a loss of data.

About this guide

Documentation feedback

1.3 Documentation feedback

To report an issue with this document, call the Customer Support Center.

When you call, be sure to include the following information. This will help identify which document you are having issues with.

- **Title:** Mitel CX OpenScape Contact Media Service, Integration Guide

2 Installing the OpenScape Contact Media Service

This chapter provides an overview of the OpenScape Contact Media Service and includes detailed instructions on how to install the OpenScape Contact Media Service software on a stand-alone server machine.

2.1 Virtualization requirements

The virtualization requirements for OpenScape Contact Media Service are the following:

	Product version	ESXi V6.0	ESXi V6.5	ESXi V6.7	ESXi V7.0	ESXi V8.0
OpenScape Contact Media Service	V12	YES	YES	YES	YES	
	Supported HW Version(s) ¹	10,11	10,11,13	10,11,13,14	10,11,13,14,15,17,18,19	

Table 1 Virtualization requirements for OpenScape Contact Media Service

¹ HW Versions 14-18 are allowed, however please note that support for VMware related issues is provided for highest verified HW version (<https://kb.vmware.com/s/article/2007240>) although no issues are known for versions 14-18.

OpenScape Contact Media Service -supported VMware VSphere Features

	vMotion	HA	FT	SRM	vStorage-APIs for Data Protection	VMware-Tools	EVC	vCloud Director
OpenScape Contact Media Service	Y	Y	N	Y	N	N	Y	N

Table 2 OpenScape Contact Media Service -supported VMware VSphere Features

2.2 System requirements

The minimum system requirements for installing the OpenScape Contact Media Service software on a stand-alone server machine depends on the expected traffic and the use of call recording.

For **Small Systems** (up to 100 agents and 2700 calls per hour):

Requirement	Description
Processor	Intel Xeon Silver 4316 2.3 GHz
CPU Cores	8 vCPU
Memory	8 GB

Table 3 System requirements for a stand-alone server machine with up to 100 agents and 2700 calls per hour

Installing the OpenScape Contact Media Service

Installation

Requirement	Description
Hard Drive	160 GB, 7200 RPM, SATA (+1 TB if recording enabled; separate disk)
Other	1 Gbps Ethernet network interface card DVD ROM Drive

Table 3 System requirements for a stand-alone server machine with up to 100 agents and 2700 calls per hour

For **Medium Systems** (up to 375 agents and 5400 calls per hour):

Requirement	Description
Processor	Intel Xeon Silver 4316 2.3 GHz
CPU Cores	8 vCPU
Memory	8 GB
Hard Drive	160 GB, 7200 RPM, SATA (+1 TB if recording enabled; separate disk)
Other	1 Gbps Ethernet network interface card DVD ROM Drive

Table 4 System requirements for a stand-alone server machine with up to 375 agents and 5400 calls per hour

For **Large Systems** (up to 1200 agents and 13000 calls per hour), 2 CMS nodes are required:

Requirement	Description
Processor	Intel Xeon Silver 4316 2.3 GHz
CPU Cores	8 vCPU (10 vCPU is call recording is enabled)
Memory	8 GB
Hard Drive	160 GB, 7200 RPM, SATA (+1 TB if recording enabled; separate disk)
Other	1 Gbps Ethernet network interface card DVD ROM Drive

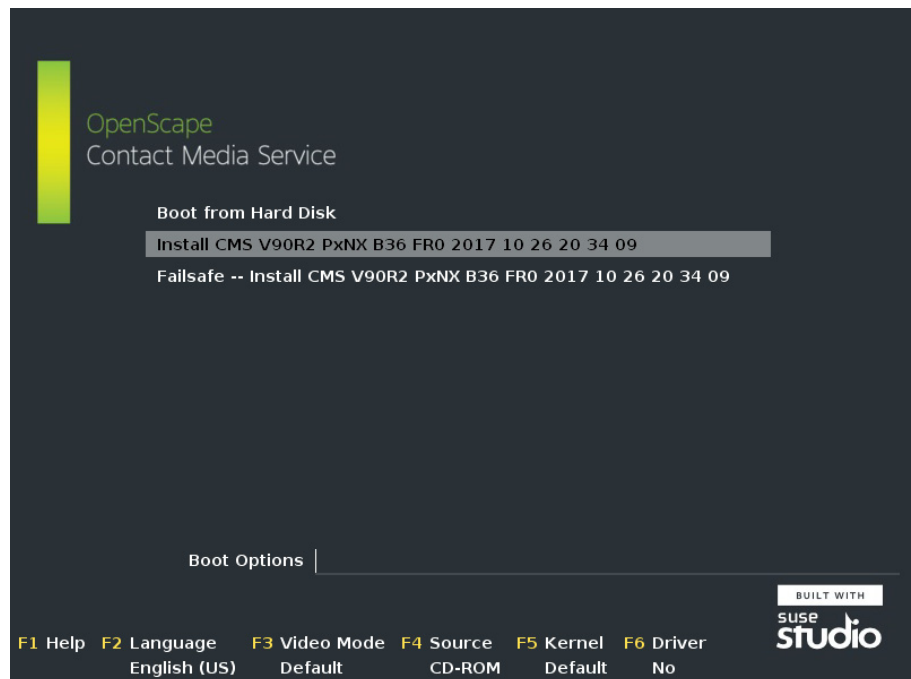
Table 5 System requirements for a stand-alone server machine with up to 1200 agents and 13000 calls per hour

2.3 Installation

During the installation of the CMS with recording, when the installer verifies that there is a 2nd hard disk, this hard disk must not be reformatted, because it will probably contain recording File System and Database.

To install the OpenScape Contact Media Service software, follow the steps below:

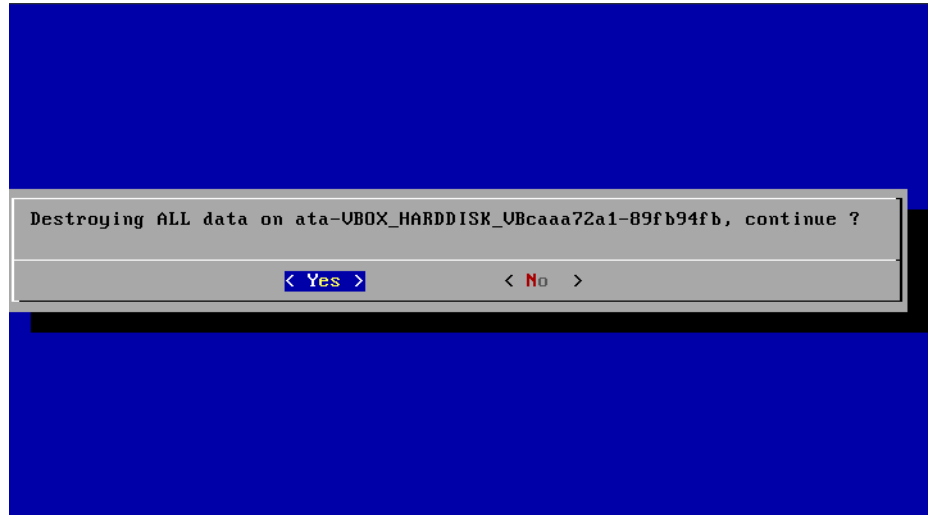
1. Insert the OpenScape Contact Media Service DVD into the DVD-ROM drive.
2. Restart the server machine and choose to boot from the DVD, not from the hard drive. How to do this will vary slightly depending on the server machine hardware. Normally, when you restart the server machine, it will boot from the hard drive even if a DVD is present. To make it boot from the DVD, watch the screen that first appears for a message that describes which key to press to configure the boot process. Typically, this requires pressing **F2** or the **Delete** key.
3. Select the option to boot from the DVD-ROM drive. (The appearance of this screen will vary depending on the server machine hardware.) This launches the openSUSE installation program, which will guide you through the rest of the installation process.
4. In the installer's initial screen, use the keyboard arrow keys to select **Install CMS**, and then press **Enter**.



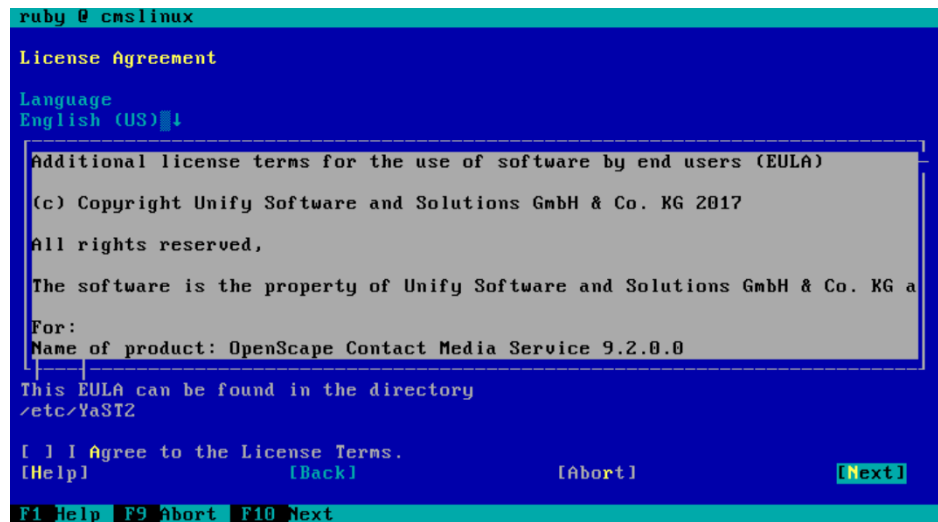
Installing the OpenScape Contact Media Service

Installation

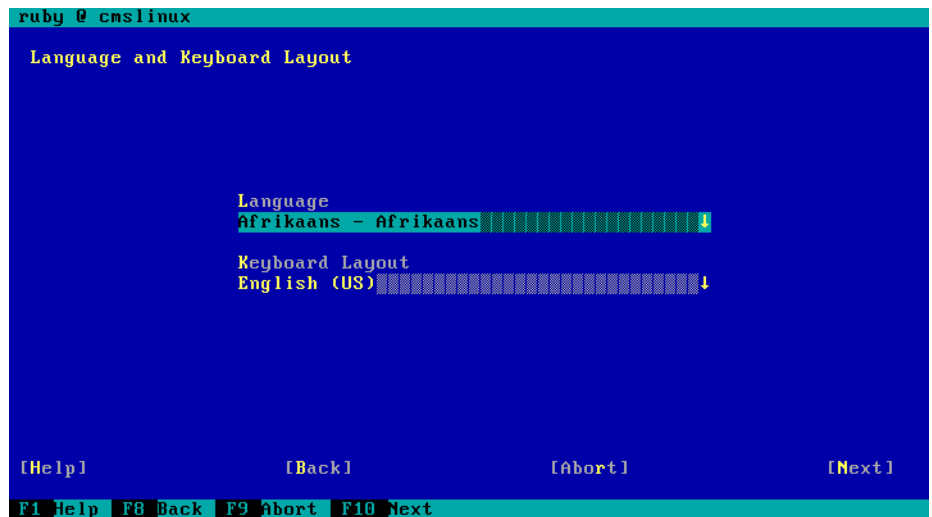
5. The installation will destroy all data in the hard disk. Select **Yes** to continue.



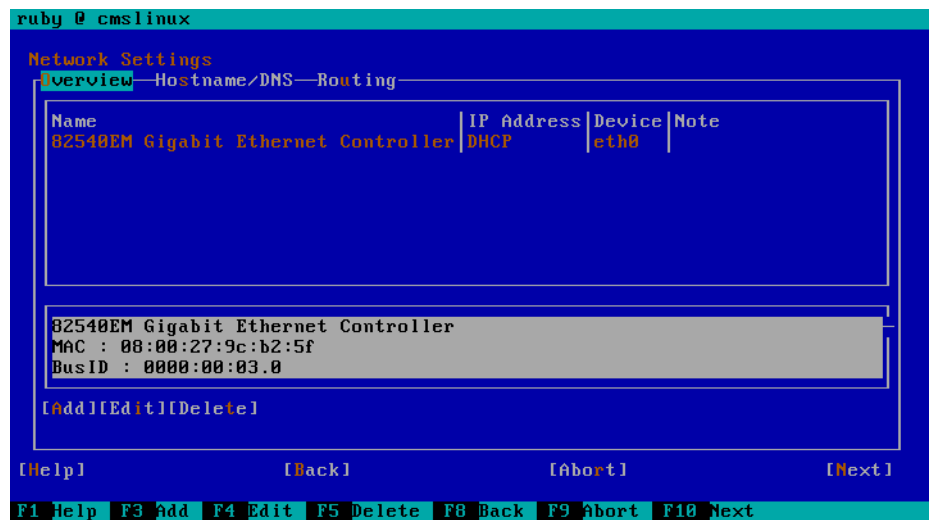
6. In the License Agreement screen, read the license agreement carefully, and then select **I Agree to the License Terms** and click **Next**.



7. In the Language and Keyboard Layout screen, select the language you want to use and your keyboard layout and click **Next**.



8. In the Network Settings screen, set your network configuration and hostname and click **Next**. You can skip this step and configure it via the web interface.



Installing the OpenScape Contact Media Service

Installation

9. In the Proxy Configuration screen, you can enable proxy settings. Click **OK**.

```
ruby @ cmslinux
Proxy Configuration

[ ] Enable Proxy
Proxy Settings
HTTP Proxy URL
http://
HTTPS Proxy URL
http://
FTP Proxy URL
http://
[ ] Use the Same Proxy for All Protocols
No Proxy Domains

Proxy Authentication
Proxy User Name
Proxy Password

[Help] [Cancel] [ OK ]
F1 Help F9 Cancel F10 OK
```

10. In the Advanced NTP Configuration you can configure a Network Time Protocol for clock synchronization. Click **OK**.

```
ruby @ cmslinux
Advanced NTP Configuration
General Settings—Security Settings—
Start NTP Daemon
( ) Synchronize without Daemon
( ) Now and on Boot

Runtime Configuration PolicyCustom Policy
Auto
Interval of the Synchronization in Minutes
+ 5+

Synchronization Type|Address
[Add][Edit][Delete] [Display Log...]

F1 Help F3 Add F4 Edit F5 Delete F9 Cancel F10 OK
```

11. In Local User screen, you can create a new Operating System's user. This user will be able to access CMS configuration page. You can skip this step and use the default administrator account to configure CMS configuration page.

```
ruby @ cmslinux

Local User

(x) Create New User
  User's Full Name
  Username
  Password
  Confirm Password
  [ ] Use this password for system administrator
  [ ] Automatic Login

( ) Skip User Creation

[Help] [Back] [Abort] [Next]

F1 Help F8 Back F9 Abort F10 Next
```

12. In the next screen, you need to create root's password. Click **Next**.

```
ruby @ cmslinux

Password for the System Administrator "root"

Do not forget what you enter here.

Password for root User
Confirm Password

Test Keyboard Layout

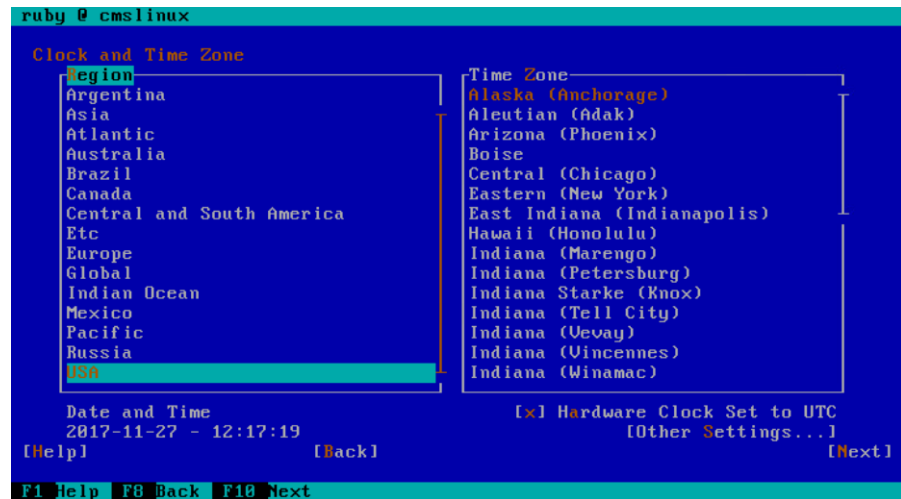
[Help] [Back] [Abort] [Next]

F1 Help F8 Back F9 Abort F10 Next
```

Installing the OpenScape Contact Media Service

Optional post-installation optimization parameters

13. In the next screen, select your region and time zone, then click Next to finish the installation process, the system will reboot automatically. Remove the DVD from the DVD drive and the system will boot from hard disk. The installation process is completed after the system reboots.



2.4 Optional post-installation optimization parameters

1. RTP ports

With this parameter you can change the default number of RTP.

The default number of RTP ports is 2000, with each call consuming 2 RTP ports. A call involving agent interaction requires 4 RTP ports.

If you need to modify the maximum number of RTP ports, edit the file:

```
/opt/Core/application_host/providers/streaming-mps/  
mfw.component.xml
```

And adjust the `<numRtpPorts>` tag to the desired value.

```
<streamingRoutes>  
  
<streamingRoute id="default">  
  
<icmpMonitoringEnabled>true</icmpMonitoringEnabled>  
  
<icmpRecoveryTime>10</icmpRecoveryTime>  
  
<icmpUnreachableCount>200</icmpUnreachableCount>  
  
<ipAddress>192.168.246.146</ipAddress>  
  
<numRtpPorts>2000</numRtpPorts>
```

```
<rtpPortRangeStart>20000</rtpPortRangeStart>  
</streamingRoute>
```

A restart of the Contact Media Service is required after each change.

Each call requires 4 RTP ports, which affects the total number of concurrent calls the CMS can handle. For example, **2,000 ports allow up to 500 concurrent calls**.

- There is no strict minimum or maximum limit. However, the number must be at least 4 to allow one concurrent call.
- We recommend **setting this to at least 2,000 ports** (which is the default) to ensure optimal performance.

2. Java Heap

This parameter changes the default Java heap maximum, which is by default set to 3 GB.

If needed, this value can be modified in the
`/opt/cmsserver.service` file.

To change the Java heap maximum update the `-Xmx3072m` value in the `ExecStart` directive to the desired amount.

However, please make sure that the specified value is smaller than the total machine memory, as a portion must be reserved for the operating system.

```
Environment=PATH=/sbin:/usr/sbin:/usr/local/sbin:/root/  
bin:/usr/local/bin:/usr/bin:/bin:/opt/Core/  
application_host/bin:/usr/lib64/jvm/temurin-8-jre/bin/  
  
ExecStart=/usr/bin/java -Xmx3072m -  
Dfile.encoding=en_US.UTF-8 -Dlog4j2.formatMsgNoLookup=true  
-jar /opt/Core/application_host/bin/apphost-starter.jar  
daemon  
  
ExecStop=/usr/bin/java -jar /opt/Core/application_host/bin/  
apphost-starter.jar exit
```

A restart of the Contact Media Service is required after each change.

The JVM maximum heap size depends on the available memory of the host system.

- **Minimum required:** At least **3GB (3072 MB)**.
- **Maximum limit:** Must be at least **2GB (2048 MB)** lower than the total host memory.
- **Recommendation:** Leave some extra memory available for system stability.

3. Recording Files Deletion

Installing the OpenScape Contact Media Service

Optional post-installation optimization parameters

This parameter determines the number of recordings deleted per hour.

If recording is enabled, a maintenance process runs hourly, removing a set number of old recordings, once the recording partition reaches its limit.

If the number of recordings per hour is greater than the number of recordings to be removed this value should be adjusted.

If necessary, to modify the number of old recordings deleted per hour, edit the `/opt/cms/cms-database.json` file and change the `diskCleanupMaxFiles` value accordingly.

A restart of the Contact Media Service is required after each change.

The number of recordings processed during cleanup should be based on the customer's call volume.

- The cleanup threshold **must be higher than the average number of calls per hour**.
- A higher threshold ensures that recordings are deleted at the same rate they are created, preventing disk space issues.
- If the threshold is too low, the system may not free up disk space quickly enough.

3 Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

This chapter describes how to configure the integration between OpenScape Contact Media Service and Mitel CX.

3.1 Prerequisites:

Before proceeding with the integration of Contact Media Service (CMS) and Mitel CX, ensure that the following prerequisites are met:

- Installation of CMS and MiCCB
- Both OS CMS and Mitel CX must be installed and properly configured on their respective platforms.
- Network connectivity must be stable.
- Adequate administrative rights for both systems.

Once these prerequisites are met, the integration process can proceed as outlined in the following sections.

3.2 Logging in the OpenScape Contact Media Service

Open a Web browser and type the following URL:

`https://<servername>:<HTTPS port>/cms`

where `servername` is the IP address or host name of the OpenScape Contact Media Service server machine, and `HTTPS port` is the port number used by the Configuration Portal of CMS. The default value is 7443.

After accessing the Contact Media Service Web page, fill in your credentials and click **Submit**.

The default credentials are:

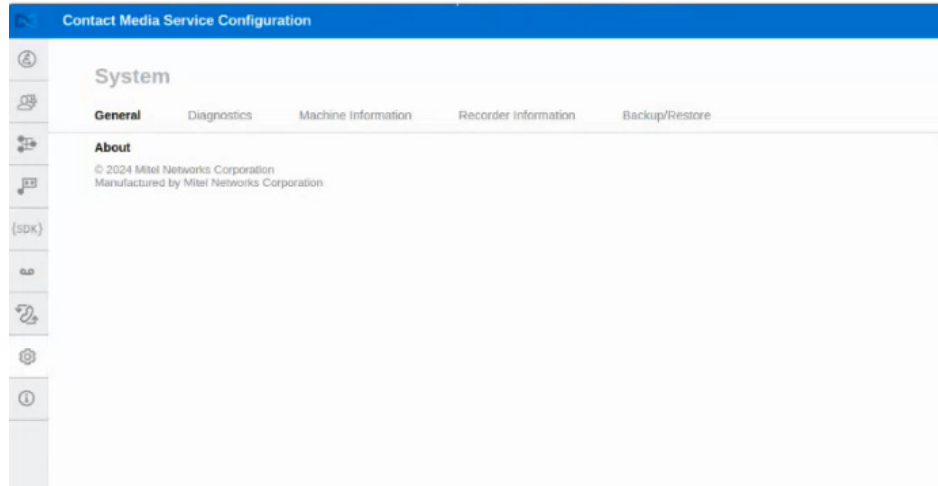
Username: administrator

Password: Asd123!.

NOTE: It is recommended to change the credentials after deployment to enhance security.

3.3 Configuring the OpenScape Contact Media Service for SIP Platforms

The starting page of the OpenScape Contact Media Service is the following



Additionally, in the top line there are two buttons:

- **Restart Service:** Click this button to restart the Contact Media Service.
- **Logout:** Click this button to logout from the configuration page.

3.3.1 VoIP Configuration

1. Click on the icon:



2. Click on the **SIP Configuration** tab. Here you can configure the Communication Platform, the Transport Type and the local SIP Port.

NOTE: You must configure either a single Communication Platform (for non-redundant SIP Server) or a DNS SRV (for SIP Server redundancy support) by checking the **Use DNS SRV** option. The chosen configuration will be applied for all CMS features.

If the SIP Load Balancer is used, the Address / FQDN field must be configured with the IP Address of the SIP Load Balancer as the SIP Server.

3. In the **Communication Platform** area set up the following parameters:
 - 3.1 In case the **Use DNS SRV** option is unchecked:
 - **Address / FQDN:** IP address or FQDN of the primary SIP Server (mandatory)

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

- **Port:** Port address of the primary SIP server (default 5060 for UDP and TCP and 5061 for TLS / mandatory).

3.2 In case the **Use DNS SRV** option is checked:

- **FQDN:** DNS SRV FQDN of the SIP Server (mandatory).
- **Port:** Port address of the DNS SRV of the SIP server (default 0 / mandatory).
- **Keep Alive Request (seconds):** Interval between SIP OPTION requests (default value: 30 seconds / mandatory).
- **Fallback to Master SIP Server Time (seconds):** The time interval at which OSCMS should check if it is able to reconnect to the master SIP Server after a Communication Platform switch over (default value: 10 seconds / mandatory).

NOTE: It is recommended to use the value of 30 seconds for Keep Alive Request and 10 seconds for Fallback to Master SIP Server Time parameters. Please double-check these values after restoring a backup from an older OSCMS release.

3.3 Set up the following parameters regardless of whether the **Use DNS SRV** option is checked or not:

- **Registration timer (seconds):** Expiry time of the registration in seconds (default value: 300 seconds / mandatory).
- **Generate 180 RINGING:** Some Communication Platforms could request the optional "180 Ringing" SIP message to be generated when a call arrives at the media server port due to call conciliation or such. When not technically necessary, keep it unchecked.
- **Allow Unknown Party Requests:** You need to check this parameter if you want to accept SIP INVITE requests for new calls from multiple SIP Trunks (this parameter is always checked when DNS SRV is enabled).

IMPORTANT: If SIP Load Balancer is used to integrate CMS with OpenScape 4000, this parameter must be checked.

4. In the **Transport Type** area select one of the following types:

- UDP
- TCP
- TLS

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

5. The **Local SIP Port** parameter indicates the port which will be used as local port for the outgoing SIP requests (default 5060 for UDP and TCP and 5061 for TLS / mandatory).
6. The **Local SIP IP** parameter is used to connect to the communication platform or PBX using a different IP address. This means that if you have two IP addresses, one can be dedicated solely for SIP connections. You must then specify which IP address should be used.
7. Click the **Payload Configuration** tab.
8. In the **SRTP Settings** area select one of the following options:
 - **Nonsecure Only (default)**
 - **Secure Only.** When selecting this option, a new **Security Protocol** area appears. Select one or more of the following protocols:
 - MIKEY
 - SDDES
 - DTLS. Use this protocol only for endpoints.
 - **Secure Preferred.** The same with **Secure Only** option.
9. In the **Audio Codecs** area, select one or more codecs to enable.
 - opus
 - G.722-1 (rate=16 kHz; bitrate=32000)
 - opus (maxplaybackrate=24000;sprop-maxcapture=24000)
 - G.722-1 (rate=32kHz; bitrate=48000)
 - G.722
 - G.711U (PCMU)
 - G.711A (PCMA)
 - G.729
 - G.729 (annexb=no).
10. In the **Video Codecs** area, select one or more codecs to enable the WebRTC Video and Screen Sharing feature.
 - VP9
 - VP8

11. Click **Save** to apply your settings.

NOTE: DTMF (Dual Tone Multi Frequency) tones are generated when callers press touch-tone keys on their phone's keypad, for example to enter a number or to select a menu, after a call has been established. These DTMF tones can be signaled to Contact Media Service in different ways. Contact Media Service supports:

In-Band RTP

The DTMF tones are part of the RTP audio stream. When a compression codec is used, these tones can be eventually distorted and Contact Media Service will not detect them. Use a codec without compression instead.

RFC4733 (only for DTMF) / RFC2833

The DTMF tones are taken out of the RTP audio stream and signaled to Contact Media Service in a separate RTP stream.

3.3.2 Users Configuration

1. Click on the icon:



2. In this area, you can change the user's password. The username is non-editable.
3. Click on the edit button (pencil).
4. Fill in the new password and confirm it one more time.
5. Click **Save** to apply your changes.

3.3.3 Networking Configuration

1. Click on the icon:



2. In this area you can set up your network.
3. Select the IP address type:
 - IPv4
 - IPv6

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

- IPv4 + IPv6
4. In the General Settings, configure the following parameters:
 - **Hostname:** The name of the host.
 - **Primary DNS:** IP address of the primary DNS server (editable if DHCP not enabled).
 - **Secondary DNS:** IP address of the secondary DNS server (editable if DHCP not enabled).
 - **Primary NTP server:** IP address of the primary NTP server.
 - **Secondary NTP server:** IP address of the secondary NTP server.
 - **HTTPS Port:** port number used by the Configuration Portal of CMS.
 5. In the **IPv4** area, if enabled, configure the following parameters:
 - **DHCP settings:** Indicates whether DHCP is enabled. Default: checked.
 - **IPv4 Address:** Editable only when DHCP is not enabled.
 - **Subnet Mask:** Editable only when DHCP is not enabled.
 - **Default gateway:** Editable only when DHCP is not enabled.
 6. In the **IPv6** area, if enabled, configure the following parameters:
 - **DHCP settings:** Indicates whether DHCPv6 is enabled. Default: checked.
 - **IPv6 Address:** Editable only when DHCPv6 is not enabled.
 - **Subnet Mask:** Editable only when DHCPv6 is not enabled.
 - **Default gateway:** Editable only when DHCPv6 is not enabled.
 7. In the **Media Interface** are, select whether IPv4 or IPv6 will be used for the SIP/RTP interface:
 - IPv4 (Default)
 - IPv6 (Default only when IPv4 is not configured.)
 8. Click **Save** to apply your settings.

3.3.4 Security Configuration

1. Click on the icon:



Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

2. Click on the **Security Credentials** tab. Here you can configure the credentials for the connection of the Mitel CX Server to Contact Media Service.
3. Click on the **Certificates** tab. Here you are able to upload different types of certificates.
 - **HTTPS Certificates**
 - CA Certificate: it is possible to Select File to load the certificate.
 - Public Certificate - it is possible to Select File to load the certificate.
 - Private Key - it is possible to Select File to load the certificate.
 - **TLS Certificates for RPC interface**
 - CA Certificate: it is possible to Select File to load the certificate.
 - Public Certificate - it is possible to Select File to load the certificate.
 - Private Key - it is possible to Select File to load the certificate.
 - **SIP/TLS Certificates for connection to OpenScape Voice**
 - CA Certificate: it is possible to Select File to load the certificate.
 - **gRPC Certificates for connection to Mitel CX**
 - Keystore - contains the private key and certificate used by the OS CMS to prove its identity. The keystore file can be a PEM, PKCS12 or JKS file. Select File to load the certificate.
 - Truststore - contains trusted CA certificates used by client to verify the server's certificate. The truststore file is a PEM file and shall be imported to both the OS CMS (server side) and the Mitel-CX (client side). Select File to load the certificate.
4. Click on the **gRPC Configuration** tab. Here you can enable the connectivity between OS CMS server and Mitel CX server. Secure gRPC link works with TLS in a Server-Client topology.

To set a secure gRPC path, we must provide the correct certificate and private key files to both the OS CMS (server side) and the Mitel-CX (client side).

In order to configure the TLS for gRPC, follow the next steps:

Step1. Create the required files for configuring TLS for gRPC:

There are several ways to create security files. It's presented the following procedure to create security files with OS CMS, using openssl:

1. Create a Certificate Authority (CA)

Step 1.1: Generate a private key from CA

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

```
openssl genpkey -algorithm RSA -out ca.key
```

Step 1.2: Create a self-signed certificate

```
openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt
```

In this case, a valid certificate for 10 years (3650 days).

2. Create a CSR for OS CMS

Step 2.1: Generate a private key

```
openssl genpkey -algorithm RSA -out server.key
```

Step 2.2: Create a CSR based on a private key

```
openssl req -new -key server.key -out server.csr
```

3. Assign CSR with CA to create a certificate for OS CMS

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 365 -sha256
```

In this case, create a certificate valid for 1 year (365 days).

4. Add Keystore (keys plus server certificate)

The keystore is used by OSCMS gRPC server to authenticate identity with MiCC-B client.

```
cat server.key server.crt > keystore.pem
```

5. Truststore (CA cert)

The truststore is used to store trust certificates. MiCCB-B gRPC client used the truststore to validate OS CMS certificate.

```
cat ca.crt > truststore.pem
```

NOTE: In the case you have multiple OS CMS servers, you must create one separate keystore file for each server. The truststore file must be the same for all servers.

NOTE: When creating a keystore file (steps above 2, 3 and 4), be sure that Common Name receives the IP or FQDN used by Mitel-CX.

Step 2: Update files to OS CMS

1.Login to the OS CMS Web page, with `https://<CMS address>:7443/cms`, and go to **security configuration**.

2.Go to Certificates and import keystore and truststore files. Choose the files and save.

3. You will receive a warning message that CMS must be restarted. You can click on **Restart Later**.

Step 3: Enable gRPC TLS on OS CMS

1. Go to **Security Configuration** and **gRPC Configuration**

2. Enable TLS

3. Enter the keystore Password (optional). This challenge password is optionally created when generating a x509 certificate to OS CMS. (see [Assign CSR with CA to create a certificate for OS CMS](#))

- The TLS encryption needs to be enabled in the Mitel CX server. Follow the steps listed in the Mitel CX Installation Guide.
- Click **Save** to apply your settings.
- You will receive a warning message that CMS must be restarted. You shall click to **Restart Now**.

3.3.5 SDK Configuration

This configuration allows you to integrate OS CMS with Mitel CX.

Configuration

1. Click the icon



In the **CTI Configuration** area, configure the following mandatory parameters:

- **CTI Type:** Select **MiCCB SDK** to enable the integration of OpenScape CMS with Mitel CX via the SDK.

This operation will disable all the tabs that are not needed for Mitel CX from the left side of the configurations menu.

- **MiCCB SDK address:** The IP address allowing you to access the Mitel CX server. For example: `http://10.8.2.5`

NOTE: If the system is running with https, add the FQDN of the system. In this case, Mitel CX needs to be configured as SSL.

- **Client ID:** The name of the Client ID needs to be the same as the Client ID in Mitel CX.
- **Encrypted Secret:** The client secret token created when the MiCC Setup -> Manage Client Credentials is rotated on the Mitel CX Server.

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

- **Impersonate admin:** The name of the agent/supervisor with which the Mitel CX will login to the OS CMS.
- **Refresh Employees Timeout (min):** The OS CMS will check the employee configuration and see if there is a new employee. By default is set to 30 minutes.
- **Synchronize Prompts:** The synchronization of CTI information for recordings.
- Click **SAVE**

3.3.6 Recorder Configuration

Requirements

The basic Recording functionality is available for Mitel CX. The system will start recording all the calls from monitored Mitel CX extensions.

Configuration

1. Click the icon



2. Click the **Recording** tab
3. In the **Recording** area, there is the following option in Recording Mode: **ANCHOR (available for Mitel CX)**.

Configuration Recording Mode: ANCHOR

1. Configure the following parameters:
 - **Recorder Enabled:** Check this flag to enable the recorder system in Contact Media Service.
 - **Encoding Extension:** Select the encoding mode from the drop-down menu. The available values are: ogg, wav
 - **Disk Cleanup Threshold (20% - 80%):** This parameter indicates the minimum percentage of free disk space for cleaning mechanism to start. Default value: 20
 - **Minimum Call Duration [s]:** This parameter defines the minimum duration of a call to be stored as recorded in seconds. Default value: 5
 - **Save:** Click **Save** to enable the recorder. You must restart Contact Media Service to enable the functionality.

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

2. Click the **Monitored Extensions** tab. This is the area where all agent extensions, which need to be recorded, are defined. Here you have the options to add a range of extensions, to remove all extensions or individual extensions and check the status of the monitored extensions.
 - Click **+Add extensions**: A pop-up window **Add device** appears, where you add a range of extensions:
 - **From**: The lower part of the extensions' range
 - **To**: The upper part of the extensions' range
 - **Mode**:
 - Full Time**: For extensions that are monitored all the time and generating a recording file for all calls received.
 - NOTE**: Agents with permission to start/stop recordings can interrupt the recording event if configured as Full Time.
 - On-Demand**: For extensions that will generate recordings only if the Agent with permission to start/stop recordings will be able to control when the call is recorded.
 - Click **Save** to add your device. Your device is now part of the list of extensions that will be recorded/monitored
 - Click **-Remove all extensions** to delete all extensions on the list
3. Click the **Client Credentials** tab. Here you can find a list of clients with their credentials. You can add a new client and remove all clients. To add a new client:
 - Click **+Add**. A pop-up window **Add Client Credentials** appears. Configure the following parameters:
 - **Client id**: The client identification. This is a mandatory field
 - **Client secret**: The pair of Client Id used for authentication. This is a mandatory field
 - **Expiration time (min)**: Time in minutes, in which the API token will be valid. This is an optional field. When the value of the parameter is 0, it means that the time is unlimited. The value must be a positive number and the recommendation is to use a timeout value for security reasons. Use 0 only for special instances.
 - **Delete recordings permission**: This flag indicates whether you can delete recordings
 - Click **SAVE** to save your entries and add the client's credentials on the list
 - Click **-Remove all** to remove all your entries
 - Click the Edit icon to modify your entries. Select the entry you want to modify and click the icon

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

4. Click the **Database** tab
5. In the Database Configuration area, configure the following parameters:
 - **Username** (dbUser): The user that can access the Postgres Database.

NOTE: This configuration will not be visible to the user. Default value: postgres

 - **Password** (dbPassword): The encrypted postgres user password

NOTE: This configuration will not be visible to the user. Default value: CmsDbAdmin!

 - **Delete records older than:** The time the recorded calls will be kept by the system before being automatically deleted. The available values from the drop-down menu: 6 months, 1 year, 2 years, 3 years, 4 years and 5 years.
 - Click **SAVE**
6. Click the **Backup** tab
7. In the **Backup** area, configure the following parameters:
 - **Backup Enabled:** Check this flag to enable backup
 - **Backup Media Threshold Alert (%):** The percentage of the disk which will trigger an alert, indicating that the disk must be changed
8. In the **Network Configuration** area, configure the following mandatory parameters:
 - **IP Address:** The IP address of the Backup server
 - **Folder:** The shared folder in the Backup server
9. In the **Network Credentials** area, configure the following parameters:
 - **Domain:** The domain of the Backup server
 - **Username:** The username to login to the Backup server
 - **Password:** The password to login to the Backup server
 - Click **SAVE**
10. In the **Network Folder Status** area, the parameter **Status** indicates whether the backup service has been initialized
11. Click the **Recovery** tab

12. In the **Recovery** area, configure the following parameters:

- **Start Date:** The initial date for starting the recovery service. This is a mandatory parameter
- **End Date:** The last date of the recovery. This is an optional parameter

13. In the **Network Configuration** area, configure the following mandatory parameters:

- **IP Address:** The IP address of the Backup server
- **Folder:** The shared folder in the Backup server

14. In the **Network Credentials** area, configure the following parameters:

- **Domain:** The domain of the Backup server
- **Username:** The username to login to the Backup server
- **Password:** The password to login to the Backup server

15. Click **SAVE**

NOTE: The configuration of the system is stored into the Contact Media Service configuration database, which is a JSON file stored in `/opt/cms/cms-database.json`

3.3.7 IVR Configuration

1. Click on the icon:



In the integration with Mitel CX, IVR configuration refers to setting up the voice portal. The OpenScape Contact Media Server delivers IVR functionality using a media server with Speech Recognition (ASR) and Text-to-Speech (TTS). These ASR and TTS capabilities are enabled through integration with Google Cloud Platform (GCP STT/TTS).

In order to use ASR or TTS functionality, follow the next steps:

1. Create credentials on the Google Cloud platform.
2. Choose the GCP Credentials (Import the json file)
3. Click **Save**

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for SIP Platforms

- You will receive a warning message that CMS must be restarted. You shall click **Restart Now**.

3.3.8 System

1. Click on the icon:



2. Click on the **General** tab.
 - In the **About** area, you get Copyright information.
3. Click on the **Diagnostics** tab.
 - **Level**: Select from: Debug, Info (Default), Warning, Fatal.
 - **Number of files**: Default is 13.
 - **Download Diagnostics**: A link to initiate the download of the diagnostics files.
 - Click **Save** to apply your settings.

NOTE: The maximum number of files that can be configured is 13. The total number of files will always increase by one, which corresponds to the file being written at the time.

4. Click on the **Machine Information** tab. Here you get data about Software version, CPU information, Memory information, Disk information and Running Since.
5. Click on the **Backup/Restore** tab. A backup and a restore of the configuration is possible.
 - **Download backup**: A link to initiate the download of the configuration backup files.
 - **Restore**: Select a file to restore a previous configuration.
6. Click **Save** to apply your settings.

3.3.9 System Messages

1. Click on the icon



2. In this area alarms and system messages are presented.

3.4 Configuring the OpenScape Contact Media Service for MiVB Platform

3.4.1 Integration with GCP for TTS and ASR

3.4.1.1 uniMRCP Configuration

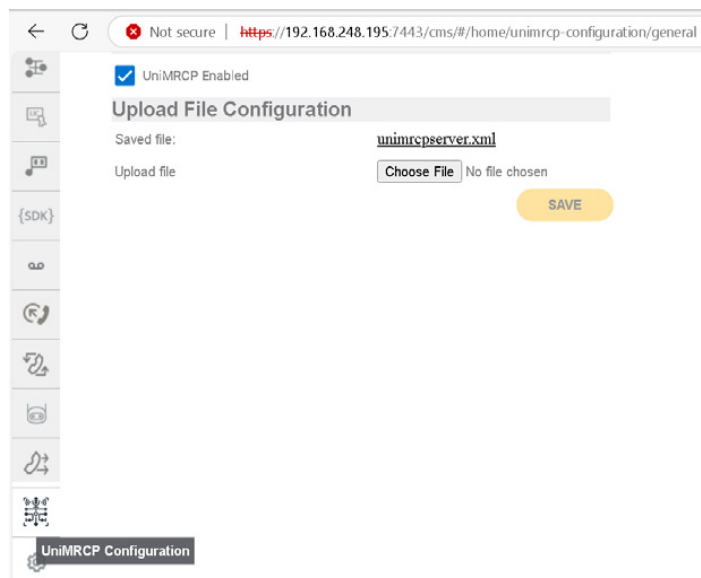
The uniMRCP server with the corresponding GCP plugins must be enabled in CMS. When the uniMRCP Enabled checkbox is checked, the uniMRCP container is started in CMS. The uniMRCP server is configured using an XML file, as described in <https://unimrcp.org/manuals/pdf/ServerConfigurationManual.pdf>.

By default, a configuration file is already loaded in CMS and will work without changes.

The user can select a file to import into CMS, which will then be imported into the container and applied to uniMRCP. Multiple files cannot be kept in CMS; only the latest uploaded file will be used for the uniMRCP configuration.

If a parameter must be manually set, for example the IP address of the uniMRCP server:

1. Navigate to the Upload File Configuration screen.



Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for MiVB Platform

2. In the **Upload file** field, click the **Choose File** button to search and select the XML file (unimrcpserver.xml).

3. Click **Save**.

When the new file configuration is saved, the uniMRCP container is restarted in CMS.

To download the currently configured file,

1. In the **UniMRCP Configuration** screen, select the **Upload File Configuration**.

2. In the **Saved file** field, click on the XML file.

The currently configured file gets downloaded.

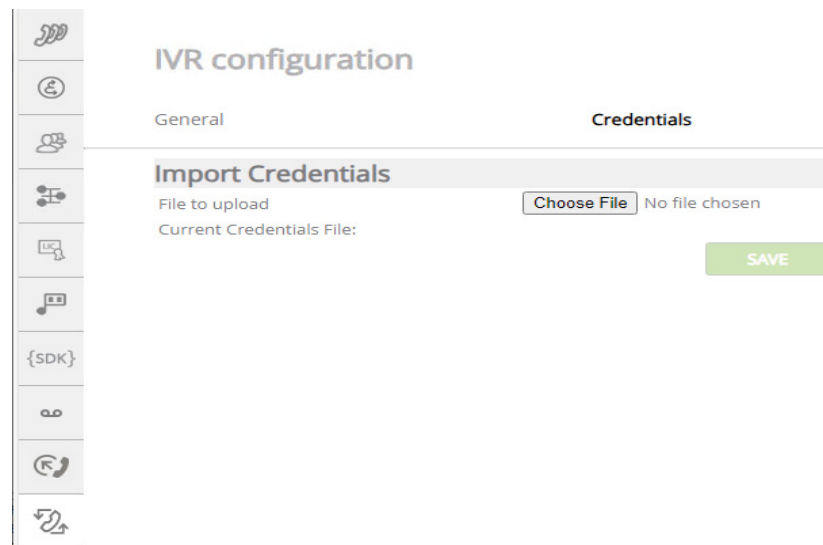
3.4.1.2 GCP Authentication

GCP creates credentials for the authentication on the Google CCAI API endpoints. The GCP credentials can be uploaded to CMS. This screen will be available if uniMRCP is enabled in CMS.

NOTE: Before creating the GCP credentials, ensure that the Speech-to-Text API and Text-to-Speech API are active in GCP.

To import the GCP credentials,

1. In the IVR Configuration screen, click the Choose File button to search and select the JSON file.



The screenshot shows the 'IVR configuration' interface. On the left is a vertical sidebar with icons for various settings. The main area is titled 'IVR configuration' and has two tabs: 'General' and 'Credentials'. The 'Credentials' tab is active. Below the tabs, there is a section titled 'Import Credentials'. It contains a 'File to upload' field with a 'Choose File' button and the text 'No file chosen'. Below that is a 'Current Credentials File:' label. At the bottom right of this section is a green 'SAVE' button.

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for MiVB Platform

2. Click **Save**.

When the configuration of the credentials is saved, the uniMRCP container is restarted in CMS.

3.4.1.3 Speech Recognition Configuration

Some parameters allow the refinement of the integration with GCP for Automatic Speech Recognition (ASR).

To configure the **Detector Sensitivity Level** parameter for ASR,

1. Navigate to UniMRCP Configuration screen.

The screenshot shows the 'Contact Media Service Configuration' interface. On the left is a vertical sidebar with various icons. The main area is titled 'UniMRCP Configuration' and has two tabs: 'General' and 'ASR'. The 'ASR' tab is selected. Below the tabs, there is a section titled 'Settings ASR'. Inside this section, there is a text input field labeled 'Detector Sensitivity Level' with the value '255' entered. To the right of this field is a yellow 'SAVE' button. At the bottom of the sidebar, there is a button labeled 'UniMRCP Configuration'.

2. Configure the following parameter:
 - **Detector Sensitivity Level** - defines the minimum sensitivity level that is acceptable on the uniMRCP server side.

Setting Up the Integration Between OpenScape Contact Media Service and Mitel CX

Configuring the OpenScape Contact Media Service for MiVB Platform

4 Quality of Service in OpenScape Contact Media Service

To configure the Quality of Service in CMS, you must access the OpenScape Contact Media Service remotely via SSH and get root permissions.

After an upgrade process, configure the parameters again, as the values are overwritten.

4.1 RTP

For the RTP stream, edit the file `mfw.component.xml` in the folder: `opt/Core/application_host/providers/streaming-mps.`

```
<mfwRoutesConfig>
<streamingRoutes>
<streamingRoute id="default">
<icmpMonitoringEnabled>true</icmpMonitoringEnabled>
<icmpRecoveryTime>10</icmpRecoveryTime>
<icmpUnreachableCount>200</icmpUnreachableCount>
<ipAddress>auto$IPv4</ipAddress>
<numRtpPorts>2500</numRtpPorts>
<rtpPortRangeStart>20000</rtpPortRangeStart>
<rtpTypeOfService>152</rtpTypeOfService>
<rtpTypeOfServiceForVideo>136</rtpTypeOfServiceForVideo>
</streamingRoute>
</streamingRoutes>
</mfwRoutesConfig>
```

4.2 SIP

For SIP you cannot configure the Quality of Service on the Media Server. The Quality of Service value is set as a rule in the Linux iptables application, which acts as an embedded firewall.

Execute the following command to create the rule:

```
iptables -t mangle -A OUTPUT -p <transport type> --sport
<Local SIP Port> -j DSCP --set-dscp <dscp value>
```

where:

- `<transport type>` can be tcp or udp. For tls, use tcp
- `<Local SIP Port>` corresponds to the port configured in:
VoIP Configuration > SIP Configuration. The default values are:

Quality of Service in OpenScape Contact Media Service

TOS/DSCP Values

- 5060 for UDP and TCP
- 5061 for TLS
- `<dscp value>` the decimal value of DSCP as indicated in [Table 1](#)

Since the iptables command is re-created every time the system is re-booted, you must add the execution of the iptables command to the startup process of OpenScape CMS.

Copy the file `sipqos.service` from the directory `/etc/system/system`. The `sipqos.service` file has the following content:

```
[Unit]
```

```
Description=OpenScape CMS - change Quality of Service
```

```
After=SuSEfirewall2_setup.service
```

```
[Install]
```

```
WantedBy=multi-user.target
```

```
[Service]
```

```
Type=oneshot
```

```
RemainAfterExit=yes
```

```
ExecStart=/usr/sbin/iptables -t mangle -A OUTPUT -p tcp --  
sport 5060 -j DSCP --set-dscp 40
```

Open the file `sipqos.service` for editing and correct the protocol, local port and dscp values if needed.

From inside the directory `/etc/system/system`, execute the following command

```
systemctl enable sipqos.service
```

From now on, when the system is re-booted, the iptables command will be executed.

4.3 TOS/DSCP Values

Use the following table as a reference for the values used in the configuration:

- For RTP use the TOS value column

- For SIP use the DSCP Dev column

DSCP Dec	TOS value
0	0
8	32
10	40
14	56
18	72
22	88
24	96
28	112
34	136
36	144
38	152
40	160
46	184
48	192
56	224

*Table 1**TOS/DSCP Values*

Index

C

configuration 17

I

installation 7, 35

