A MITEL
PRODUCT
GUIDE

Mitel OpenScape Mobile

Mitel OpenScape Mobile Pro V10

Administration Guide
12/2025

A31003-M40A0-M100-10-76A9

Notices

Trademarks

Contents

1 Introduction.. 5

2 OpenScape Mobile Pro V10 application overview........................ 6
2.1 OpenScape Mobile Pro V10 Topology.................................... 6
2.2 Configuration.. 9

3 Prerequisites... 11

4 OpenScape Communication Platform Configuration...................... 12
4.1 OpenScape Voice Configuration....................................... 12
4.1.1 How to Configure Registration of OpenScape Mobile Pro in OpenScape Voice.................................. 12
4.1.2 How to Create a PNP for OpenScape Mobile Pro Subscribers........... 13
4.1.3 How to Create an Office Code and Directory Number Range for OpenScape Mobile Pro Subscribers.. 13
4.1.4 How to Create a Number Definition Rule for the Office Code......... 14
4.1.5 How to Configure Call Forwarding - Remote Activation............... 15
4.1.6 How to Create an OpenScape Mobile Pro custom URL................... 16
4.1.7 How to Configure Quality of Service................................ 17
4.1.8 Licensing Administration... 18
4.1.8.1 How to Configure License Warning Threshold....................... 18
4.1.8.2 How to Display License Usage..................................... 19
4.1.8.3 How to Activate License Logging.................................. 20
4.1.8.4 How to Monitor Licensing... 21
4.1.9 How to Configure Digest Authentication............................. 22
4.1.10 Video calls Administration.. 23
4.2 OpenScape 4000 Configuration... 23
4.3 SBC Administration... 24
4.3.1 How to Configure the SBC Address to Enable Remote Access........... 24
4.3.2 How to configure the DNS on SBC.................................... 25
4.3.3 How to configure the certificates for SBC.......................... 25
4.3.4 How to enable Push Notifications for OpenScape Mobile Pro.......... 26
4.3.5 How to configure the Maximum registration expiry for OpenScape Mobile Pro.................................. 27
4.4 Creating OpenScape Mobile Pro Users.................................. 27
4.4.1 How to Create the OpenScape Mobile Pro Subscriber.................. 27
4.4.1.1 How to Use the General Tab....................................... 28
4.4.1.2 How to Use the Security Tab...................................... 31
4.4.1.3 Other Tabs... 32
4.4.2 How to Display the Subscriber in OpenScape Voice Configuration..... 32
4.5 Mobile Client Profiles... 32
4.5.1 MDM Key-Value Pairs.. 33
4.6 Preparing the Desk Phone for OpenScape Mobile Pro.................... 33
4.6.1 How to Prepare OpenStage Phone for OpenScape Mobile Pro............ 33
4.6.2 How to Disable Phone Hold Music.................................... 34
4.7 Configure Push Notifications for Chat messages....................... 35

5 OpenScape Voice Server-to-UC Server Configuration.................... 36
5.1 How to Configure the OSV-to-UC Interface............................. 36

6 UC-Only Configuration... 38

7 Mobile Device Wi-Fi Configuration................................... 39
7.1 What Information to send to OpenScape Mobile Pro V10 User............ 39

8 Firewall settings for OpenScape Mobile Pro V10 42

9 Known Restrictions 43
9.1 Restrictions for OpenScape Mobile Pro 43

10 Third-Party Device Information 44

11 Additional Suggestions 45

12 Error Reporting, Data collection and Diagnosis 46

13 Infrastructure Requirements and Recommendations 47
13.1 Speech Bandwidth 47
13.2 Signaling Bandwidth 47
13.3 Wireless Network Infrastructure Requirements and Recommendations 47
13.4 Voice Over WLAN RF Recommendations 47
13.5 Network Configuration Requirements and Recommendations 49
13.6 Network Performance Requirements 50
13.7 MDM Key-Value Pairs 51

14 Appendix 52
14.1 RTP Parameters 52
14.2 Key-Value Pairs 53
14.3 Glossary of Terms 54

1 Introduction

This book explains how to administer Mitel OpenScape Mobile using the Mitel OpenScape Voice Assistant.

Intended Audience

Prerequisite Knowledge

The audience for this guide is Mitel personnel, customers, or third-party service providers.

This guide is written for the user who has:

- Practical knowledge of how to configure and manage communications systems.
- Adequate administrator access rights.

2 OpenScape Mobile Pro V10 application overview

With the new solution both OpenScape Mobile Pro V10 applications (OpenScape Mobile Pro V10 for Apple Devices and OpenScape Mobile Pro V10 for Android Devices) are functional as the implementation on server side (SBC and Mitel OpenScape Voice/ Mitel OpenScape 4000) is backward compatible.

The Session Border Controller (SBC) plays the role of the provider and every OpenScape Mobile Pro V10 call passes through SBC even if the device is using the corporate WiFi network in SIP-only mixed mode.

OpenScape Mobile Pro V10 application for Apple devices supports iOS SDK 10 and CallKit. Additional features as Push notifications supported for both Apple and Android devices. In order to support that, OpenScape Mobile Pro V10 introduced changes in the OpenScape Mobile DN registration and the call flow for the reception of an incoming call to OpenScape Mobile Pro V10.

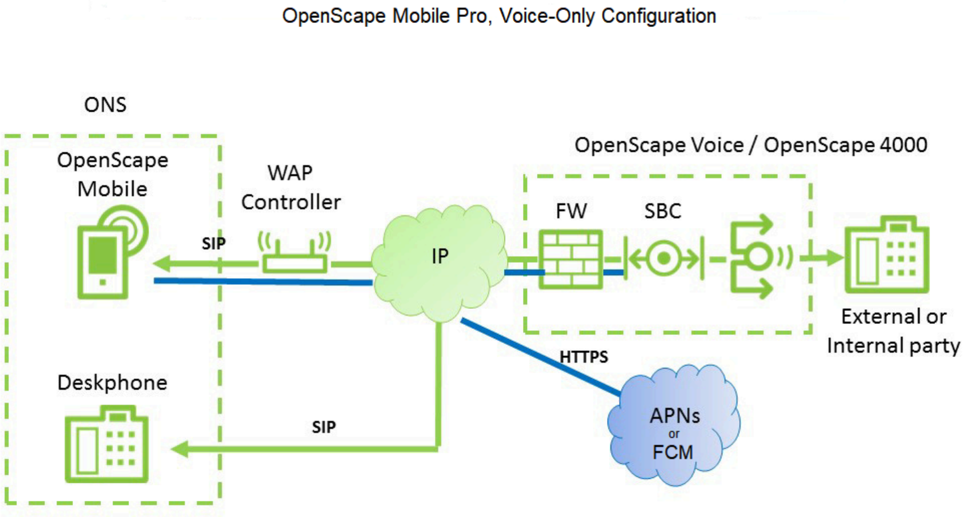
Push Notifications concept requires a service provider (SBC) to send a VoIP type message notification to either Apple (APN) or Goole Firebase (FCM) notification servers for iOS or Android operation systems respectively. Next the notification server notifies the OpenScape Mobile Pro V10 application that retrieves the call from the provider

2.1 OpenScape Mobile Pro V10 Topology

Voice-Only Configuration

The following figures illustrates the two typical deployments of the voice-only variant of OpenScape Mobile Pro V10 in an Enterprise environment. An OpenScape Mobile Pro V10 User has a desktop phone and a mobile device with the OpenScape Mobile Pro V10 Application loaded on it. The mobile device uses Wi-Fi to connect to OpenScape Voice.

OpenScape Mobile Pro V10 uses an SBC for the SIP connection independently whether the device is using a Corporate WiFi, a WiFi hotspot or Home office or Cellular network. The SBC communicates with the Apple/Google Notification Servers over HTTPs. For the OpenScape Mobile Pro V10 application, special configuration is required in the Corporate Firewall for the communication of APN/FCM servers with SBC and mobile device in Corporate WiFi is allowed. Also, the corporate firewall must be properly configured to allow SIP signaling and RTP traffic between corporate WiFi and external IP address of SBC.


OpenScape Mobile Pro, Voice-Only Configuration
ONS
OpenScape Mobile
Deskphone
WAP Controller
SIP
IP
SIP
HTTPS
APNs or FCM
OpenScape Voice / OpenScape 4000
FW
SBC
External or Internal party

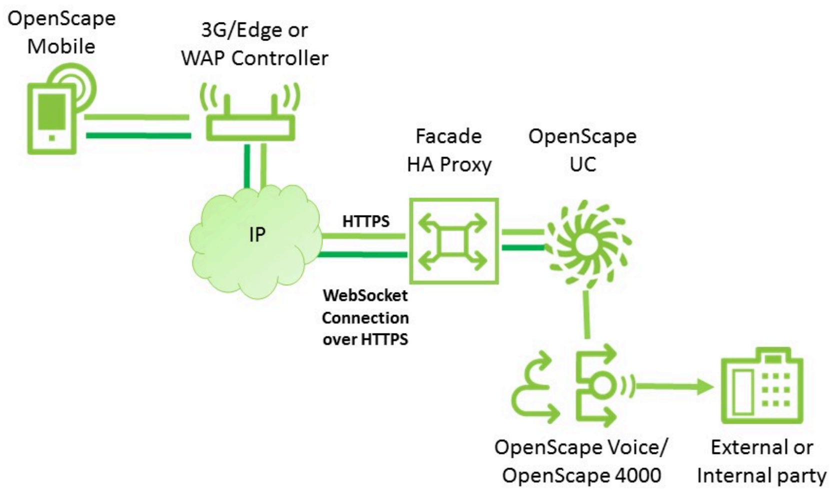
UC-Only Configuration

OpenScape Mobile Pro V10 is connected to the HAProxy Server and supports UC features like call control functionalities. However, this configuration does not support OpenScape Voice features, like for example VoIP calls.

The UC-Only mode enhancements are implemented thanks to the new interface (i.e. HAProxy) that allows clients to be notified about the call stage and perform call control requests. There is a new connection to the Even Server. As a result, the OpenScape Mobile application and UC Front-End do not communicate with each other directly, but via HAProxy. From the end-user perspective, nothing has been changed in the login process. The users still need to enter Server Address (IP address or server name) given by their System Administrator.

The following figure illustrates a typical deployment of the UC-only configuration for both Apple and Android devices:

OpenScape Mobile Pro, UC-only mode


OpenScape Mobile
3G/Edge or WAP Controller
IP
HTTPS
WebSocket Connection over HTTPS
Facade HA Proxy
OpenScape UC
OpenScape Voice/ OpenScape 4000
External or Internal party

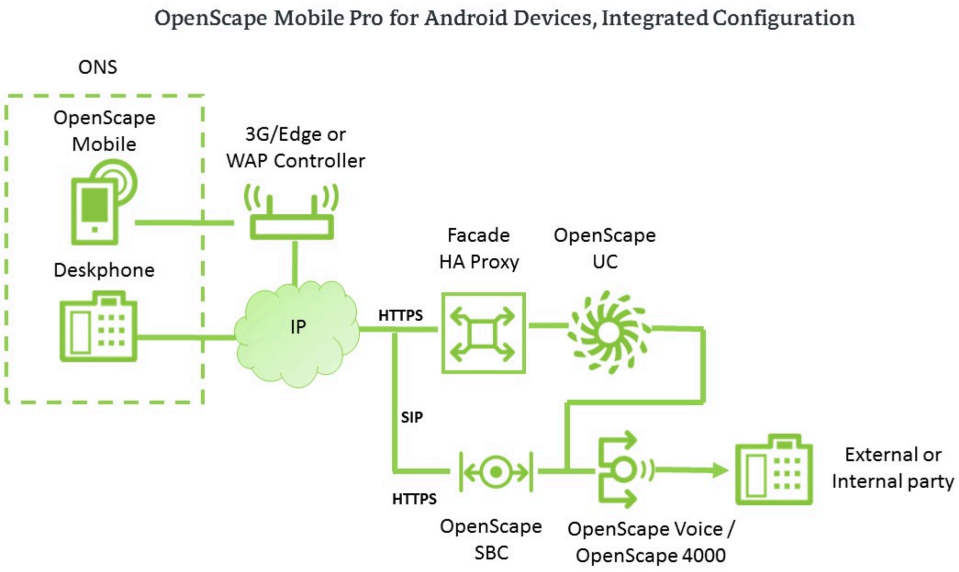
Integrated Configuration (Voice + UC)

The following figure illustrates the typical deployment of both Mitel OpenScape Mobile Pro V10 and Mitel OpenScape UC in an Enterprise environment. In this integrated configuration, the OpenScape Mobile Pro V10 Application contacts the UC Server via HTTPS and registers with the OpenScape Voice Server via SIP. The SBC communicates with the APN/FCM via HTTPs. The OpenScape Mobile Pro V10 Subscriber has a desk phone and his OpenScape Mobile Pro V10-enabled mobile phone (Wi-Fi and cellular). The OpenScape Mobile Pro V10 Application allows the subscriber to control where the call is to be received at any time.

The Integrated Configuration will also support connection to OpenScape 4000. An OpenScape Mobile client when connected to an OpenScape 4000 system will operate in the same way as when connected to an OpenScape Voice system.

Special configuration is required in the Corporate Firewall in order the Communication of APN/FCM with SBC and mobile device in Corporate WiFi is allowed. Also, the corporate firewall must be properly configured to allow SIP signaling and RTP traffic between corporate WiFi and external IP address of SBC.

The following figures illustrate these two typical deployments for Apple and Android devices respectively:


OpenScape Mobile Pro for Android Devices, Integrated Configuration
ONS
OpenScape Mobile
Deskphone
3G/Edge or WAP Controller
IP
HTTPS
SIP
HTTPS
Facade HA Proxy
OpenScape UC
OpenScape SBC
OpenScape Voice / OpenScape 4000
External or Internal party

NOTICE:

OpenScape Mobile Pro V10 client does not support connections over VPN.

2.2 Configuration

The following definitions are used:

- OpenScape Mobile Pro V10 Application - The client application running on the mobile device to provide this functionality.
- OpenScape Mobile Pro V10 User - The user of the OpenScape Mobile Pro V10 Application.
- Desk Phone Subscriber - The subscriber configured in OpenScape Voice for the desk phone.
- OpenScape Mobile Pro V10 Subscriber - The subscriber configured in OpenScape Voice for the OpenScape Mobile Pro V10 Application.

For an OpenScape Mobile Pro V10 User, two subscribers are configured in OpenScape Voice:

1) Desk Phone Subscriber - A subscriber for the desk phone. This subscriber is configured with the user’s business number. Typically with a DID number that can also be reached via extension dialing by other enterprise users.

2) OpenScape Mobile Pro V10 Subscriber - A subscriber for the OpenScape Mobile Pro V10 Application. This subscriber is configured with a number that is not published. This number is not known to the OpenScape Mobile Pro V10 User. The OpenScape Mobile Pro V10 directory number is known only to the System Administrator who associates it with the Desk Phone Subscriber.

As a result, one OpenScape Mobile Pro V10 User needs two licenses on OpenScape Voice: one dynamic license for the configured Desk Phone

Subscriber and one OpenScape Mobile Pro V10 license for the OpenScape Mobile Pro V10 Subscriber. OpenScape Voice uses the One Number Service (ONS) feature to allow the OpenScape Mobile Pro V10 Application to make and receive calls with the same number as the desk phone.

The following chapters describe in detail the OpenScape Voice configuration for the Desk Phone Subscriber and the OpenScape Mobile Pro V10 Subscriber.

3 Prerequisites

Voice Only Configuration

- Refer to the Release Notes for the minimum production versions of the OpenScape Voice Server, SBC and UC required to support OpenScape Mobile Pro V10.
- A desk phone for the OpenScape Mobile Pro V10 User. The desk phone must support “CSTA over SIP” (or “Type 1” CSTA capabilities), Call Forwarding, and Call Transfer. All Unify Desk phones and Desktop Client Personal Edition V7 support the above.
  - SBC Version **V9 R4** is the minimum required SBC version
  - UC **V9 R4** or later
  - OSV **OpenScape 4000 V8R2** or later
- Mobile devices with operating system iOS **V11 or higher**.
- A session border controller configured for TLS or MTLS for remote user access.

NOTICE:

MTLS refers to mutual TLS, that is, Mutual Transport Layer Security. It is form of TLS where the transmitting party requests the client’s credentials. If both parties can establish trust in the other then the connection is called mutually authenticated – also referred to as client authenticated. This adds another layer of security by also authenticating the client part

Integrated Configuration

- Refer to the Release Notes for the minimum production versions of the OpenScape Voice Server, SBC and UC required to support OpenScape Mobile Pro V10.
- A desk phone for the OpenScape Mobile Pro V10 User. The desk phone must support “CSTA over SIP” (or “Type 1” CSTA capabilities), Call Forwarding, and Call Transfer. All Unify Desk phones and Desktop Client Personal Edition V7 support the above.
  - SBC Version **V9 R4** is the minimum required SBC version
  - UC **V9 R4** or later
  - OpenScape 4000 v8R2 or later
- Mobile devices with operating system iOS **V11 or higher**.
- A session border controller configured for TLS or MTLS for remote user access.
- A reverse Proxy (HAProxy) configuration is mandatory for OpenScape Mobile Pro V10.

UC-Only Configuration

- Refer to the Release Notes for the minimum production versions of the OpenScape UC Server, HAProxy Server and Façade Server required to support Version 9 of OpenScape Mobile Pro V10.
- Mobile devices with operating system iOS **V11 or higher**.

4 OpenScape Communication Platform Configuration

NOTICE:

This chapter is not needed if your are deploying OpenScape Mobile Pro in a UC-Only configuration. Skip to chapter 6.

Use this chapter to configure OpenScape Mobile Pro to work with either OpenScape Voice or OpenScape 4000, depending on your configuration. The OpenScape Voice/OpenScape 4000 configuration can be broken down into the following ordered steps:

1) Setting up the environment for OpenScape Mobile Pro Users:

   a) Creating a Private Numbering Plan (PNP) for OpenScape Mobile Pro Subscribers.
   b) Creating an office code and a home directory number range for OpenScape Mobile Pro Subscribers.
   c) Creating a Number Definition and a Number Modification rule for the new office code.
   d) Configuring the SBC address, voicemail access, QoS, etc.

2) Creating OpenScape Mobile Pro Users:

   a) Enabling the user’s desk phone - Done automatically when assigning the OpenScape Mobile Pro User (e.g., CSTA access, Call Transfer).
   b) Creating the OpenScape Mobile Pro Subscriber for the OpenScape Mobile Pro Application.

3) Preparing the desk phone for OpenScape Mobile Pro.

4.1 OpenScape Voice Configuration

This chapter guides you on how to configure OpenScape Mobile Pro to connect to OpenScape Voice and set up the environment for OpenScape Mobile Pro Users.

4.1.1 How to Configure Registration of OpenScape Mobile Pro in OpenScape Voice

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

2) Click on **Administration** > **General Settings > RTP**.

3) Check the value Srx/Sip/OSMO_Extended_Register_Time and click **View/ Edit**.

   This parameter defines the registration of OpenScape Mobile Pro. The number of the value can be from 1 to 10 days. The default value is 7 days

4.1.2 How to Create a PNP for OpenScape Mobile Pro Subscribers

This private numbering plan isolates the "hidden" OpenScape Mobile Pro Subscriber numbers. No translation configuration is required in this numbering plan. All translations for OpenScape Mobile Pro calls are made in the numbering plan of the user's desk phone. All numbers in this numbering plan are private.

Prerequisites

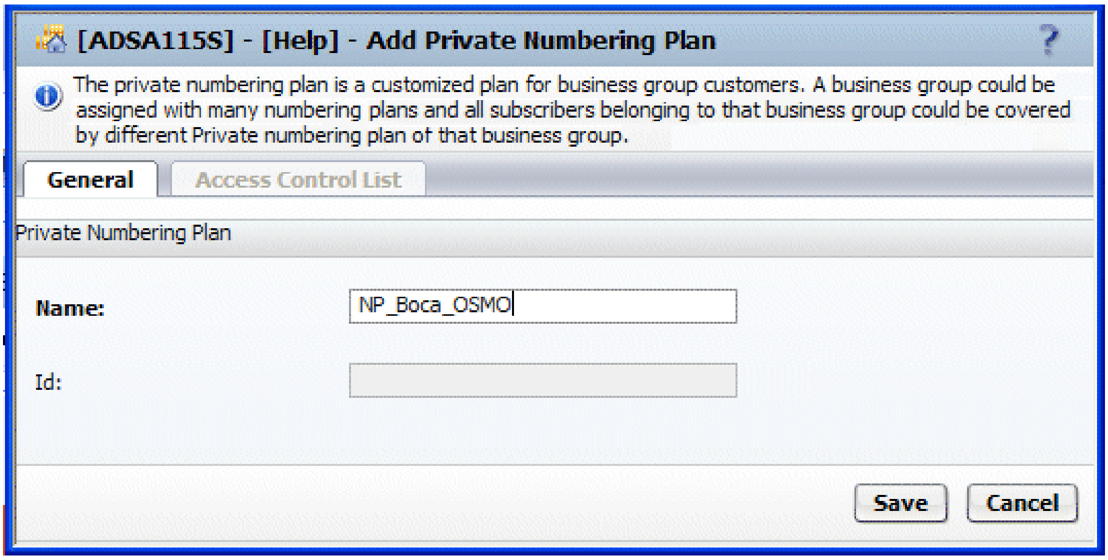
Have administration rights in Common Management Platform (CMP).

Step by Step

1) Click on **Configuration > OpenScape Voice** or tab in CMP.

2) Click on **Business Group > Private Numbering Plan List**.

3) Click on **Add** button and enter a **Name** and an **ID** for the PNP.



[ADSA115S] - [Help] - Add Private Numbering Plan

The private numbering plan is a customized plan for business group customers. A business group could be assigned with many numbering plans and all subscribers belonging to that business group could be covered by different Private numbering plan of that business group.

Private Numbering Plan

Name: NP_Boca_OSMO

Id:

4) Click on **Save.**

4.1.3 How to Create an Office Code and Directory Number Range for OpenScape Mobile Pro Subscribers

To simplify the management of OpenScape Mobile Pro Users it is recommended to use overlapping numbers for a user's desk phone and OpenScape Mobile Pro Application. For example if a user's published DID number is +1 561 923 1234 the hidden OpenScape Mobile Pro number may be configured as 993 1234. This configuration allows easily looking up both the desk phone and the OpenScape Mobile Pro Subscribers in the OpenScape Voice Assistant using a wild card (e.g., *31234).

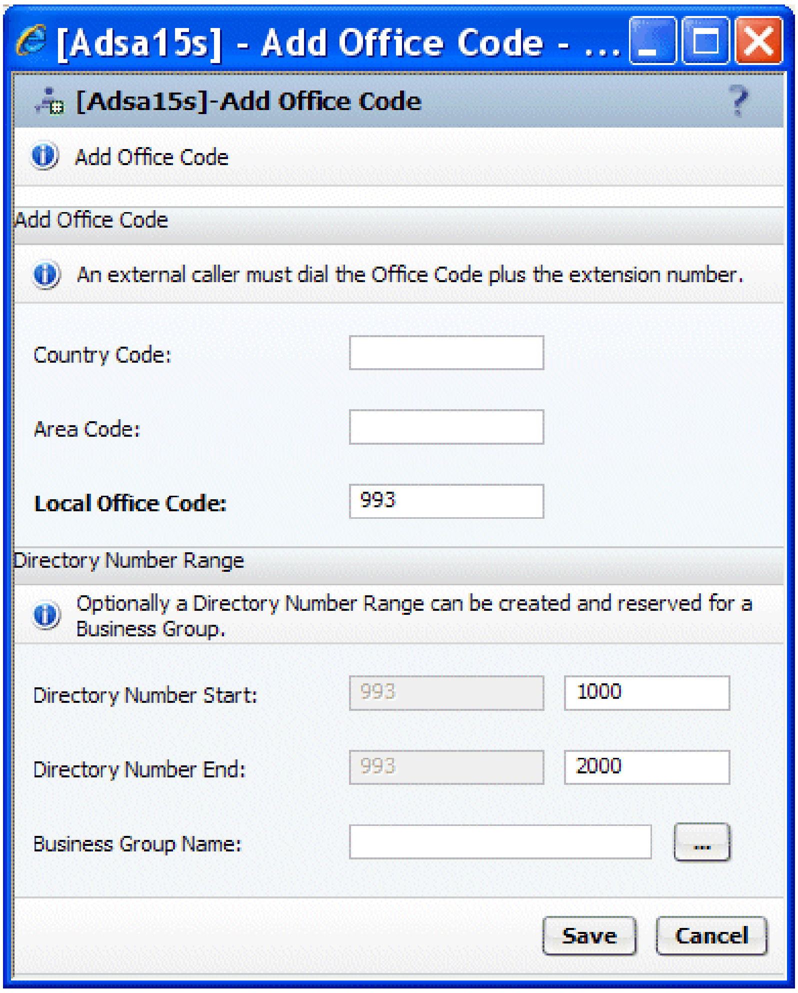
Prerequisites

Have administration rights in Common Management Platform (CMP).

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

2) Click on **Global Translation and Routing > Directory Numbers**.
3) Click on **Office Codes > Add** button.
4) Enter a **Local office code** leaving the *Country* and *Area Code* fields blank.
5) Enter the range of directory numbers to be created in **Directory Number Start** and **Directory Number End** fields and click on **Save**.


[Adsa15s] - Add Office Code - ...

[Adsa15s]-Add Office Code

Add Office Code

Add Office Code

An external caller must dial the Office Code plus the extension number.

Country Code:

Area Code:

Local Office Code: 993

Directory Number Range

Optionally a Directory Number Range can be created and reserved for a Business Group.

Directory Number Start: 993 1000

Directory Number End: 993 2000

Business Group Name:

4.1.4 How to Create a Number Definition Rule for the Office Code

A number definition rule is needed for the new office code. The example shown is that of a private office code with an L0 code of 993. It could also be created with L2 or L1 level code.

Prerequisites

Have administration rights in Common Management Platform (CMP).

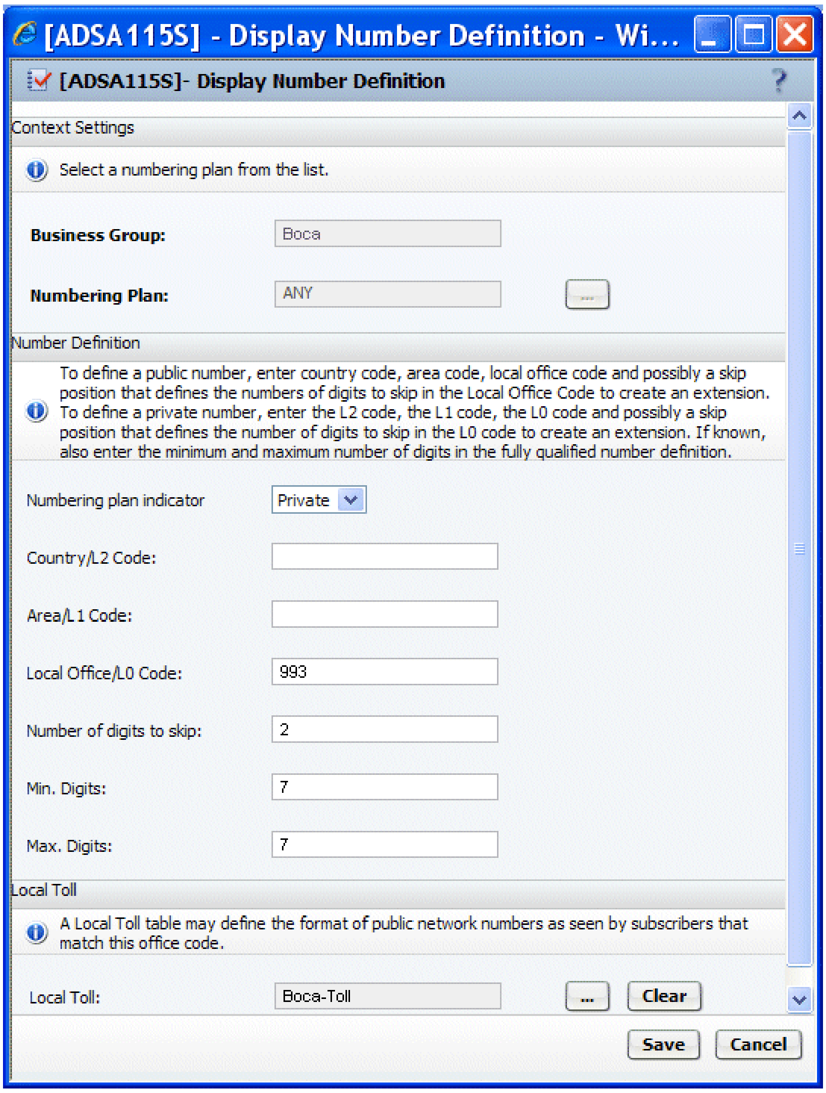
Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.
2) Click on **Business Group > Display Number Modification > Definitions**.

3) Click the ***Add*** button.

NOTICE:

The Local Toll configuration should be the same as the one used for the desk phone’s office code.


[ADSA115S] - Display Number Definition - Wi...
[ADSA115S]- Display Number Definition
?
...
Clear
Save
Cancel

Context Settings

Select a numbering plan from the list.

Business Group: Boca

Numbering Plan: ANY

Number Definition

To define a public number, enter country code, area code, local office code and possibly a skip position that defines the numbers of digits to skip in the Local Office Code to create an extension. To define a private number, enter the L2 code, the L1 code, the L0 code and possibly a skip position that defines the number of digits to skip in the L0 code to create an extension. If known, also enter the minimum and maximum number of digits in the fully qualified number definition.

Numbering plan indicator: Private

Country/L2 Code:

Area/L1 Code:

Local Office/L0 Code: 993

Number of digits to skip: 2

Min. Digits: 7

Max. Digits: 7

Local Toll

A Local Toll table may define the format of public network numbers as seen by subscribers that match this office code.

Local Toll: Boca-Toll

4.1.5 How to Configure Call Forwarding - Remote Activation

Remote activation of call forwarding (RACF) enables an OpenScape Mobile Pro User to control Call Forwarding for the ONS from his mobile device.

Configure the subscriber with the same permissions as the ONS number. The OpenScape Mobile Pro User will then be able to manage station call forwarding options and change forwarding destinations from home or from another work location.

NOTICE:

For detailed step-by-step procedures refer to OpenScape Voice Administrator Documentation, Chapter “Call Forwarding - Remote Activation”.

In summary:

Step by Step

1) Prepare the RACF access number.

2) Provision subscribers for RACF via either:

- a switch-level feature profile
- a business group-level feature profile
- or individually by subscriber.

NOTICE:

An OpenScape Mobile Pro device that is created in OpenScape Voice and it is not registered in UC, cannot redirect calls to ONS to voicemail after the default set time. The OpenScape Mobile Pro device must be connected to UC too. If this is not possible then the administrator can activate Call Forwarding Voicemail service on OpenScape Voice.

4.1.6 How to Create an OpenScape Mobile Pro custom URL

This URL can be used to invoke OpenScape Mobile Pro from external applications.

NOTICE:

The custom URL works for the following scenarios:

- OpenScape Mobile Pro is already up and running

- OpenScape Mobile Pro is in Wi-Fi mode.

Step by Step

To start a conference call using OpenScape Mobile Pro, the following line has to be integrated into the e-mail for a conference call invitation:

osmo:// callednumber [postdialdigits]

NOTICE:

The formal definition of the URL (BNF) is:

OSMO-URI = *" osmo:// " callednumber [postdialdigits]*

callednumber = gnf / telnumber

gnf = "+" 1*DIGIT

telnumber = 1*DIGIT

postdialdigits = pause 1*DIGIT "#"

pause = 1* ","

For example, add "*osmo://+15619231999,,123456*" to the email.

By pressing that line, OpenScape Mobile Pro will be invoked and it will dial the number +15619231999, wait and then dial the 123456 passcode, automatically connecting to the conference bridge.

4.1.7 How to Configure Quality of Service

The quality of service used by OpenScape Mobile Pro can be controlled using RTP parameters.

Prerequisites

Have administration rights in Common Management Platform (CMP).

When OpenScape Mobile Pro connects to OpenScape Voice, it gets the configured values and uses them for its signaling and speech network connections. QoS for the speech (RTP) is controlled using: *Srx/IpPacketPriority/DSCPTOS/RTP/Type* and *Srx/IpPacketPriority/DSCPTOS/RTP/Value*. Signaling QoS uses: *Srx/IpPacketPriority/DSCPTOS/SIP/Type* and *Srx/IpPacketPriority/DSCPTOS/SIP/Type*. (See appendix).

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

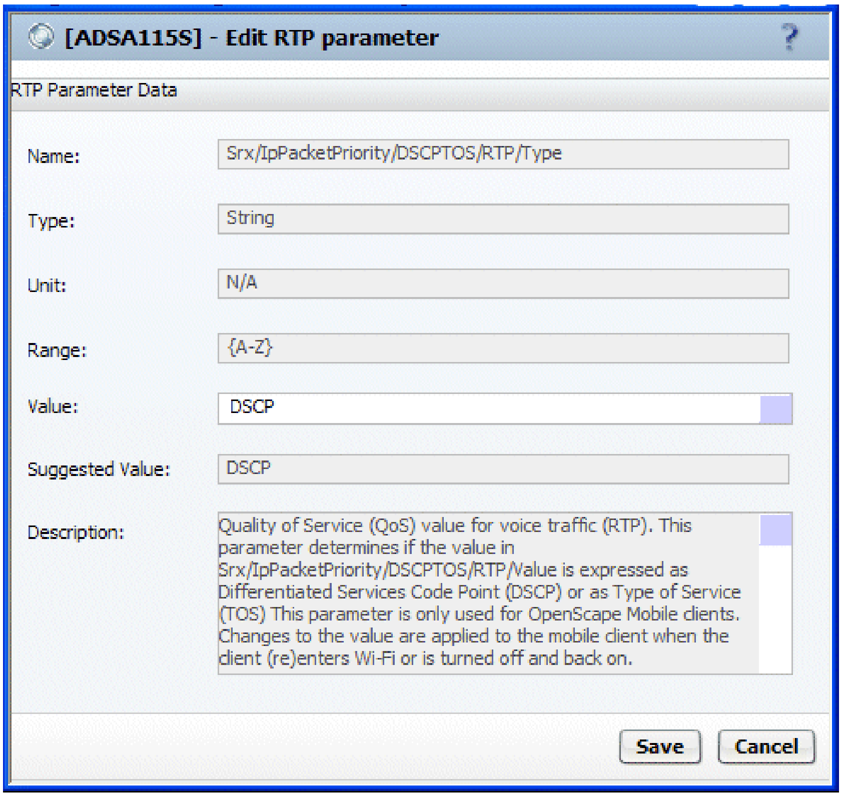
2) Click on **Administration** > **General Settings > RTP**.

3) Check the desired RTP parameter and click ***View/Edit***. (Parameter *Srx/IpPacketPriority/DSCPTOS/RTP/Type* is shown below as an example.)

4) Edit the ***Value*** field and click ***Save***.

NOTICE:

Changes to the value are applied to the mobile client when the client (re)enters Wi-Fi or the app is turned off and back on. Either action will force an initialization sequence to happen at which time the values are fetched from the server.



RTP Parameter Data

Name: Srx/IpPacketPriority/DSCPTOS/RTP/Type

Type: String

Unit: N/A

Range: {A-Z}

Value: DSCP

Suggested Value: DSCP

Description: Quality of Service (QoS) value for voice traffic (RTP). This parameter determines if the value in Srx/IpPacketPriority/DSCPTOS/RTP/Value is expressed as Differentiated Services Code Point (DSCP) or as Type of Service (TOS) This parameter is only used for OpenScape Mobile clients. Changes to the value are applied to the mobile client when the client (re)enters Wi-Fi or is turned off and back on.

4.1.8 Licensing Administration

The licensing mechanism includes an OpenScape Mobile Pro license type.

The handling of this license type closely follows the current behavior of dynamic licenses except that its count is managed separately. OpenScape Mobile Pro licenses control the number of concurrent registered clients, each reserving a single license for its DN.

If the license file does not contain an entry for OpenScape Mobile Pro then OpenScape Voice considers OpenScape Mobile Pro licensing as not being activated. License usage will operate as before (i.e., the dynamic license pool will be used to serve OpenScape Mobile Pro users).

NOTICE:

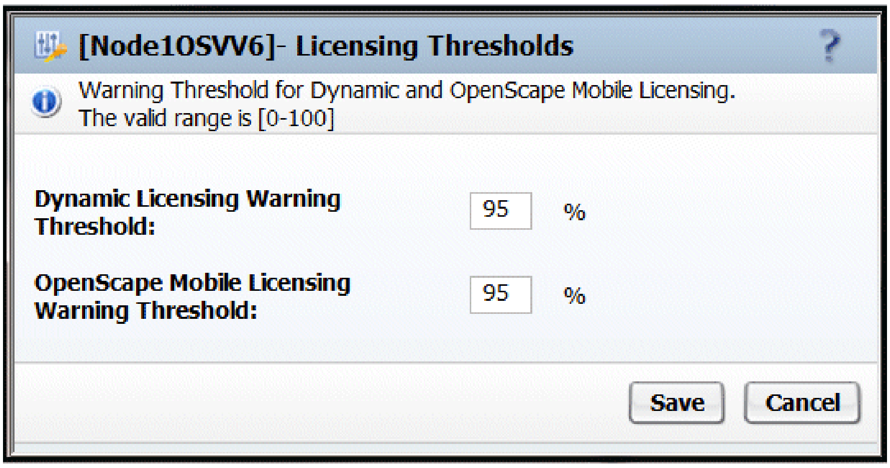
The Trace Manager is able to monitor the key performance indicator *Used OpenScape Mobile Pro Licenses*.

4.1.8.1 How to Configure License Warning Threshold

A warning is generated when the number of OpenScape Mobile Pro licenses currently in use is about to exceed the total available. The threshold at which this warning is given is configurable as a percentage of total licenses. (95% is the recommended default.)

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.
2) Click on **Licensing Management > Thresholds**.
3) Set to the desired threshold and click **Save**.



[Node10SVV6]- Licensing Thresholds

Warning Threshold for Dynamic and OpenScape Mobile Licensing.
The valid range is [0-100]

Dynamic Licensing Warning Threshold: 95 %

OpenScape Mobile Licensing Warning Threshold: 95 %

4.1.8.2 How to Display License Usage

A "snapshot" of OpenScape Mobile Pro licensing displays the following status information (read-only fields):

- The licenses assigned to the system
- Current *in use* count
- The count of maximum usage from the previous day
- Customer violations/customer violation limit.

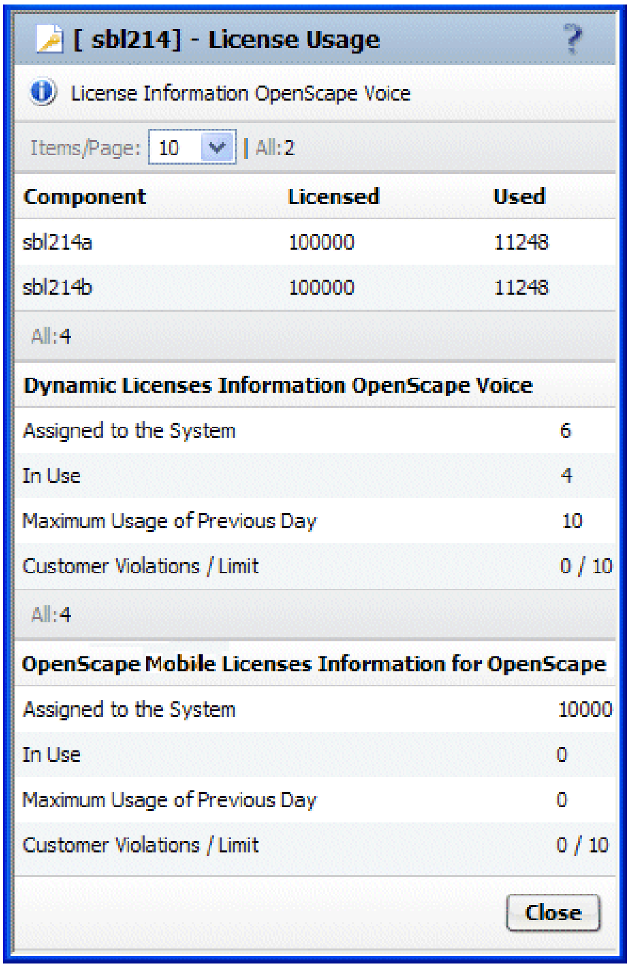
NOTICE:

If OpenScape Mobile Pro licensing is not enabled then the counters are not shown and “OpenScape Mobile Pro Licensing is disabled” is displayed instead).

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

2) Click on **Licensing Management > Usage**.



[sbl214] - License Usage

License Information OpenScape Voice

Items/Page: 10 | All:2

Component	Licensed	Used
sbl214a	100000	11248
sbl214b	100000	11248

All:4

Dynamic Licenses Information OpenScape Voice	
Assigned to the System	6
In Use	4
Maximum Usage of Previous Day	10
Customer Violations / Limit	0 / 10

All:4

OpenScape Mobile Licenses Information for OpenScape	
Assigned to the System	10000
In Use	0
Maximum Usage of Previous Day	0
Customer Violations / Limit	0 / 10

4.1.8.3 How to Activate License Logging

The *OpenScape Mobile Pro License Statistics* tab is used to activate the logging of OpenScape Mobile Pro license usage. (Currently, only the number of licenses used is logged.)

NOTICE:

This tab is greyed out if OpenScape Mobile Pro licensing is not enabled.

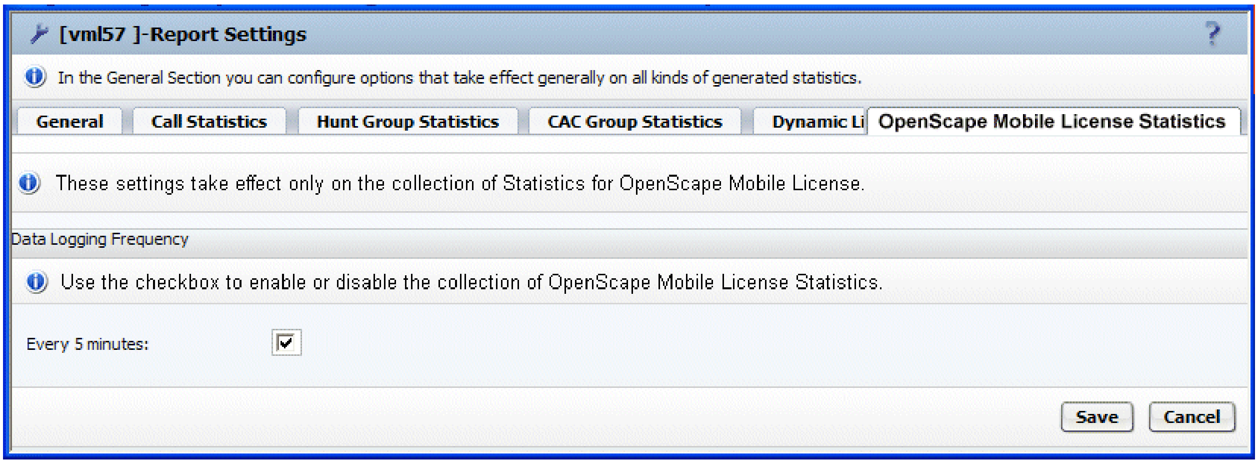
Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

2) Click on **General Settings > Report**.

3) Click on the ***OpenScape Mobile License Statistics*** tab.

4) Enable statistics collection by clicking the check box.



[vml57]-Report Settings

In the General Section you can configure options that take effect generally on all kinds of generated statistics.

These settings take effect only on the collection of Statistics for OpenScape Mobile License.

Data Logging Frequency

Use the checkbox to enable or disable the collection of OpenScape Mobile License Statistics.

Every 5 minutes: ☑

4.1.8.4 How to Monitor Licensing

With the statistics logging activated, periods of time can be searched to analyze usage patterns and identify peaks and valleys of license usage.

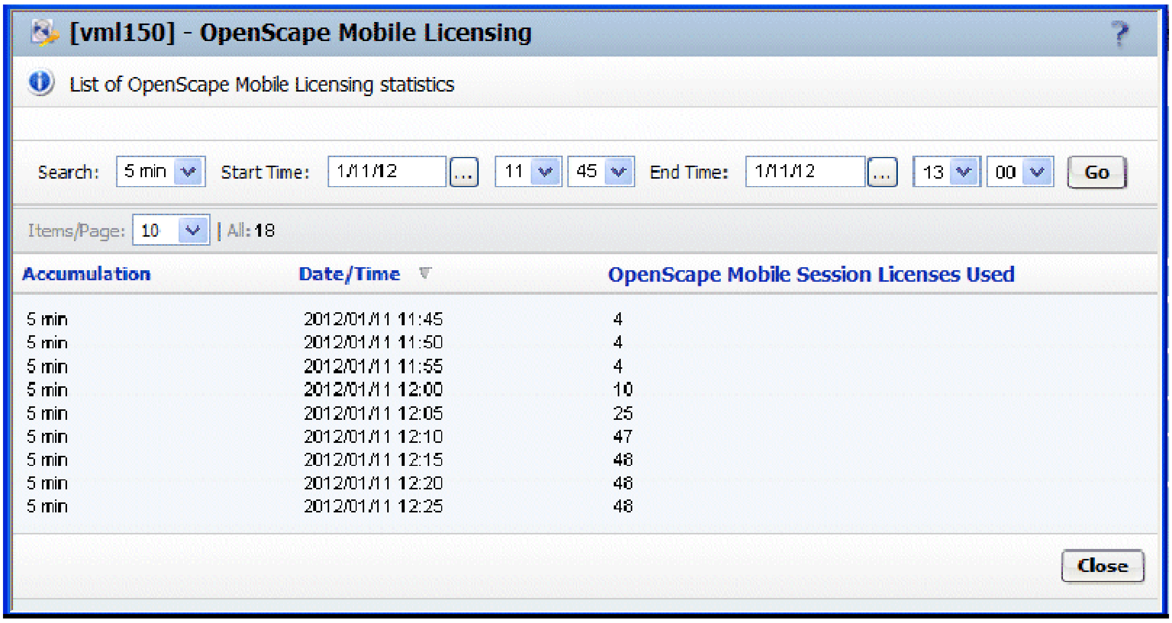
NOTICE:

If OpenScape Mobile Pro licensing is not enabled then the window ‘OpenScape Mobile Pro Licensing’ shows text indicating that no statistics exist.

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

2) Click on **Licensing Management > OpenScape Mobile Licensing**.



[vml150] - OpenScape Mobile Licensing

List of OpenScape Mobile Licensing statistics

Search: 5 min Start Time: 1/11/12 11 45 End Time: 1/11/12 13 00

Items/Page: 10 | All: 18

Accumulation	Date/Time	OpenScape Mobile Session Licenses Used
5 min	2012/01/11 11:45	4
5 min	2012/01/11 11:50	4
5 min	2012/01/11 11:55	4
5 min	2012/01/11 12:00	10
5 min	2012/01/11 12:05	25
5 min	2012/01/11 12:10	47
5 min	2012/01/11 12:15	48
5 min	2012/01/11 12:20	48
5 min	2012/01/11 12:25	48

4.1.9 How to Configure Digest Authentication

Use the RTP parameter *Srx/MobileClient/OSMOMutualAuth* to determine whether or not OpenScape Mobile Pro should validate the identity of OpenScape Voice (with digest authentication).

If this parameter is set to RtpTrue (default), OpenScape Voice will always issue a digest challenge to a mobile client. OpenScape Voice will provide an Authentication-Info response to the mobile client on REGISTER messages to allow the mobile client to authenticate OpenScape Voice.

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

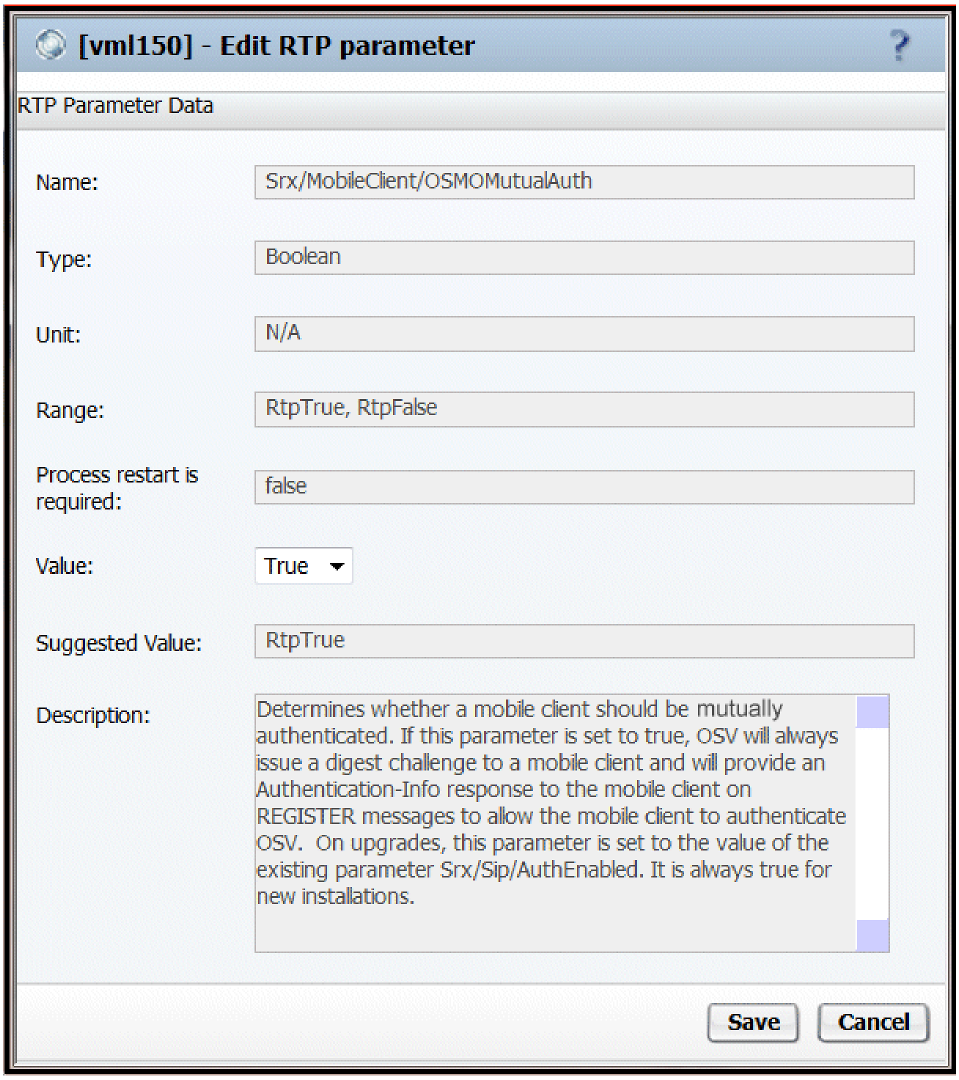
2) Click on **Administration** > **General Settings > RTP**.

3) Check *Srx/MobileClient/OSMOMutualAuth* and click **View/Edit**.

4) Edit the *Value* field and click **Save**.

NOTICE:

For additional protection, after system is upgraded, it is recommended to turn on **Digest Authentication**. This can be done in **CMP** > **Configuration** > **OpenScape Voice** > **Administration** > **Signaling Management** > **Digest Authentication.**



RTP Parameter Data

Name:	Srx/MobileClient/OSMOMutualAuth
Type:	Boolean
Unit:	N/A
Range:	RtpTrue, RtpFalse
Process restart is required:	false
Value:	True
Suggested Value:	RtpTrue
Description:	Determines whether a mobile client should be mutually authenticated. If this parameter is set to true, OSV will always issue a digest challenge to a mobile client and will provide an Authentication-Info response to the mobile client on REGISTER messages to allow the mobile client to authenticate OSV. On upgrades, this parameter is set to the value of the existing parameter Srx/Sip/AuthEnabled. It is always true for new installations.

4.1.10 Video calls Administration

A new feature, video call, has been introduced in the OpenScape Mobile Pro Application. Video calls are available with OpenScape Voice V7R1 PS30 and above.

4.2 OpenScape 4000 Configuration

OpenScape Mobile Pro supports OpenScape 4000 V8R2 or higher.

OpenScape Mobile Pro connected to OpenScape 4000 uses the same behavior like OpenScape Voice and the so called Auto Pilot Routing. It can be compared with a hunt group. As soon as the OSMO Pro is logged in the Auto Pilot Routing is activated. Incoming calls are routed always in this sequence: First the OpenScape Mobile Pro rings and after a systemwide configured time (Default=15 sec) the call is routed to the Deskphone (Info: Feature can also be used without dedicated Deskphone). From then on the normal via OpenScape 4000 call processing is executed. If the OpenScape Mobile Pro client has a cell number configured and route call to cell is active in the settings then an incoming call is routed to the cell number in case the client is logged off.

OpenScape Mobile Pro Clients must be configured in an OpenScape 4000 system as UFIP SIP device. There is one UFIP SIP device per OpenScape Mobile Pro Client user. This UFIP SIP device acts as a proxy for all of the user’s OpenScape Mobile Pro Clients.The UFIP SIP is an auxiliary device therefore it’s number is not presented on any phone display and known only by the system administrator.

For details on how to configure OpenScape 4000 to connect to OpenScape Mobile Pro, please refer to chapter "OpenScape Mobile Pro Client" of the document *OpenScape 4000, IP Solutions, Service Documentation.*

You can find this document at: https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/download/pdf/676475b2-d035-4262-840c-789e9ee1b335

4.3 SBC Administration

If access outside of the corporate network is needed (e.g., home Wi-Fi or Wi-Fi Hotspot), a Session Border Controller (SBC) must be used. The preferred SBC is the Mitel OpenScape SBC.

NOTICE:

SBC is mandatory for the operation in Voice Only Configuration or Integrated Configuration.

NOTICE:

Refer to the OpenScape SBC Administrator Documentation for configuration details.

4.3.1 How to Configure the SBC Address to Enable Remote Access

Regarding OpenScape 4000 to find details on how to Enable Remote Access please refer to chapter "OpenScape Mobile Pro Client" of the document: *OpenScape 4000, IP Solutions, Service Documentation.* Regarding OpenScape Voice for requirements specific to OpenScape Mobile Pro, configure the public SIP IP addresses of the SBC in OpenScape Voice to enable remote access for the OpenScape Mobile Pro Application. OpenScape Voice will communicate the SBC addresses to the OpenScape Mobile Pro Application the first time the user signs on.

Prerequisites

Have administration rights in Common Management Platform (CMP).

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

2) Click on **Administration > Feature Settings > Mobile Client Profiles.**

3) Select your OpenScape Mobile profile and click on it.

4) Click on the Connection tab of the pop up window and enter the **SBC IP Address**.

> **NOTICE:**
>
> It is recommended to use a non-standard port on the public SIP interface of the SBC (instead of the default SIP TLS port 5061 or in case of SIP MTLS, port 5161).
>
> The OpenScape Mobile Pro Application uses TLS/MTLS as transport. Firewalls deployed in front of the SBC must allow TLS/MTLS access to the public SIP address.

> **IMPORTANT:**
>
> In case of a SIP MTLS connection only the last imported certificate is used.

> **IMPORTANT:**
>
> To avoid any payload issues, it is mandatory to apply the following configuration change in the OpenScape Mobile Pro client. Navigate to **VOIP** > **Media**:
>
> **a)** Disable **Reset SRTP context upon key change**.
> **b)** Enable **Use single bridge/port for audio**.
> After making these changes, select **OK**, then choose **Apply Changes** to save the configuration.

4.3.2 How to configure the DNS on SBC

Step by Step

1) Click on **Configuration > OpenScape SBC** in CMP.
2) Select the SBC you want to configure the DNS form the drop down menu in **OpenScape SBC list**.
3) Click on **Network/ Net Services > DNS** to add your DNS IP address.
4) The DNS should be able to resolve the api.development.push.apple.com:443 and api.push.apple.com:443.

4.3.3 How to configure the certificates for SBC

For Android devices, in Folder Features, option Enable Push Notification Service, the Notification Server (Android) was created. Firebase Database URL must be filled with the client Firebase Database URL in case of user certificate upload. Otherwise, there is no need of change because It already has a default value.For Apple devices, if the user requires to configure certificates to enable the communication of SBC with APN in SBC version V9 R3.23.00-2 the procedure is described in the following steps:

Step by Step

1) Click on **Configuration > OpenScape SBC** in CMP.
2) Select the SBC you want to configure the DNS form the drop down menu in **OpenScape SBC list**.
3) Click on **Security > Certificate managements** and upload the .P12 or .P8 certificates.
4) Create a Certificate Profile for Push Notifications.
5) Setup the certificate password and the requested fields:

   Click on **Features** and check the **Enable Push Notifications Service** check box.

   Click on the **Configuration** button of the Enable Push Notification Service and fill in the following fields: **Push Certificate Passphrase, Apple account TeamId and Mobileapplication Bundle Id**.

> **NOTICE:**
>
> The **Enable Sandbox Push Server** should only be enabled after explicit request from GVS or Development Team.

> **NOTICE:**
>
> > **NOTICE:**
> >
> > For customers using the OpenScape Mobile Pro application directly from the Appstore, the certificates and Push Certificate Passphrase, Apple Account Team Id and Mobile Application Bundle Id have to be provided after communication with Product Manager.

4.3.4 How to enable Push Notifications for OpenScape Mobile Pro

The Push Notifications feature for Android is not enabled by default. The feature is supported from SBC version V9 R4.12.0 and later. The user needs to enable the feature through applications settings **Advanced** > **SIP Push Notifications**.

Step by Step

1) Click on **Configuration > OpenScape SBC** in CMP.
2) Select the SBC form the drop down menu in **OpenScape SBC list**.
3) Click on **Features** and check the **Enable Push Notification Service** check box.
4) Click the Configure button of the Enable Push Notification Service and then:
   a) Set **Call Hold** time to 15 seconds.
   b) Check the **Send Ringing** (180) during hold time check box.
   c) Set Push server port to 2195 (for iOS application only).
   d) Click **OK**.

4.3.5 How to configure the Maximum registration expiry for OpenScape Mobile Pro

Step by Step

1) Click on **Configuration > OpenScape SBC** in CMP.
2) Select the SBC form the drop down menu in **OpenScape SBC list**.
3) Click on **Features** and click the **Configure** button of the **Enable Remote Subscribers** option.
4) Set the **Maximum Registration Expiry time (sec)** to 604800.
5) Click **OK**.

4.4 Creating OpenScape Mobile Pro Users

The following summarizes the creation of the OpenScape Mobile Pro Subscriber and associates the mobile subscriber with the Desk Phone Subscriber. The configuration parameters required for the OpenScape Mobile Pro Subscriber are:

- Numbering Plan - The numbering plan created previously for OpenScape Mobile Pro Subscribers.
- Office Code - The office code created previously for OpenScape Mobile Pro Subscriber.
- Directory Number - The private home directory number created previously for OpenScape Mobile Pro Subscribers.
- Type of Number - Private.
- OpenScape Mobile Pro Device - Checked.

NOTICE:

In Integrated configurations, checking this box will indicate to the UC Server that this subscriber is UC-capable.

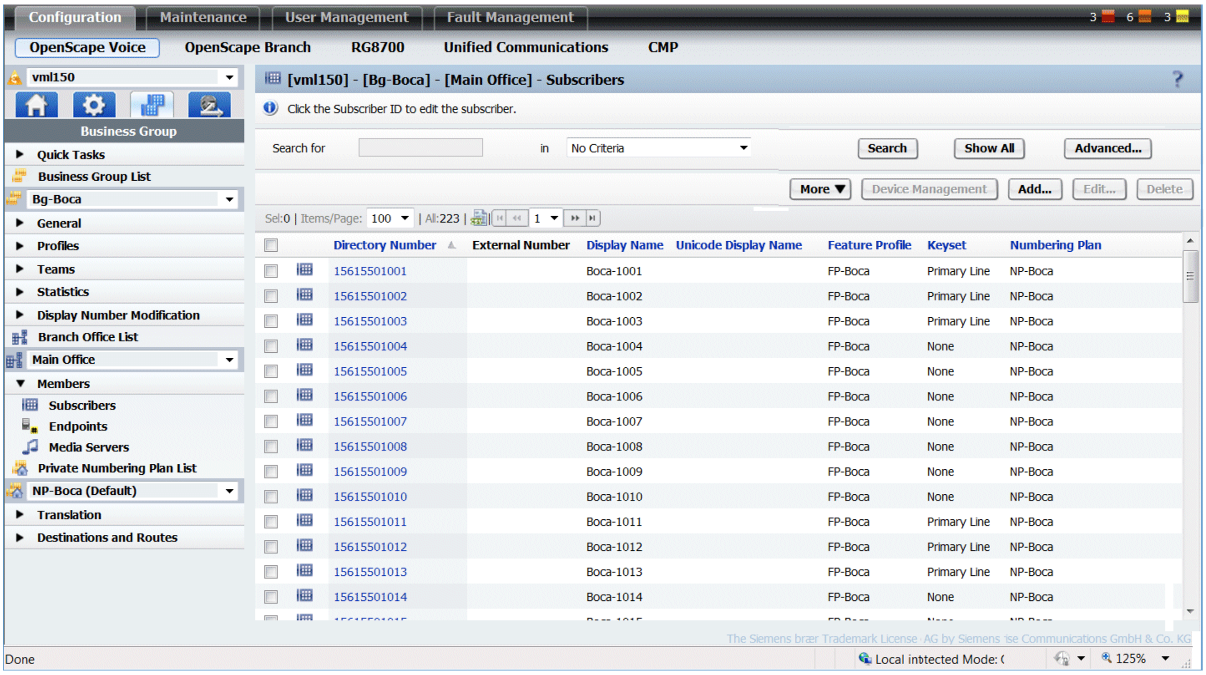
- Main Device ONS Number - This is the directory number of the user’s desk phone.
- Display Name - Automatically made the same as the one for the user’s desk phone subscriber. This enables a search by name in the Assistant.
- Digest Authentication - The Realm and Password digest authentication fields.
- All other fields are automatically set to default values and are blocked from editing.
- Registration via Central SBC Allowed - if you want to allow the SIP-Registrar to register the subscriber and its associated endpoint is a "Central SBC" endpoint

4.4.1 How to Create the OpenScape Mobile Pro Subscriber

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.
2) Click on **Business Group > Members > Subscribers.**

3) Click the ***Add*** button.



[vml150] - [Bg-Boca] - [Main Office] - Subscribers

Click the Subscriber ID to edit the subscriber.

Search for in No Criteria

Sel:0 | Items/Page: 100 | All:223 | 1

□		Directory Number	External Number	Display Name	Unicode Display Name	Feature Profile	Keyset	Numbering Plan
□		15615501001		Boca-1001		FP-Boca	Primary Line	NP-Boca
□		15615501002		Boca-1002		FP-Boca	Primary Line	NP-Boca
□		15615501003		Boca-1003		FP-Boca	Primary Line	NP-Boca
□		15615501004		Boca-1004		FP-Boca	None	NP-Boca
□		15615501005		Boca-1005		FP-Boca	None	NP-Boca
□		15615501006		Boca-1006		FP-Boca	None	NP-Boca
□		15615501007		Boca-1007		FP-Boca	None	NP-Boca
□		15615501008		Boca-1008		FP-Boca	None	NP-Boca
□		15615501009		Boca-1009		FP-Boca	None	NP-Boca
□		15615501010		Boca-1010		FP-Boca	None	NP-Boca
□		15615501011		Boca-1011		FP-Boca	Primary Line	NP-Boca
□		15615501012		Boca-1012		FP-Boca	Primary Line	NP-Boca
□		15615501013		Boca-1013		FP-Boca	Primary Line	NP-Boca
□		15615501014		Boca-1014		FP-Boca	None	NP-Boca

The Siemens brær Trademark License AG by Siemens ise Communications GmbH & Co. KG

4.4.1.1 How to Use the General Tab

Step by Step

1) In the **Directory Number** field, select an OpenScape Mobile Pro directory number created previously for OpenScape Mobile Pro Subscribers.

2) Set **Type of Number** to Private.

3) Check **OpenScape Mobile Device**.

NOTICE:

In Integrated configurations, checking this box will indicate to the UC Server that this subscriber is UC-capable.

4) In the **Main Device (ONS)** field, set the subscriber’s desk phone directory number (e.g., 15619231234).

The Users must have an ONS Number, but if they do not have an Office phone that is registered on OpenScape Voice or OpenScape 4000, then the Call Forwarding - Dependable target could be used to support an Office phone.

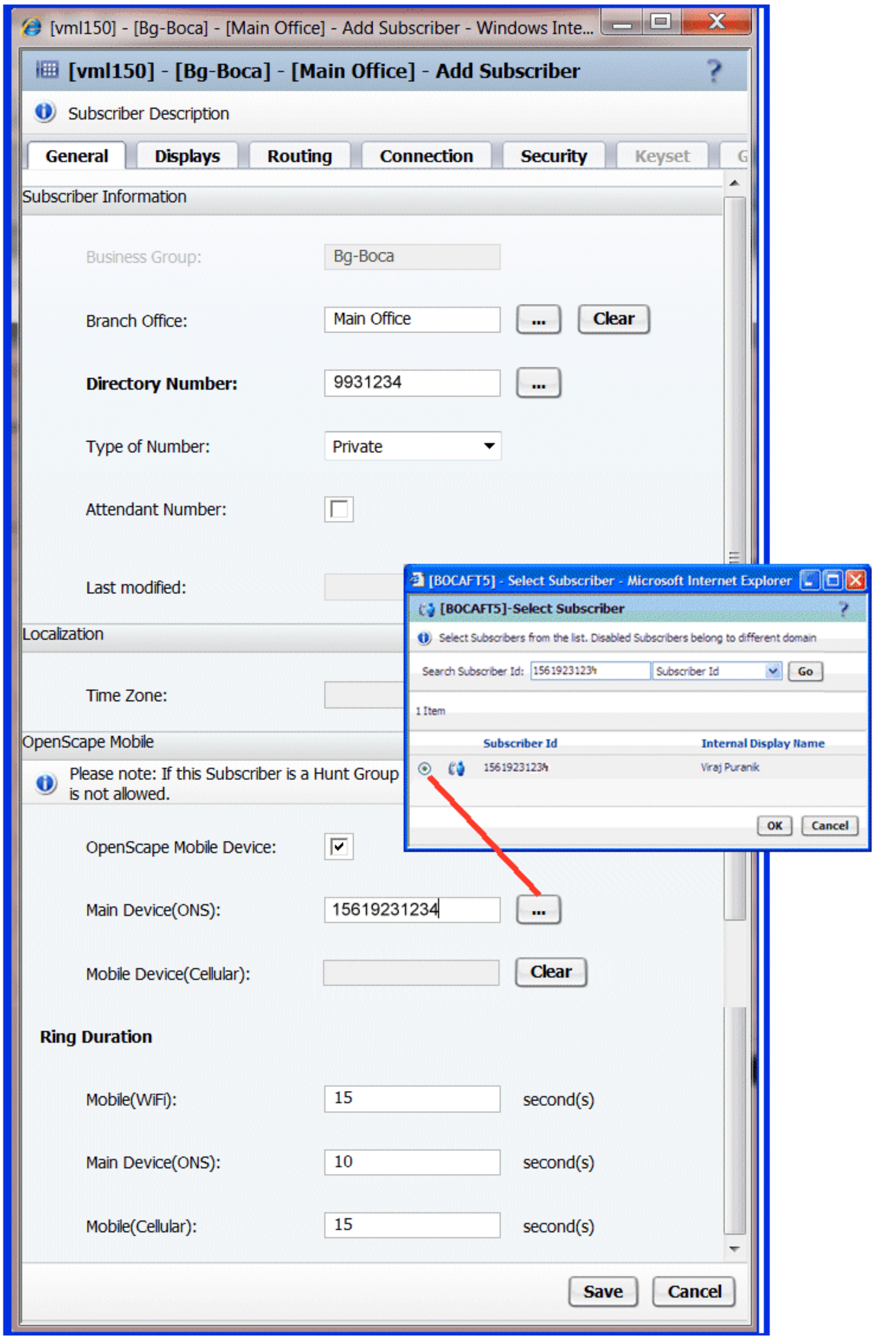
5) Provision the Main Device (ONS) by selecting the Desk Phone directory number. Change (if needed) the default ring duration to 15, 10, and 15 seconds for **Mobile (Wi-Fi)**, **Main Device (ONS)**, and **Mobile (Cellular)**, respectively. The ring duration determines the number of seconds the call

will alert a specific directory number before progressing to the next target (i.e., device).

NOTICE:

If an OpenScape Mobile Pro User asks you to increase a ring duration, it can be increased to a maximum of 25 seconds in 1-second increments. If you are asked, however, to reduce the cell time, be aware that “splash" ringing can result if it is reduced too much.

The **Mobile Device (Cellular)** field is filled in only when the user has turned on "Route calls to cell" in the client application; otherwise, the field is empty.



[vml150] - [Bg-Boca] - [Main Office] - Add Subscriber - Windows Inte...

[vml150] - [Bg-Boca] - [Main Office] - Add Subscriber

Subscriber Description

Subscriber Information

Business Group: Bg-Boca

Branch Office: Main Office

Directory Number: 9931234

Type of Number: Private

Attendant Number: □

Last modified:

Localization

Time Zone:

OpenScape Mobile

Please note: If this Subscriber is a Hunt Group is not allowed.

OpenScape Mobile Device: ☑

Main Device(ONS): 15619231234

Mobile Device(Cellular):

Ring Duration

Mobile(WiFi): 15 second(s)

Main Device(ONS): 10 second(s)

Mobile(Cellular): 15 second(s)

[BOCAFT5] - Select Subscriber - Microsoft Internet Explorer

[BOCAFT5]-Select Subscriber

Select Subscribers from the list. Disabled Subscribers belong to different domain

Search Subscriber Id: 15619231234 Subscriber Id

1 Item

	Subscriber Id	Internal Display Name
●	15619231234	Viraj Puranik

4.4.1.2 How to Use the Security Tab

This tab is used to configure the Digest Authentication (DA) for the OpenScape Mobile Pro Subscriber.

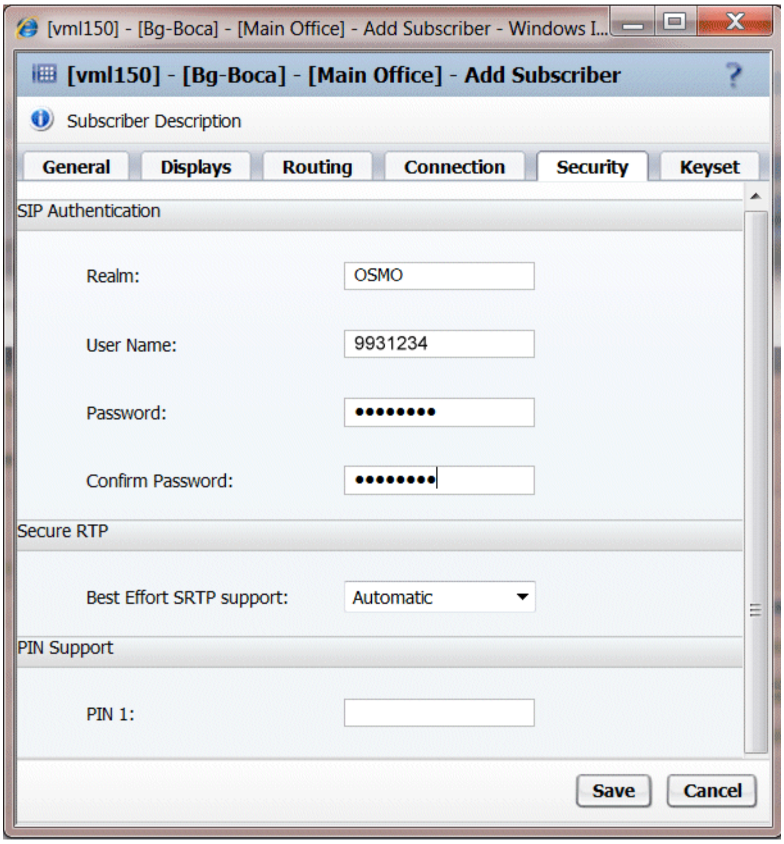
Step by Step

1) **Realm** was automatically set equal to the value for the desk phone when the OpenScape Mobile Pro Subscriber was created. This value does not have to be equal; it can be changed.
2) Set the **User Name** equal to the subscriber number assigned to the OpenScape Mobile Pro device.

> **NOTICE:**
>
> If OpenScape Mobile Pro is used and Digest Authentication is enabled on OpenScape Voice/4000, the OpenScape Mobile Pro subscriber and ONS subscriber should be configured as followed:
>
> - for the ONS subscriber, set the **Username** that is equal to the ONS Number
>
> - for the OpenScape Mobile Pro subscriber, set the **Username** that is equal to the OpenScape Mobile Pro device number
>
> If the DA **Username** of ONS subscriber is different from the ONS Number, the OpenScape Mobile Pro registration will fail because the Digest Authentication entries will not be correctly populated to OpenScape Mobile Pro.

3) **Password** was automatically set equal to the value for the desk phone when the OpenScape Mobile Pro Subscriber was created. To ensure the best security possible it is strongly advised that **Password** be set to a different value from that of the desk phone.

4) Confirm by re-entering the password then click **Save**.



[vml150] - [Bg-Boca] - [Main Office] - Add Subscriber - Windows I...

[vml150] - [Bg-Boca] - [Main Office] - Add Subscriber

Subscriber Description

General | Displays | Routing | Connection | Security | Keyset

SIP Authentication

Realm: OSMO

User Name: 9931234

Password: ••••••••

Confirm Password: ••••••••

Secure RTP

Best Effort SRTP support: Automatic

PIN Support

PIN 1:

Save | Cancel

4.4.1.3 Other Tabs

No data entry is required in the other tabs.

4.4.2 How to Display the Subscriber in OpenScape Voice Configuration

Once created, the subscriber should be listed in the subscriber table.

Step by Step

1) Click on **Configuration > OpenScape Voice** tab in CMP.

2) Click on **Business Group > Members > Subscribers.**

4.5 Mobile Client Profiles

The OpenScape Mobile Pro RTP parameters are moved into a Mobile Client Profile configurable via the OpenScape Voice Assistant or OpenScape 4000 Assistant and CLI. These profiles can be created System-wide or Business Group-wide. Each user is assigned exactly one Mobile Client Profile. Mobile Client Profiles can be System-wide or Business-Group specific. They can be assigned to and used by a subscriber.

A Mobile Client Profile defined on a Business-Group level that is marked as default profile replaces the default profile defined on a system-wide level. When creating a new OpenScape Mobile Pro subscriber the default Business-Group level profile is pre-populated as default, and if there is none then the default global mobile client profile is suggested.

For details of how to add, clone, edit and delete a Mobile Client Profile, please refer to chapter "Mobile Client Profile" of the document *OpenScape Voice, Administrator Documentation* for OpenScape Voice or chapter "OpenScape Mobile Pro Client Configuration" of the document *OpenScape 4000, IP Solutions, Service Documentation.*

4.5.1 MDM Key-Value Pairs

OpenScape Mobile Pro V10 starting from version 2.0.1 supports multiple key-value pairs for remote management. Additionally it supports MobileIron AppConnect iOS SDK 4.1.0.58, for configuring key-value pairs.

NOTICE:

VPN tunneling is not supported.

To use AppConnect you have to connect to MobileIron Cloud platform and add the new application by selecting OpenScape Mobile Pro V10 from AppStore. Once installed, you can configure the supported key-values and enable/disable UI elements according to Key-Value pairs that you can find in Key-Value Pairs.

For further details regarding the MobileIron Cloud Platform please refer to "MobileIron Support Documentation".

4.6 Preparing the Desk Phone for OpenScape Mobile Pro

In order for the OpenScape Mobile Pro solution to work seamlessly, the user’s desk phone must be configured for CSTA operation. Chapter 2 of document “*SIP Phone and Client Configuration for CSTA-enabled Applications*” explains the various steps necessary to configure devices and soft clients for CSTA.

NOTICE:

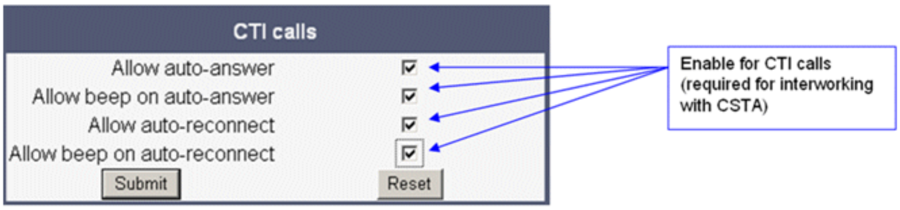
In a typical configuration the OpenScape SBC can support only a single device or branch proxy behind a remote NAT router. To safeguard against having multiple devices behind NAT using the same port numbers, the OpenStage phone should have a unique RTP port number when configured with SBC.

4.6.1 How to Prepare OpenStage Phone for OpenScape Mobile Pro

The minimal settings for OpenStage phones to allow seamless interworking with OpenScape Mobile Pro are as follows.

Step by Step

1) In the Device Web Admin navigate to **User Pages > Configuration > Incoming Calls.**
2) Select **CTI Calls** and check all to enable.
3) Click **Submit**.



CTI calls

Allow auto-answer ☑

Allow beep on auto-answer ☑

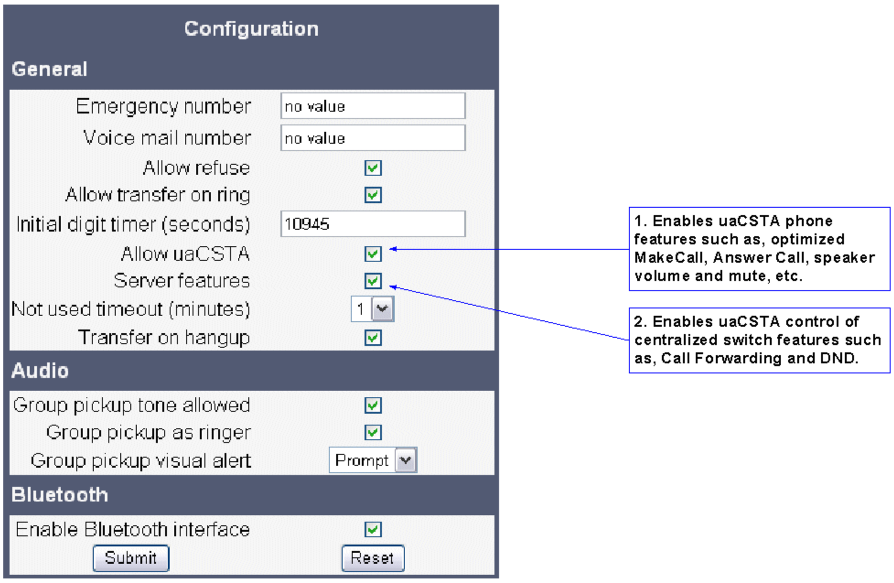
Allow auto-reconnect ☑

Allow beep on auto-reconnect ☑

Submit Reset

Enable for CTI calls (required for interworking with CSTA)

4) In the Device Web Admin navigate to **Administrator Pages > System > Features > Configuration**.
5) Select General and check "Allow uaCSTA" and "Server features".
6) Click **Submit**.



Configuration

General

Emergency number: no value

Voice mail number: no value

Allow refuse ☑

Allow transfer on ring ☑

Initial digit timer (seconds): 10945

Allow uaCSTA ☑

Server features ☑

Not used timeout (minutes): 1

Transfer on hangup ☑

Audio

Group pickup tone allowed ☑

Group pickup as ringer ☑

Group pickup visual alert: Prompt

Bluetooth

Enable Bluetooth interface ☑

Submit Reset

1. Enables uaCSTA phone features such as, optimized MakeCall, Answer Call, speaker volume and mute, etc.

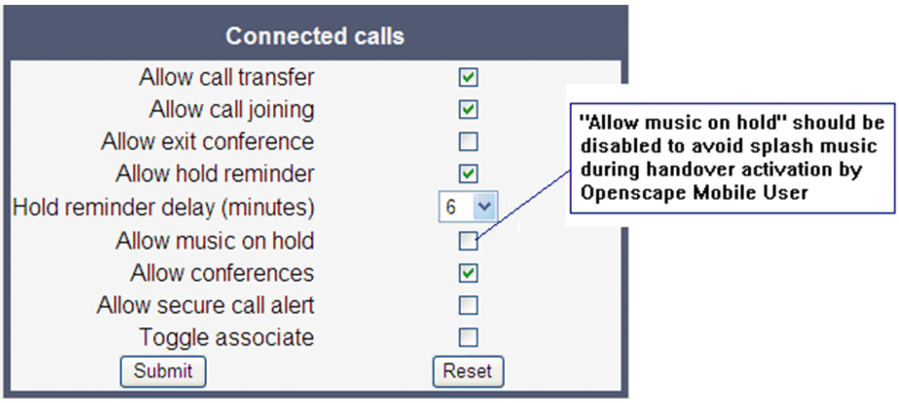
2. Enables uaCSTA control of centralized switch features such as, Call Forwarding and DND.

4.6.2 How to Disable Phone Hold Music

This is an optional step for enhanced user experience. Disable the local phone music when the call is placed on hold. This will ensure that there is no splash music during call hand over.

Step by Step

1) In the Device Web Admin navigate to **User Pages > Configuration**.
2) Select **Connected Calls** and uncheck "Allow music on hold".
3) Click **Submit**.



Connected calls

Allow call transfer ☑
Allow call joining ☑
Allow exit conference □
Allow hold reminder ☑
Hold reminder delay (minutes) 6
Allow music on hold □
Allow conferences ☑
Allow secure call alert □
Toggle associate □

"Allow music on hold" should be disabled to avoid splash music during handover activation by Openscape Mobile User

4.7 Configure Push Notifications for Chat messages

For configuring the Push Notifications for chat messages please refer to the following:

- *OpenScape UC Application V10 Installation and Upgrade, Installation Guide*

  Section: 13.6 Installing UC Pushy Messaging Middleware

5 OpenScape Voice Server-to-UC Server Configuration

NOTICE:

This chapter is not needed if your are deploying OpenScape Mobile Pro V10 in a UC-Only configuration. Go to the next chapter.

In the Integrated configuration, a SOAP interface exists between the OpenScape Voice Server and the OpenScape UC Server. This interface must be configured, security certificates must be exported/imported, and packet filter rules properly set.

5.1 How to Configure the OSV-to-UC Interface

Step by Step

1) Create a SOAP instance on OpenScape Voice to listen to port 8758.

a) Login as srx user.

b) startCli

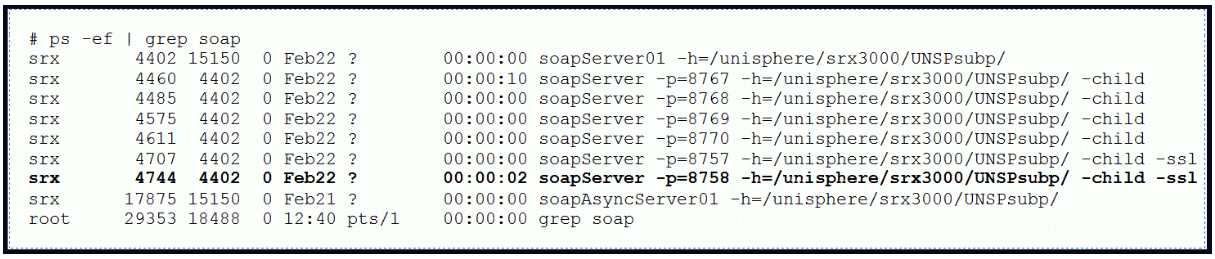
c) Select menu options: 1, 1, 3

d) Enter parameter name *Srx/Subp/NumberOfInstancesWithTLS* and increase value by additional one.

e) Save and exit cli.

f) Restart SOAP server with the command: pkill soapServer

g) Verify that SOAP is accepting requests on port 8758 with the command ps -ef | grep soapServer



```
# ps -ef | grep soap
srx       4402 15150  0 Feb22 ?        00:00:00 soapServer01 -h=/unisphere/srx3000/UNSPsubp/
srx       4460  4402  0 Feb22 ?        00:00:10 soapServer -p=8767 -h=/unisphere/srx3000/UNSPsubp/ -child
srx       4485  4402  0 Feb22 ?        00:00:00 soapServer -p=8768 -h=/unisphere/srx3000/UNSPsubp/ -child
srx       4575  4402  0 Feb22 ?        00:00:00 soapServer -p=8769 -h=/unisphere/srx3000/UNSPsubp/ -child
srx       4611  4402  0 Feb22 ?        00:00:00 soapServer -p=8770 -h=/unisphere/srx3000/UNSPsubp/ -child
srx       4707  4402  0 Feb22 ?        00:00:00 soapServer -p=8757 -h=/unisphere/srx3000/UNSPsubp/ -child -ssl
srx       4744  4402  0 Feb22 ?        00:00:02 soapServer -p=8758 -h=/unisphere/srx3000/UNSPsubp/ -child -ssl
srx      17875 15150  0 Feb21 ?        00:00:00 soapAsyncServer01 -h=/unisphere/srx3000/UNSPsubp/
root     29353 18488  0 12:40 pts/1    00:00:00 grep soap
```

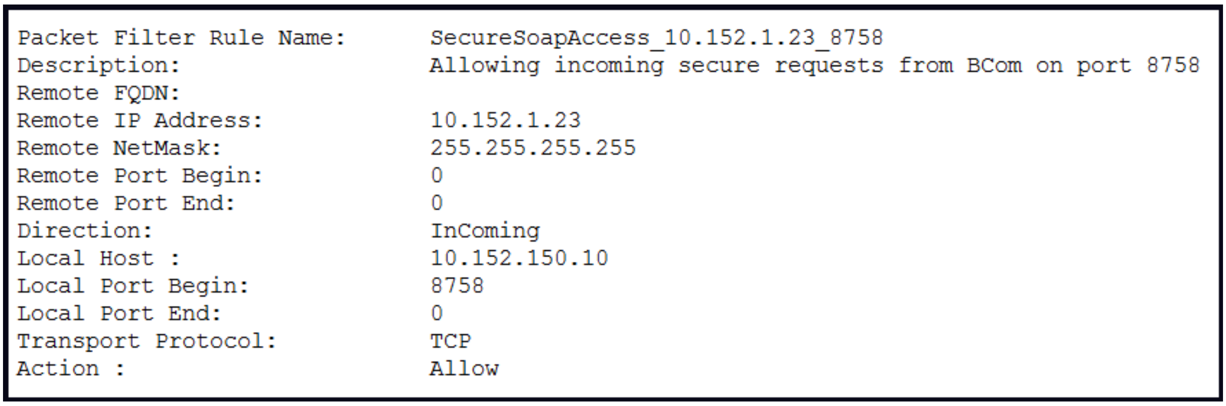
2) Create a packet filter rule on OpenScape Voice:

a) startCli

b) Select menu options: 6, 8, 3, 1

c) See the following example (replacing the IP address with the one from the UC Server).

d) Save and exit cli.



```
Packet Filter Rule Name:      SecureSoapAccess_10.152.1.23_8758
Description:                  Allowing incoming secure requests from BCom on port 8758
Remote FQDN:
Remote IP Address:            10.152.1.23
Remote NetMask:               255.255.255.255
Remote Port Begin:            0
Remote Port End:              0
Direction:                    InComing
Local Host :                  10.152.150.10
Local Port Begin:             8758
Local Port End:               0
Transport Protocol:           TCP
Action :                      Allow
```

3) If you installed your own certificates in OpenScape Voice, follow the procedure in the section on "Bcom" of the OpenScape Solution Set, *Solution Guide Certificate Management and TLS Administrator Documentation* to install certificates in the UC server. The certificate authority that signs the OpenScape Voice certificate must be the one that signs the BCOM certificate.

6 UC-Only Configuration

So far the UC-Only users were not able to receive any kind of notification related to the current call state (e.g. alerting, ongoing call, etc.). Furthermore, in UC-Only mode the OpenScape Mobile Pro application did not offer any kind of call control capabilities other than simple transferring and clearing of an ongoing call.

In order to resolve the aforementioned issues and allow users of 3G and 4G network to use more comprehensive set of features in UC-Only mode, the latest version of OpenScape Mobile Pro has introduced the following enhancements:

- notifications for the current call state and for the changing of the call state
- new call control capabilities that include:
  - call transfer
  - deflect a call
  - call on hold
  - conference
  - consultation
  - clear a call.

The UC-Only mode enhancements are implemented thanks to the new interface (i.e. HAProxy) that allows clients to be notified about the call stage and perform call control requests. There is a new connection to the Event Server. As the result, the OpenScape Mobile Pro application and UC Front-End do not communicate with each other directly, but via HAProxy. For more information regarding the configuration of HAProxy, please refer to the *OpenScape UC Application V9 Installation and Upgrade* document.

NOTICE:

A reverse Proxy (HAProxy) configuration is mandatory for OpenScape Mobile Pro.

From the end-user perspective, nothing has been changed in the login process. The users still need to enter Server Address (IP address or server name) given by their System Administrator. When the client tries to login to the OpenScape UC, it also tries to open a WebSocket to the OpenScape UC Front-End that will be used for the communication between the client and the REST API. If the connection succeeds, the WebSocket remains opened until the user logs off.

NOTICE:

The call control enhancements in UC-Only mode are available in OpenScape Mobile Pro Version 9 and higher. The minimum requirement for the OpenScape UC server is that it has to be V9 HF6 or higher.

As far as backward compatibility is concerned, the OpenScape Mobile Pro application version 9 will work in the old UC-Only mode if the OpenScape UC version is lower than V9 HF9 or the HAProxy is not configured.

7 Mobile Device Wi-Fi Configuration

The System Administrator must provide the user with certain information which they will need to configure the OpenScape Mobile Pro V10 Application on their mobile device. Refer to the “OpenScape Mobile Pro V10 User Guide” for instructions on how to install, configure, and operate the client application.

The OpenScape Mobile Pro V10 application is available for:

- iOS-based devices (e.g., iPhone, iPad) - Search for OpenScape Mobile Pro V10 at Apple’s Application Store.

  http://itunes.apple.com/us/app/openscape-mobile/id460445589?mt=8
- Android-based devices (e.g Android Smartphone, Android Tablet) - Search for OpenScape Mobile Pro V10 at Google Play Store.

7.1 What Information to send to OpenScape Mobile Pro V10 User

In addition to providing the sign-in credentials listed below, it is also recommended that the System Administrator direct the User to the OpenScape Mobile Pro V10 Forum for a copy of Quick References of OpenScape Mobile Pro V10.

> **NOTICE:**
>
> OpenScape Mobile Pro V10 is released to be connected directly to OpenScape Voice/OpenScape 4000 or via an SBC. It is not released to be connected via a proxy. (Voice-Only and Integrated configurations)

Voice-Only Configuration

UC-Only and Integrated Configurations

Device Activation - The following credentials enable the OpenScape Mobile Pro V10 User to sign in to the OpenScape Voice Server:

- Subscriber - This is the user’s desk phone directory number.
- Server Address - This is either an IP address or server name (i.e., FQDN and port) for:
  - The OpenScape Voice Server for sign-in via the corporate net
  - The SBC for sign-in outside the corporate net.
- Password - The SIP digest password.

The first time a user signs in to connect to OpenScape Voice/4000 (either over the corporate Wi-Fi or remotely through an SBC), the OpenScape Voice/4000 Server address (SIP) as well as the entire list of SBC addresses will be automatically communicated to the OpenScape Mobile Pro V10 Application. After the first sign-in a user can connect either directly over the corporate WAN or remotely through the SBC to OpenScape Voice/4000.

Device Activation - The following credentials enable the OpenScape Mobile Pro V10 User to sign in to the UC via HAProxy:

- Subscriber - This is their UC ID.

- Server Address - This is an IP address or server name (i.e. FQDN and port) for the HAProxy server for sign-in inside or outside the corporate network.

IMPORTANT:

If you are using the standard https configuration for the HAProxy server (i.e. https://<address>:8443/axis/services) all you need to send to your OpenScape Mobile Pro Users is the https://<address> part. OpenScape Mobile Pro will auto-complete the port and service names using the default ":8443/axis/services".

- Password - The UC password.

NOTICE:

- If you use an http address without the port then the default port of the app is 8081.

  IMPORTANT: http and port 8081 should NOT be used for privacy and security reasons because with HTTP anyone can sniff the network and read all traffic.
- If you use an https address without the port then the default port of the app is 8443.
- If you use a plain IP (SIP configuration) without the port then the default port of the app is 5061.

For any other case/configuration you should type the port as well.

QR code configuration generation

The administrator can produce a QR code with login/server configuration information and distribute to users so they can scan it with the OpenScape Mobile client. The QR code must be produced using the following URL format:

```
oscmob://account_details?
username=**********&server_url=*******&cell=*********
```

- "**oscmob://account_details?**"

  Required field Header for valid OSMO QR detection.
- "**username**"

  Required field The complete Login user name.
- "**server_url**"

  Required field The server URL for Login.
- "**cell**"

  Optional field The user's full cell phone number if it is known/exists.

NOTICE: The following characters "%", "&" and "+", when used in any of the fields above have to be escaped accordingly:

- % -> %25
- & -> %26
- + -> %2B

For example for the user Bob.Smith%@system, in server https://mobile.domain&.com:1234 with phone number +441234567899 the administrator must generate the QR using the following string:

```
oscmob://account_details?username=Bob.Smith
%25@system&server_url=https://mobile.domain
%26.com:1234&cell=%2B441234567899
```

8 Firewall settings for OpenScape Mobile Pro V10

You have to configure the following firewall settings:

Allow TCP traffic on ports 5223, 2195, 2196, 443. These ports are used for the communication between OpenScape Mobile Pro V10 Application and Apple Notification Server.

- TCP port 5223: used by devices to communicate to the APNs servers
- TCP port 2195: used to send notifications to the APNs
- TCP port 2196: used by the APNs feedback service
- TCP Port 443: used as a fallback on Wi-fi only, when devices are unable to communicate to APNs on port 5223

Allow TCP outgoing traffic on ports 5228,5229,5230. These ports are used for the communication between OpenScape Mobile Pro V10 Application and Firebase Cloud Messaging Servers. These ports should not be blocked, otherwise push notifications will not be delivered to user devices.

Allow direct SIP signaling traffic (TCP, UDP, TLS, MTLS) between corporate WiFi network and external IP Address of SBC. To see which ports that are configured in SBC and have to open firewall settings from CMP and navigate to **Network > Net Services >Settings.**

Allow RTP traffic between corporate WiFi network and external IP Address of SBC. To see the corresponding ports that are configured in SBC and have to open the firewall settings from CMP and navigate to **VoIP > Port> Signaling Settings**.

Push Notifications

Reference:

https://firebase.google.com/docs/cloud-messaging/network-configuration ports section.

Ideally, allow list ports 5228-5230 & 443 with no IP restrictions. Please note that, if you must have an IP restriction setup in your firewall, you should whitelist all of the IP addresses listed in goog.json.

9 Known Restrictions

OpenScape Mobile Pro V10 has the following restrictions for all configurations:

- A call made directly from or to the mobile device cell phone number (e.g., the telephone number provided by the service provider) cannot be moved.

OpenScape Mobile Pro V10 has the following restrictions for the Voice-Only configuration:

- Before installing OpenScape Mobile Pro V10 uninstall all previous versions of OpenScape Mobile because the two applications cannot share the same keychain to save settings.
- A call made from the mobile device when OpenScape Mobile Pro V10 is turned off or when Wi-Fi is not available cannot be moved.
- OpenScape Mobile Pro V10 must be connected to OpenScape Voice/4000 to change the “Route calls to cell” option. (As an alternative, the System Administrator, with access to the OpenScape Voice Assistant, may also make this change on behalf of the OpenScape Mobile Pro V10 User.)

OpenScape Mobile Pro has the following restriction for Integrated configurations:

- OpenScape Mobile Pro V10 must be connected to OpenScape Voice/4000 to change the “Route calls to cell” option. (As an alternative, the System Administrator, with access to the OpenScape Voice Assistant, may also make this change on behalf of the OpenScape Mobile Pro V10 User.)

9.1 Restrictions for OpenScape Mobile Pro

	UC-Only	Integrated Mode
Chat Feature	The user can not receive any chat when the OpenScape Mobile Pro application is in the background	The user can not receive any chat when the OpenScape Mobile Pro application is in the background
Enhanced Call Control	No reception of notification for Incoming call when the application is in the background	No reception of notification for Incoming call on a preferred device other than OpenScape Mobile Pro WiFi when the application is in the background.

NOTICE:

For a detailed restriction list with OpenScape 4000 please refer to chapter "OpenScape Mobile Pro Client" of the document: OpenScape 4000, IP Solutions, Service Documentation and the actual OpenScape 4000 Release Notes.

NOTICE:

The network handover feature is currently supported only for established calls and not for calls in transient or ringing state.

10 Third-Party Device Information

Routing Equipment:

- D-Link DIR-601 - Employees should be discouraged from using this as their wireless home router. Although outgoing calls are possible, this router drops the network connection without any notice when OpenScape Mobile Pro V10 is left idle for more than one minute thus making it unreachable over Wi-Fi. If *Route Calls to Cell* is enabled on the employee’s device, OpenScape Voice/4000 will be forced to try the cell number.
- Linksys WRT54G - Employees should be discouraged from using this as their wireless home router. OpenScape Mobile Pro V10 is able to connect from within the corporate network but not from another Wi-Fi network that uses this router. They can try upgrading to the latest firmware version available for the router but, if that doesn't work, they should get a new router. (The problem is related to issues with NAT support in that router.)

11 Additional Suggestions

- Wireless Access Points (WAP) with Wi-Fi controllers (such as the Enterasys Wi-Fi controllers) are preferred. These controllers provide IP address hand over between two WAPs when a device transitions from one WAP to another.
- If a majority of the devices show problems with WAPs, downgrading the connectivity to 802.11g or 802.11b may improve stability with mobile devices.
- Update mobile devices to the latest firmware as suggested by the manufacturers or service providers to include fixes and performance enhancements.
- In order to avoid splash music tone from desk phone during hand over, it is necessary to unsubscribe to the MoH option on desk phones. The System Administrator/user is able to access this option from the desk phone menu or from the desk phone configuration web page. See the previous section on disabling phone hold music.

Recommended Minimum Hardware requirements (Android) devices)

- Devices CPU:

- Qualcomm Snapdragon 636 and better or
- HiSilicon Kirin 710 and better or
- Samsung Exynos 9610 and better or
- MediaTek Helio P65 and better

- RAM: 3 GB minimum.

12 Error Reporting, Data collection and Diagnosis

Users can report errors by sending OpenScape Mobile Pro V10 Application log files via e-mail (for details see the OpenScape Mobile Pro V10 User Guides, *Diagnostics* and *Log File Management* sections).

- For iOS - Settings -> Advanced -> Log File Management -> Options -> Send.
- For Android - Settings -> Advanced -> Log File Management -> Options -> Send

The e-mail address where the log files are sent for analysis is centrally configurable in Openscape Voice via the RTP parameter *Srx/MobileClient/ServiceContactEmail*. See the appendix for details.

Optionally deploy the OpenScape Trace Manager for end-to-end diagnostic data collection.

IMPORTANT: It is strongly advised to NOT change error codes coming from UC (e.g. 401 to 401). Please configure the Web entry server to not change the UC error codes.

13 Infrastructure Requirements and Recommendations

13.1 Speech Bandwidth

OpenScape Mobile Pro V10 supports ISAC, G.711, G.722, and iLBC codecs over 802.11. The required bandwidth per call (in each direction) is 83.2 Kbps. The bandwidth for ISAC is variable from 10 Kbps-to-15 Kbps and for iLBC it is 15 Kbps.

13.2 Signaling Bandwidth

In addition to the bandwidth required for speech, 1 Kbps signaling bandwidth is required for each active OpenScape Mobile Pro V10 application.

13.3 Wireless Network Infrastructure Requirements and Recommendations

The requirements are:

- The WLAN infrastructure must provide sufficient coverage to support OpenScape Mobile Pro V10 client devices in all areas where they will be used.
- The WLAN must provide sufficient capacity to support the wireless telephony application taking into account other WLAN services.
- OpenScape Mobile Pro V10 application, always needs an internet connectivity to communicate to the Apple or Firebase Push Notification Service.

It is recommended that:

- A Wi-Fi site survey be performed. A range of assessment, consultancy, and design services for any network that is to be used for speech is offered.
- All WLAN Access Points are Wi-Fi Alliance certified for IEEE 802.11a, b, g, and n.
- All WLAN Access Points are Wi-Fi Alliance certified for Wi-Fi Protected Access. (WPA 2 Enterprise).
- All WLAN Access Points are Wi-Fi Alliance certified for Wi-Fi Multimedia™ (WMM®).
- All WLAN Access Points are Wi-Fi Alliance certified for Wi-Fi Multimedia Power Save™ (WMM Power Save®).

13.4 Voice Over WLAN RF Recommendations

Voice services require signals that are consistent and stronger than WLAN data-only networks. Attention must also be given to call density planning. Consider the use case of a phone vs a laptop.

A phone is typically used at eye level versus a laptop that is used on a surface such as a desk or a person’s lap. With a phone it has been found that people tend to seek out quiet areas to talk. These are often areas where WLAN coverage is challenging. A good example is a stairwell which is typically a nice quiet place for a private call but not the first place under consideration for a WLAN survey. Additionally, the attenuation of the human skull plus soft tissue can amount to as much as 10-to-12 dB. This makes the importance of a strong signal quite clear.

Most common minimum signal strength for an 802.11 VoWLAN deployment is -70 dB. Lower signal strength may cause choppy audio.

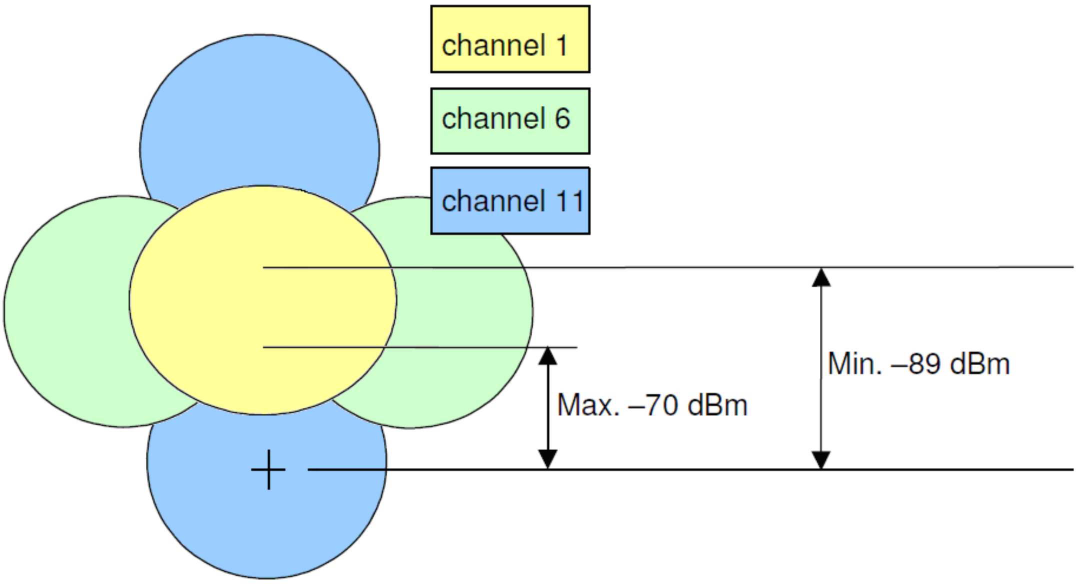
- The cell boundary for voice calls should be -70 dBm or stronger. It is recommended to measure the field strength several times and calculate an average value. The value of -70 dBm has been found to be optimal for most applications as it allows a high data rate connection while avoiding small cell sizes.

NOTICE:

Roaming thresholds may vary from device to device. Some devices may wait until the signal strength falls to -70dBm before roaming to an Access Point (AP) with a stronger signal strength. Other devices may have an -80 dBm roaming threshold. Transmission delays may occur when roaming with a device whose roaming threshold is not adjusted to the target cell power boundary.

- The minimal distance between two WLAN cells with the same channel should be -19 dBm.
- WLAN cells should overlap 20-to-30% to guarantee safe roaming.
- Channel utilization QoS Basic Service Set (QBSS) should be less then 45%.
- Packet Error Rate (PER) should be less then 1%.
- Signal-to-Noise Ratio (SNR) should be higher then 25 dB.
- AP should use diversity antennas.
- APs should be bridged so that calls will not be lost when moving from one AP to another.

The following figure shows a typical deployment with a 15-to-20% overlap of a given AP's cell from each of the adjoining cells. The separation of same channel cells should be 19 dBm. The radius of the cell should be not more then -70 dBm.



13.5 Network Configuration Requirements and Recommendations

The following is recommended:

- Differentiated Services Code Point (DSCP) should be configured on the network. DSCP can be provisioned in OpenScape Voice with the RTP parameters listed below.
  - Srx/IpPacketPriority/DSCPTOS/SIP/Type (default DSCP)
  - Srx/IpPacketPriority/DSCPTOS/SIP/Value (default 40)
  - Srx/IpPacketPriority/DSCPTOS/RTP/Type (default DSCP)
  - Srx/IpPacketPriority/DSCPTOS/RTP/Value (default 46)
  - Srx/IpPacketPriority/EnableWmm (default RtpTrue).

IMPORTANT:

There are problems on different Android versions and devices with WMM. If you have WMM enabled on your network please verify that the mobile devices you plan to deploy are Wi-Fi Alliance certified for WMM (http://www.wi-fi.org/search_products.php Voice-Capable Devices, Smartphones). If issues persist when using WMM, disabling WMM on Wi-Fi Access Points is often the solution to solve connectivity problems with Android devices.

The following are required:

- Firewalls must be configured to allow OpenScape Mobile Pro V10 voice and signaling packets to pass. Keep the following ports open:
  - 5008 - Used for RTP
  - 5009 - Used for RTCP
  - 5060 - Used for TCP signaling
  - 5061 - Used for TLS signaling
  - 5161 - Used for MTLS signaling
  - 2195 - Used for Push Notifications
- Provision the firewall to accept traffic on port range 5008-5015 (both, 5008 and 5015 included). These ports are used by OpenScape Mobile Pro V10 for RTP communication to and from OpenScape Mobile Pro V10. The above mentioned ports shall be used for:
  - RTP packet exchange
  - RTCP packet exchange
  - Audio channel
  - Video channel
  - Secure media
  - Insecure media

NOTICE:

One example could be:

1) insecure audio will use 5008 for RTP, 5009 for RTCP

2) secure audio will use 5010 for SRTP, 5011 for SRTCP

3) insecure video will use 5012 for RTP, 5013 for RTCP

4) secure video will use 5014 for SRTP, 5015 for SRTCP.

- Regarding OpenScape Mobile Pro V10 for Apple devices, Network Address Translation (NAT) must not be applied to VoIP traffic. The exception is that an approved Session Border Controller (SBC) may be used in conjunction with a NAT firewall. Approved SBCs are listed in the OpenScape Voice Release notes.

13.6 Network Performance Requirements

The network performance requirements are:

- The maximum end-to-end network latency for RTP packets should be less than 100 ms.
- The maximum end-to-end network jitter for RTP packets should be less than 30 ms.
- The maximum packet loss should be less than 1% peak over a 5-minute period.

NOTICE:

Additional network planning information is available in the *OpenScape Voice Design and Planning Manual, SIP Network Planning*.

13.7 MDM Key-Value Pairs

OpenScape Mobile Pro V10 starting from version 2.0.1 supports multiple key-value pairs for remote management. Additionally it supports MobileIron AppConnect iOS SDK 4.1.0.58, for configuring key-value pairs.

NOTICE:

VPN tunneling is not supported.

To use AppConnect you have to connect to MobileIron Cloud platform and add the new application by selecting OpenScape Mobile Pro V10 from AppStore. Once installed, you can configure the supported key-values and enable/disable UI elements according to Key-Value pairs that you can find in Key-Value Pairs.

For further details regarding the MobileIron Cloud Platform please refer to "MobileIron Support Documentation".

14 Appendix

14.1 RTP Parameters

RTP parameters are set to enforce global (i.e., switch-wide) policies and ensure proper feature networking. Following are the RTP parameters for OpenScape Mobile Pro V10.

RTP Parameter	Default	Usage
Srx/IpPacketPriority/ DSCPTOS/RTP/Type	DSCP	QoS value for voice traffic (RTP). This parameter determines if the accompanying Value parm is expressed as Differentiated Services Code Point (DSCP) or as Type of Service (TOS).
Srx/IpPacketPriority/ DSCPTOS/RTP/Value	46	QoS value for the media (RTP) stream between devices. This parameter allows the setting of traffic class value (DSCP) or Type of Service value (TOS) to ensure the media traffic gets enough priority in the network.
Srx/IpPacketPriority/ DSCPTOS/SIP/Type	DSCP	QoS value for SIP Signaling. This parameter determines if the accompanying Value parm is expressed as Differentiated Services Code Point (DSCP) or as Type of Service (TOS).
Srx/IpPacketPriority/ DSCPTOS/SIP/Value	40	QoS value for SIP Signaling. This parameter allows the setting of traffic class value DSCP or Type of Service (TOS) value.
Srx/MobileClient/ OSMOMutualAuth	RtpTrue	Determines whether a mobile client should be mutually authenticated. If this parameter is set to true, OSV will always issue a digest challenge to a mobile client and will provide an Authentication-Info response to the mobile client on REGISTER messages to allow the mobile client to authenticate OSV. On upgrades, this parameter is set to the value of the existing parameter Srx/ Sip/AuthEnabled. It is always true for new installations.
Srx/MobileClient/ TimeoutOSMONotReachable	6000	The time OSV will wait before rerouting a call when the Mobile Client is still registered, but not reachable (doesn't send any reply to incoming calls). This usually indicates that the user walked out of Wi-Fi coverage while the Mobile Client was registered. OSV will redirect the call to another destination (desk or cell) after this timer expires.

RTP Parameter	Default	Usage
hiQ/CSTA/ OSMOVirtualDeskPhoneOption	False	This parameter allows OpenScape Mobile Pro V10 enabled subscribers that do not have a registered Desk Phone on the OpenScape Voice system (e.g., OpenScape 4000 device) to use their Call Forwarding – Dependable non-voicemail target as a Virtual Desk Phone routing of inbound calls. When the value of this parameter is set to True, OpenScape Mobile Pro V10 routing will use the OpenScape Mobile Pro V10 enabled subscriber’s Call Forward – Dependable non-voicemail target, if provisioned, as a virtual Desk Phone device. On the other hand, once it is set to False, OpenScape Mobile Pro V10 routing follows standard routing and device selection rules for OpenScape Mobile Pro V10 enabled subscribers.

14.2 Key-Value Pairs

In order to disable a setting in your user device you have to provide the key that is listed in column "Key for disabling UI element" below with the boolean value false, or otherwise all UI elements, are enabled.

Key	Require	Key for disabling UI element	In app setting location	Description
serverUserName	required	serverUserNameEnabled	Account > Subscriber	Your subscriber UC username or OSV number
serverUrl	required	serverUrlEnabled	Account > Server Address	The UC server or SBC address: i.e. https:// or https:// or an IP
serverPassword	required	Not supported	Account > Password	Your subscriber UC password or OSV password. Must be in base64 format.
osv_cellular_number_pref	optional	cellularNumberEnabled	Account > Cellular Number	Phone Cell number in MSISDN format Your mobile cell number that want to send the calls on OpenScape Mobile Cellular device
log_state_pref	optional	logStateEnabled	Advanced > Log Level	Accepted values: Off, Min, Med, Max **NOTICE:** Max level may affect application performance and should only used after GVS/ DEV request. Default is Med

Key	Require	Key for disabling UI element	In app setting location	Description
disableCallQualityWarningPrompt	optional	disableCallQualityWarningPromptEnabled	Advanced > Disable Call Quality Warnings	Boolean value with true / false Prevent indication of network quality from displaying during a call Default is false
cell_routing_pref	optional	cellRoutingEnabled	Route Calls To Cell	Boolean value with true / false Route calls to cell when Auto-Pilot is active and not reachable over VoIP Default is false
base64CertPassword	optional	Not UI element. Not supported.	Input dialog during certificate import	Certificate password must be in base64 format. This field is required in case a base64Cert key is provided
base64Cert	optional	Not UI element. Not supported.	Advanced > Certificates	The application client certificate will be the exchanged with the HAproxy To fill that value you can use the following command at an existing .osmc certificate.openssl base64 < osmo.osmc | tr -d '\n' | pbcopy
autoSave	optional	Not UI element. Not supported.	Not an application setting only available from MDM.	Will perform the auto save of provided values.Boolean value with true / false. Default is false.
allowInvCert	optional	allowInvCertEnabled	Advanced > Allow Invalid Certificates	Switch that enables the allow invalid certificates.Boolean value with true / false.Default is false.
allow_cdn_calls	optional	allowCdnCallsEnabled	Allow VoIP Calls	Boolean value with true / false. Use VoIP functionality over 3G/LTE networks. Default is false
3g_routing	optional	useWifiEnabled	Use Wi-Fi only (Reversed)	Boolean value with true / false. YES when we want to use application over 3G/LTE. NO otherwise. Do not set this value to false when allow_cdn_calls is trueDefault is false
disableChatFeature	optional			Boolean value with true / false. Disable chat and remove chat tab from tab bar. Default is false

14.3 Glossary of Terms

Diversity Antenna	Device using two or more antennas to improve the quality and reliability of a wireless link.
DSCP	Differentiated Services Code Point is a field in the IP packet header used for packet classification. It is used to give priority to voice and signaling traffic.
NAT	Network Address Translation

OpenScape Mobile Pro V10 Application	Refers to the client installed on the mobile device.
OpenScape Mobile Pro V10 Device	The iOS or Android device that hosts the OpenScape Mobile Pro V10 application.
OpenScape Mobile Pro V10 User	The user of the OpenScape Mobile Pro V10 application.
OSV	OpenScape Voice server
PER	Packet error rate is the number of incorrectly received data packets divided by the total number of received packets.
QBSS 802.11e	Quality of Service Basic Service Set
SBC	Session Border Controller
SNR	Signal-to-Noise Ratio
WAP	Wireless Access Point
WAP Controller	An intelligent controller which can seamlessly hand over IP addresses when devices transition from one WAP to another.
Wi-Fi	Wireless local area network based on the IEEE 802.11.
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks.

mitel.com