A MITEL
PRODUCT
GUIDE

MiVoice MX-ONE

Integration with Microsoft Teams Through OpenScape Session Border Controller

Release 11.0
Document Version 3.0

August 2024

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL®).**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), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

What's New in this Document 1

This section summarizes changes in the Microsoft Teams integration with MiVoice MX-ONE (MX-ONE) through OpenScape Session Border Controller (SBC) for the release 11.0.

Table 1: Document Version 3.0

Feature/ Enhancement	Update	Location	Publish Date
Configuring OpenScape SBC	Removed the default configuration parameters as they are not required during initial installation.	Configuring OpenScape SBC on page 37	August 2024
Installing OpenScape Session Border Controller	Documentation improvements and updates.	Installing OpenScape SBC on page 28	

Table 2: Document Version 2.0

Feature/ Enhancement	Update	Location	Publish Date
E911 Solution	E911 solution routes the E911 call to the appropriate Public Safety Answering Point (PSAP) and notifies security personnel.	Configuring an E911 Solution on page 106	July 2024
Firewall Configuration	Added prerequisites for firewall configuration.	Prerequisite on page 50	
Certificates Configuration	Improved certificates configuration procedure.	Configuring Certificates	

Table 3: Document Version 1.0

Feature/ Enhancement	Update	Location	Publish Date
Integration of Microsoft Teams	Microsoft Teams integration with MX-ONE through OpenScape SBC.	Entire Document	July 2024

Preface 2

This chapter contains the following sections:

This guide outlines the steps required to connect Microsoft Teams with MiVoice MX-ONE (MX-ONE) through OpenScape SBC.

Note:

This document focuses only on the MiVoice MX-ONE (MX-ONE), OpenScape SBC, and Microsoft Teams configuration. The initial configuration for each component, such as installation, creation of users, enabling telephony features, and modifying calling policies are not in the scope of this document. For information on MiVoice MX-ONE (MX-ONE) initial configuration, refer to the MiVoice MX-ONE (MX-ONE) documentation on the Document Center.

2.1 About This Document

This document provides a reference to Mitel Authorized Solutions providers for configuring the MX-ONE to integrate Microsoft Teams through OpenScape SBC. The different devices can be configured in various configurations depending on your VoIP solution.

2.2 Related Documentation

For additional information on OpenScape SBC, refer to the following documents:

- OpenScape SBC V11 Configuration Guide
- OpenScape SBC V11 with Survivable Branch Appliance (SBA) Installation Guide
- OpenScape Voice with Microsoft Teams and OpenScape SBC Configuration Guide
- OpenScape SBC V11 Administration Guide
- OpenScape SBC V11 Configuration Guide, Administration Documentation
- OpenScape SBC V11 Installation Guide
- OpenScape SBC V11 Security Checklist

For additional information on Microsoft Teams solution, refer to the following document:

- MS Teams Solution Guide (HTML)

For additional information on E911 Solution, refer to the following documents:

- MiVoice MX-ONE Emergency Services and RAY BAUM Integration with RedSky
- MiVoice MX-ONE Emergency Services and RAY BAUM Integration with Intrado
- Microsoft Teams Emergency Calling

For additional information on MX-ONE, refer to the following document:

- Mitel MiVoice MX-ONE Technical Documentation

2.3 Intended Audience

This document is aimed primarily at the following professionals:

- Administrators
- Engineers

> **Note**:
> It is recommended that the intended audience have the basic installation, configuration, and maintenance knowledge of MiVoice MX-ONE (MX-ONE, Microsoft Teams, and OpenScape SBC.

2.4 Disclaimer

In this document, the images, screenshots, server names, file names, and database names are subject to change. The actual data might vary from the user's environment.

About the MX-ONE - OpenScape SBC - Microsoft Teams Solution 3

This chapter contains the following sections:

3.1 Overview

MiVoice MX-ONE offers a scalable and feature-rich communication system for businesses of varying sizes, employing a unified software stream. Tailored to meet the requirements of enterprises ranging from 5 to 500,000 users, MX-ONE accommodates both single-site deployments and multi-site networks across onsite, private cloud, public cloud, or hybrid environments.

The OpenScape SBC serves as a software-based network border element, enhancing Voice over IP (VoIP) security and cost efficiency within the Mitel and OpenScape Enterprise Solution set. Designed for secure extension of OpenScape SIP-based communication and applications beyond enterprise network boundaries, OpenScape SBC is particularly useful for centralized deployment scenarios. It provides essential interoperability, security, management, and control capabilities to support SIP trunking applications.

This document outlines the essential configuration steps for seamlessly integrating MX-ONE and OpenScape SBC with Microsoft Teams. Additionally, it describes the steps required for configuring Emergency Calls. For information on restrictions and known issues, refer to the Appendix A: Restrictions and Known Issues on page 118.

For information on the configuration, refer to the following sections in this documentation:

- Configuring MX-ONE on page 9
- Configuring OpenScape SBC on page 37
- Configuring Microsoft Teams on page 99
- Configuring an E911 Solution

3.2 Deployment Scenarios

This section describes the single-arm and multiple-arm deployment scenarios for the OpenScape SBC. In this document, an Arm is defined as a network connection to a physical or virtual network interface card. Single-arm or one-arm deployments refer to deployments using only one Network Interface Card (NIC). In a multi-arm configuration, the OpenScape SBC is deployed across multiple network segments, typically segregating external and internal traffic using multiple NICs.

Note:
In single and multiple-arm configurations, the OpenScape SBC must be deployed behind the customer's firewall.

- **Single-arm Configuration (recommended)**

  In a single-arm configuration, both incoming and outgoing traffic of the OpenScape SBC passes through the same NIC. Traffic from the client, passing through the OpenScape SBC, undergoes Network Address Translation (NAT) rules introduced in the firewall(s) located in the Demilitarized Zone (DMZ). The DMZ functions as a perimeter network, providing an additional layer of security for an organization's internal LAN.

  For media, the ICE mechanism is used in the media profile by Microsoft Teams. In this case, the Microsoft Teams media profile must be set as **ICE-FULL**; otherwise, the OpenScape SBC will not initiate ICE negotiations, and Microsoft Teams will not send either.

  The following figure depicts the single-arm configuration.

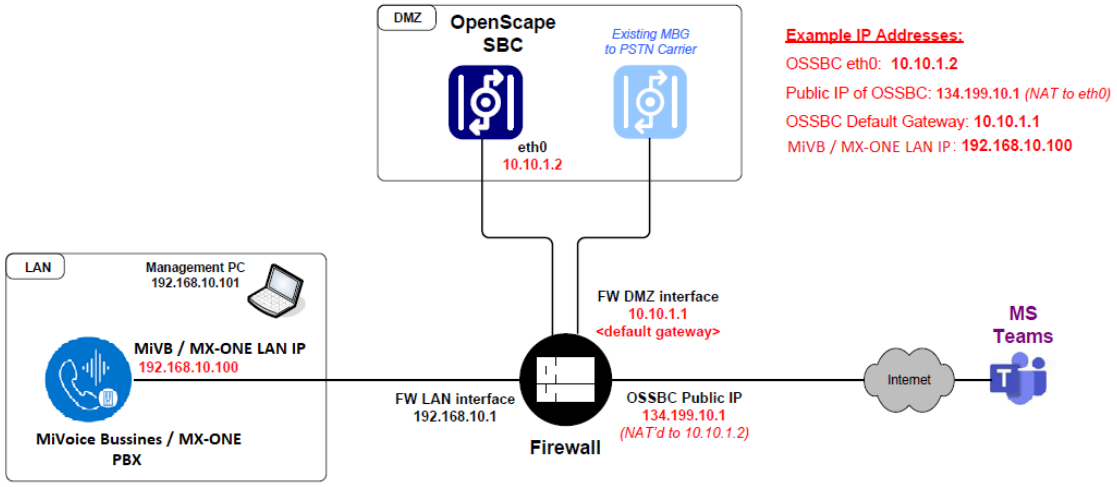


Figure 1: Single-arm Configuration

- **Multiple-arm Configuration**

  In multi-arm configuration, the OpenScape SBC is deployed across multiple network segments with a NIC connected to each, typically segregating external and internal traffic. This setup allows for more precise control over communication flows, enabling enhanced security measures.

  Firewalls may be deployed either in bridged/transparent mode or NAT mode. In OpenScape SBC, the firewall settings (external firewall configuration) for the network access realm used by Microsoft Teams must be configured with the IP address of the external firewall (WAN address). In this case, the Microsoft Teams media profile should be configured to **ICE-LITE** for **Firewall Bridged** mode (see Figure 2: Multiple-arm Configuration - Firewall Bridged Mode on page 7) and **ICE-FULL** for

Firewall NAT mode (see Figure 3: Multiple-arm Configuration - Firewall NAT Mode on page 7) because Microsoft Teams receives the external address of the firewall in the SDP.

The following figures depict the multiple-arm deployment scenarios.

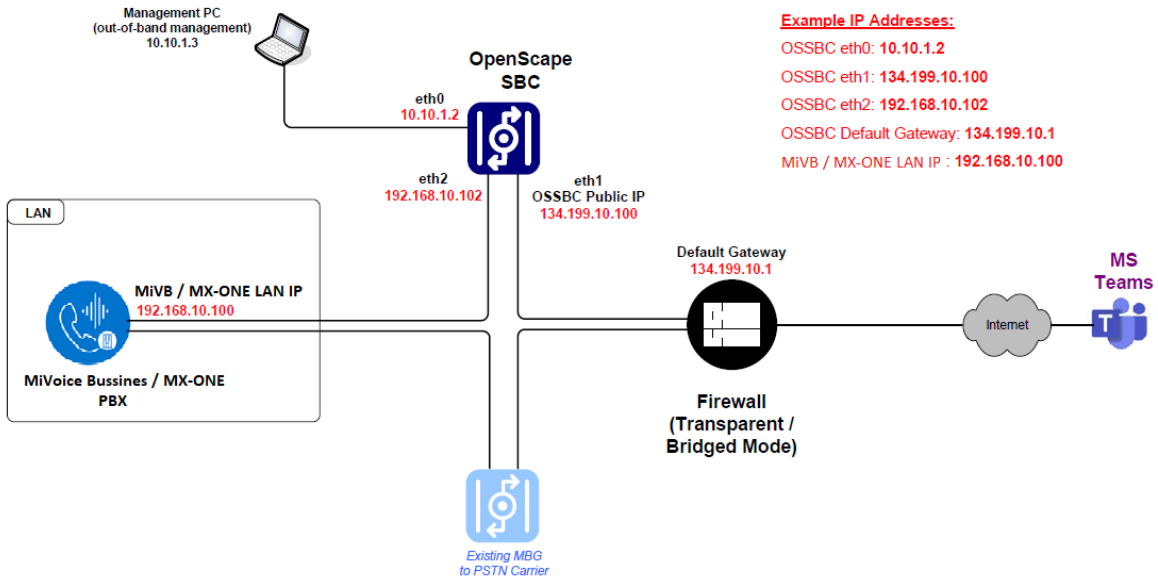


Figure 2: Multiple-arm Configuration - Firewall Bridged Mode

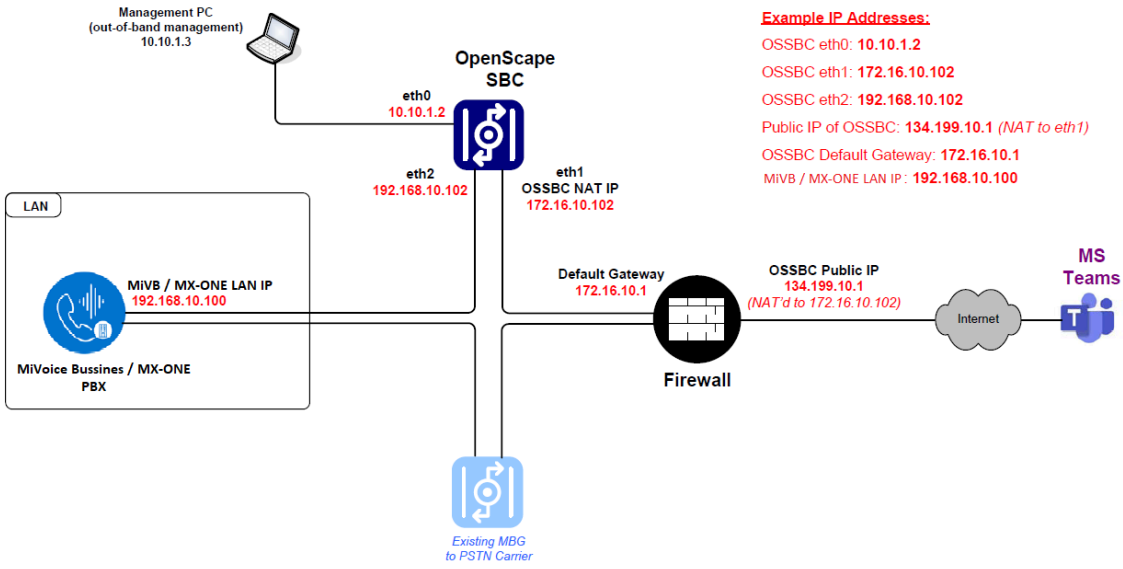


Figure 3: Multiple-arm Configuration - Firewall NAT Mode

Network Realms Configuration

OpenScape SBC also uses the concept of network realms. A realm is a logical connection associated with one network interface card. The Core Realm connects to the LAN side of OpenScape SBC, and the Access Realm connects to the WAN side of OpenScape SBC. The administrator must add the network interface to the required realm. Each realm on the OpenScape SBC can be configured using the following:

- Single IP with multiple ports

  (Or)
- Multiple IPs with single port

3.3 Software Versions

The following table lists the products included in this solution test environment and their corresponding software versions.

Note:

This section provides the **minimum** software requirements and can be extended to future software variants compatible with similar firmware.

Product	Minimum Software Version
MiVoice MX-ONE	7.6 SP1 HF0
IP Phone 69XXw	SIP 6.3.3.57
OpenScape SBC	11.0 (11 R0.05.00)
Microsoft Teams Web Client / Desktop Client / Mobile clients Android and iOS	V2

Configuring MX-ONE 4

This chapter contains the following sections:

This chapter describes the various configuration steps necessary for integrating MX-ONE with Microsoft Teams through OpenScape SBC. Most of the actions detailed in this section are performed using the MX-ONE Service Node Manager (SNM) web interface.

4.1 Assumptions

It is assumed that the SIP signaling connection uses TLS on Port 5061 for the programming of MX-ONE.

4.2 Network Requirements

The following table lists the required bandwidth to support the VoIP for MX-ONE configuration.

Table 4: Network Requirements

Ethernet Bandwidth	Voice Session (20ms Packetization)
96.8 Kbps assuming 802.1 p/Q frame	G.711
40.8 Kbps assuming 802.1 p/Q frame	G.729

For more information on network requirements, refer to the *MX-ONE Engineering Guidelines*.

4.3 Accessing Service Node Manager

Note:
User can also directly login to the SNM using the valid portal URL, such as *http://<MX-ONE_IP_Address>/wbm/loginUser.doas*.

To access the Service Node Manager (SNM) through the Provisioning Manager (PM):

1. Log in to the Provisioning Manager application with default user name and password.

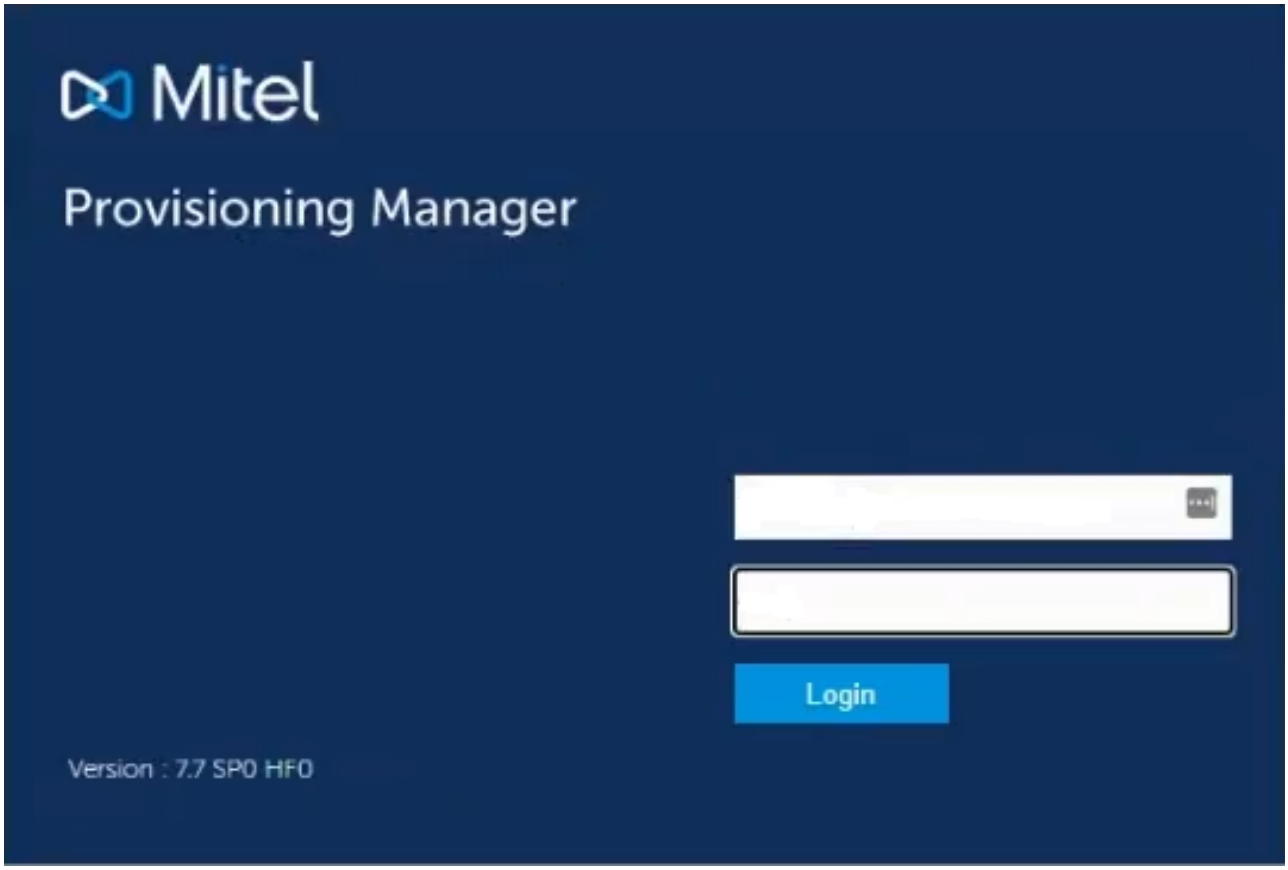


Figure 4: Provisioning Manager Login Screen

2. Navigate to **System > Subsystem > <User_Defined_Name>**. The Service Node Manager page is displayed.

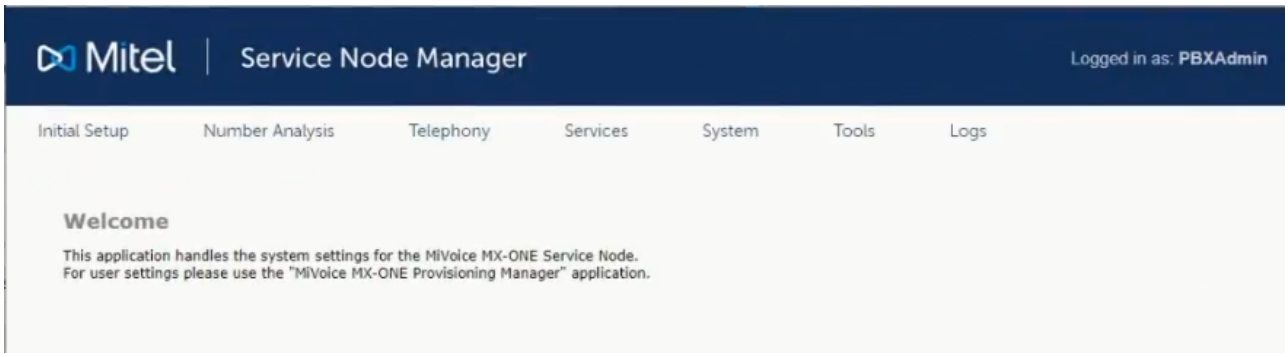


Figure 5: Service Node Manager

For more information on the SNM application, refer to the *MX-ONE Service Node Manager*.

4.4 Verifying SIP Trunk License

Ensure the MX-ONE has a SIP trunk license to connect with OpenScape SBC.

Note:

Only an **Administrator** user with **System Setup Admin Security** profile can verify the SIP trunk license status.

To verify the SIP trunk license status:

1. In the PM application, navigate to **System > Subsystem**.

2. Click on **Traditional**.

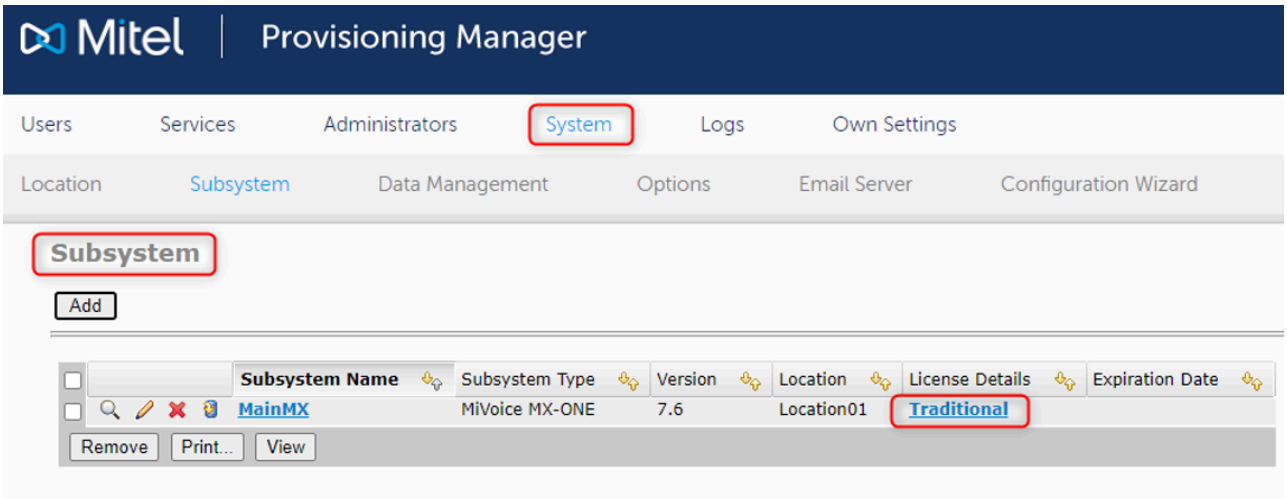
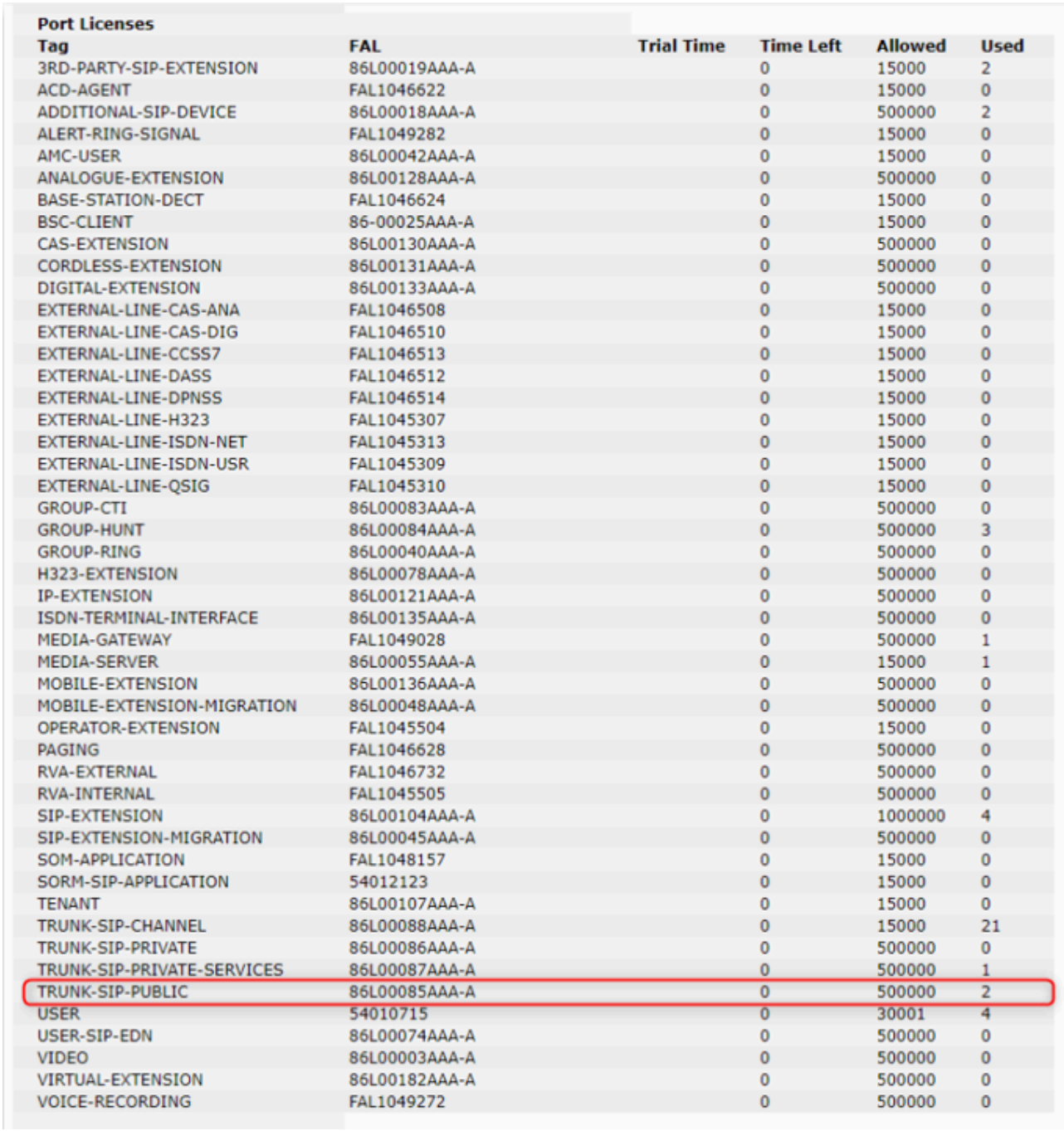


Figure 6: SIP Trunk License (1 of 2)

3. Ensure that the *TRUNK-SIP-PUBLIC* license is displayed as depicted in the following figure.



Port Licenses

Tag	FAL	Trial Time	Time Left	Allowed	Used
3RD-PARTY-SIP-EXTENSION	86L00019AAA-A		0	15000	2
ACD-AGENT	FAL1046622		0	15000	0
ADDITIONAL-SIP-DEVICE	86L00018AAA-A		0	500000	2
ALERT-RING-SIGNAL	FAL1049282		0	15000	0
AMC-USER	86L00042AAA-A		0	15000	0
ANALOGUE-EXTENSION	86L00128AAA-A		0	500000	0
BASE-STATION-DECT	FAL1046624		0	15000	0
BSC-CLIENT	86-00025AAA-A		0	15000	0
CAS-EXTENSION	86L00130AAA-A		0	500000	0
CORDLESS-EXTENSION	86L00131AAA-A		0	500000	0
DIGITAL-EXTENSION	86L00133AAA-A		0	500000	0
EXTERNAL-LINE-CAS-ANA	FAL1046508		0	15000	0
EXTERNAL-LINE-CAS-DIG	FAL1046510		0	15000	0
EXTERNAL-LINE-CCSS7	FAL1046513		0	15000	0
EXTERNAL-LINE-DASS	FAL1046512		0	15000	0
EXTERNAL-LINE-DPNSS	FAL1046514		0	15000	0
EXTERNAL-LINE-H323	FAL1045307		0	15000	0
EXTERNAL-LINE-ISDN-NET	FAL1045313		0	15000	0
EXTERNAL-LINE-ISDN-USR	FAL1045309		0	15000	0
EXTERNAL-LINE-QSIG	FAL1045310		0	15000	0
GROUP-CTI	86L00083AAA-A		0	500000	0
GROUP-HUNT	86L00084AAA-A		0	500000	3
GROUP-RING	86L00040AAA-A		0	500000	0
H323-EXTENSION	86L00078AAA-A		0	500000	0
IP-EXTENSION	86L00121AAA-A		0	500000	0
ISDN-TERMINAL-INTERFACE	86L00135AAA-A		0	500000	0
MEDIA-GATEWAY	FAL1049028		0	500000	1
MEDIA-SERVER	86L00055AAA-A		0	15000	1
MOBILE-EXTENSION	86L00136AAA-A		0	500000	0
MOBILE-EXTENSION-MIGRATION	86L00048AAA-A		0	500000	0
OPERATOR-EXTENSION	FAL1045504		0	15000	0
PAGING	FAL1046628		0	500000	0
RVA-EXTERNAL	FAL1046732		0	500000	0
RVA-INTERNAL	FAL1045505		0	500000	0
SIP-EXTENSION	86L00104AAA-A		0	1000000	4
SIP-EXTENSION-MIGRATION	86L00045AAA-A		0	500000	0
SOM-APPLICATION	FAL1048157		0	15000	0
SORM-SIP-APPLICATION	54012123		0	15000	0
TENANT	86L00107AAA-A		0	15000	0
TRUNK-SIP-CHANNEL	86L00088AAA-A		0	15000	21
TRUNK-SIP-PRIVATE	86L00086AAA-A		0	500000	0
TRUNK-SIP-PRIVATE-SERVICES	86L00087AAA-A		0	500000	1
TRUNK-SIP-PUBLIC	86L00085AAA-A		0	500000	2
USER	54010715		0	30001	4
USER-SIP-EDN	86L00074AAA-A		0	500000	0
VIDEO	86L00003AAA-A		0	500000	0
VIRTUAL-EXTENSION	86L00182AAA-A		0	500000	0
VOICE-RECORDING	FAL1049272		0	500000	0

Figure 7: SIP Trunk License (2 of 2)

4.5 Configuring SIP Routing

It is recommended to use the existing public routing to connect the OpenScape SBC. This routing must be used for all external calls, such as Microsoft Teams and PSTN.

To configure SIP routing:

1. In the SNM application, navigate to **Telephony > External Lines > Route**.
2. Configure **General**.

   a. Set **Route Number** as **1**.
   b. Set **Route Name** as **SBC**.
   c. Set **Customer Group** as **None**.
   d. Select **Open for Incoming Traffic**.
   e. Set **Line Selection During Outgoing Traffic** as **Even Seizure in server**.
   f. Set **Route Characteristics Outgoing Traffic** as **Normal route**.
   g. Select **Allow Number Conversion**.
   h. Set **Dial Tone Characteristics after Eternal Line Seizure** as **A-party has monitoring path**.
   i. Deselect **User of Digit Transmission for Transit Exchange**.
   j. Set **Ringing Tone Transmission for Outgoing Traffic** as **A-party receives ringing tone**.

The following figure depicts the sample **General** configuration.

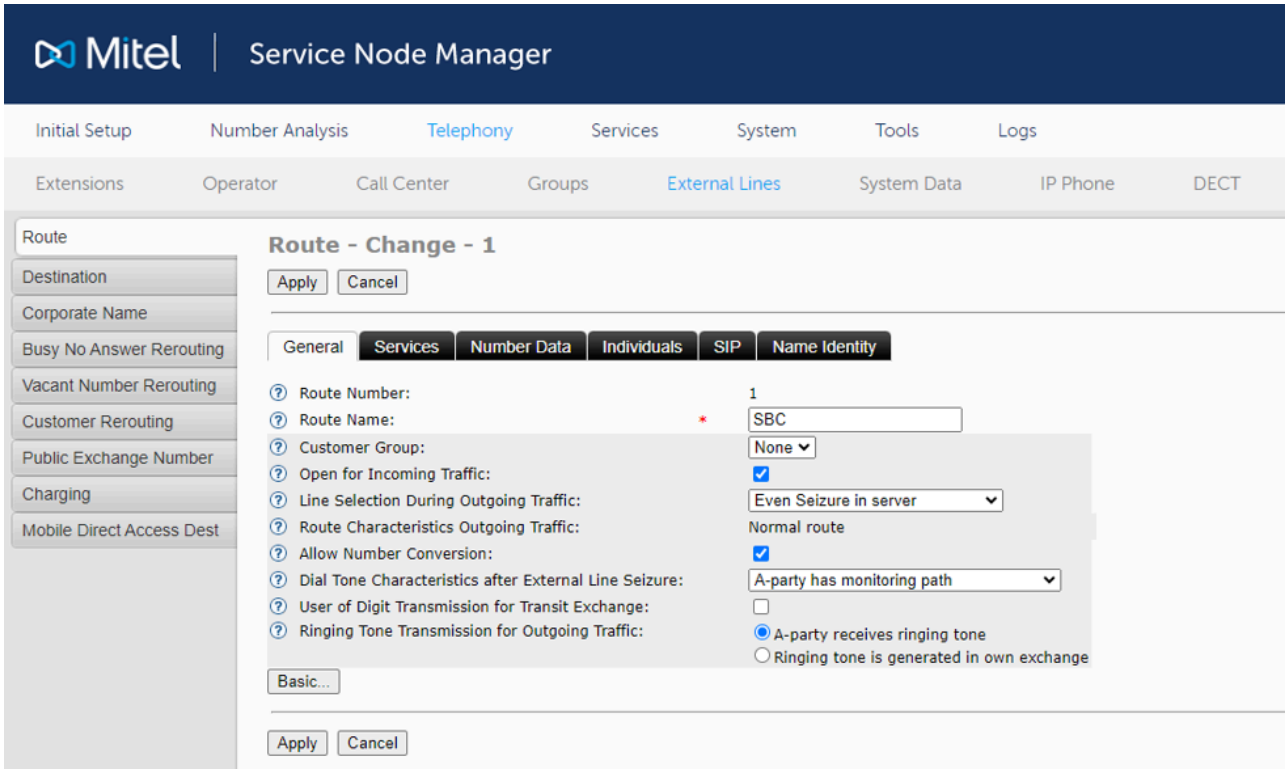


Figure 8: SIP Routing: General Configuration

3. Configure **Services**.

   a. Deselect **Rerouting on Congestion**.
   b. Deselect **Rerouting on Busy**.
   c. Deselect **Rerouting on no Answer**.
   d. Select **Allow Initiation of Call Waiting Tone Transmission**.
   e. Select **Allow Reception of Call Waiting Tone and Intrusion**.
   f. Set **Call Discrimination Group Night for Incoming External Lines** as **Fully Open**.
   g. Set **Call Discrimination Group Day for Incoming External Lines** as **Fully Open**.
   h. Set **Traffic Connection Class** as **Fully Open**.
   i. Select **Allow Alternative Route Selection**.
   j. Set **Presentation of Calling / Connected Number** as **Controlled by the extension**.
   k. Deselect **Mobile Extension without R1 Number**.
   l. Set **Abbreviated Dialing Traffic Class** as **0**.

The following figure depicts the sample **Services** configuration.

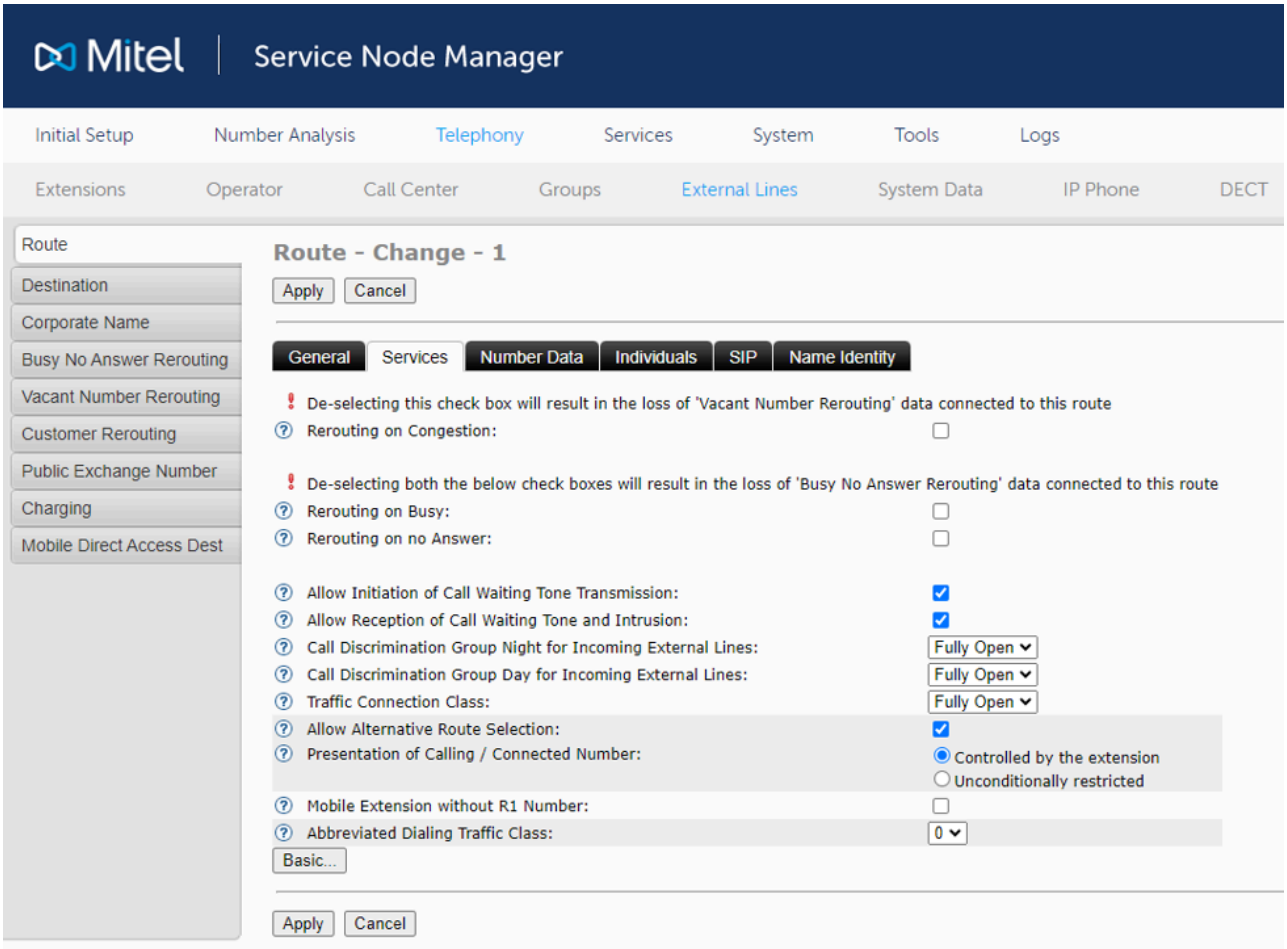


Figure 9: SIP Routing: Services Configuration

4. Configure **Number Data**.

   a. Configure **Prefix Number Data** as follows:

      i. Set **Prefix Digits for Private Calling Number** as environment specific value.
      ii. Set **Private Type of Number** as environment specific value.
      iii. Set **Prefix Digits for Public Calling Number** as environment specific value.
      iv. Set **Public Type of Number** as environment specific value.
      v. Set **Predigits for Direct In-dialing Traffic** as environment specific value.
      vi. Set **Route Directory Number** as environment specific value.
      vii. Set **Terminating Area Code for Route** as environment specific value.

   b. Configure **Public Exchange Data** as follows:

      i. Set **Unknown Number for Public Exchange** as environment specific value.
      ii. Set **International Number for Public Exchange** as environment specific value.
      iii. Set **National Number for Public Exchange** as environment specific value.
      iv. Set **Network Specific Number for Public Exchange** as environment specific value.
      v. Set **Local Public Number for Public Exchange** as environment specific value.

The following figure depicts the sample **Number Data** configuration.

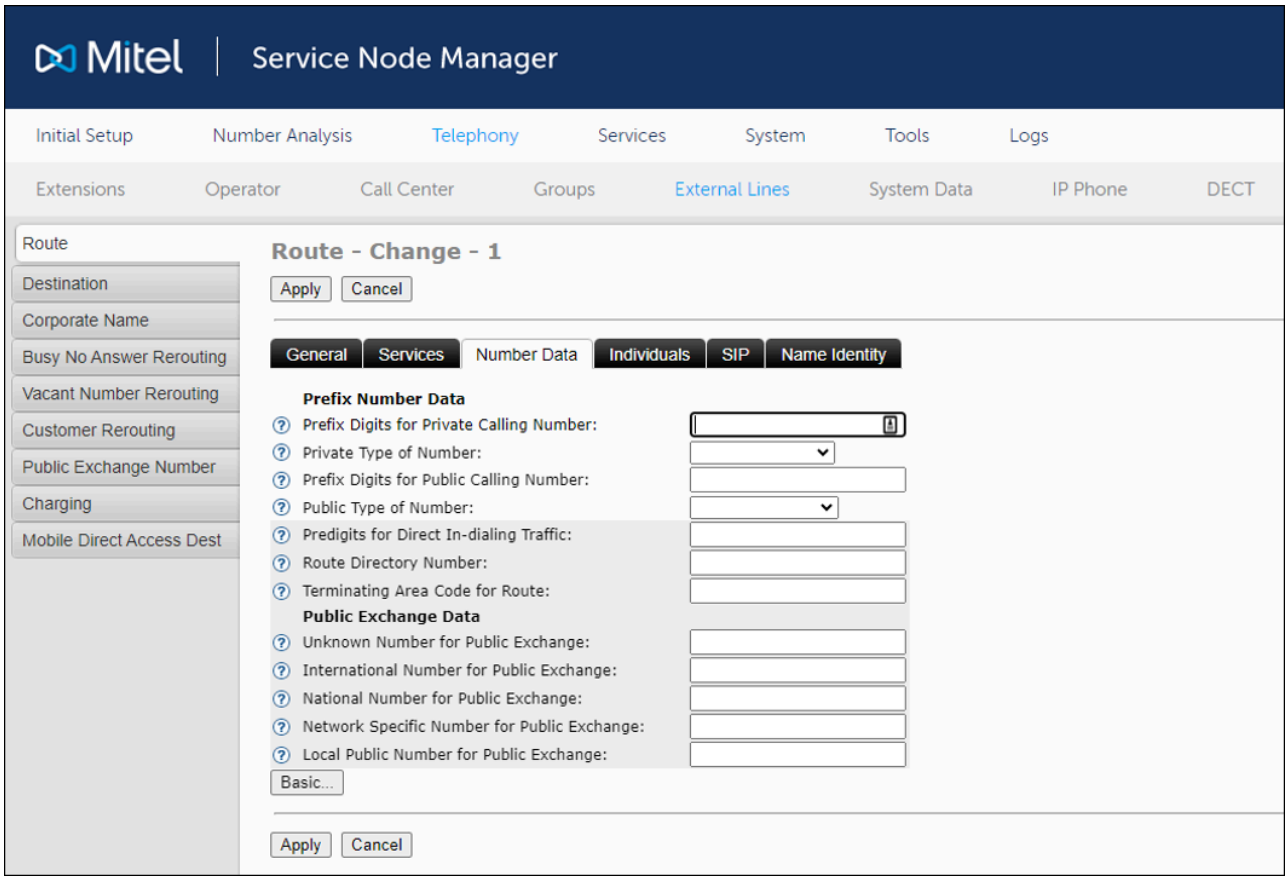


Figure 10: SIP Routing: Number Data Configuration

5. Configure **Individuals**.

   a. Set **Server** as **1**.
   b. Set **Trunk Index** as **1-10**.

The following figure depicts the sample **Individuals** configuration.

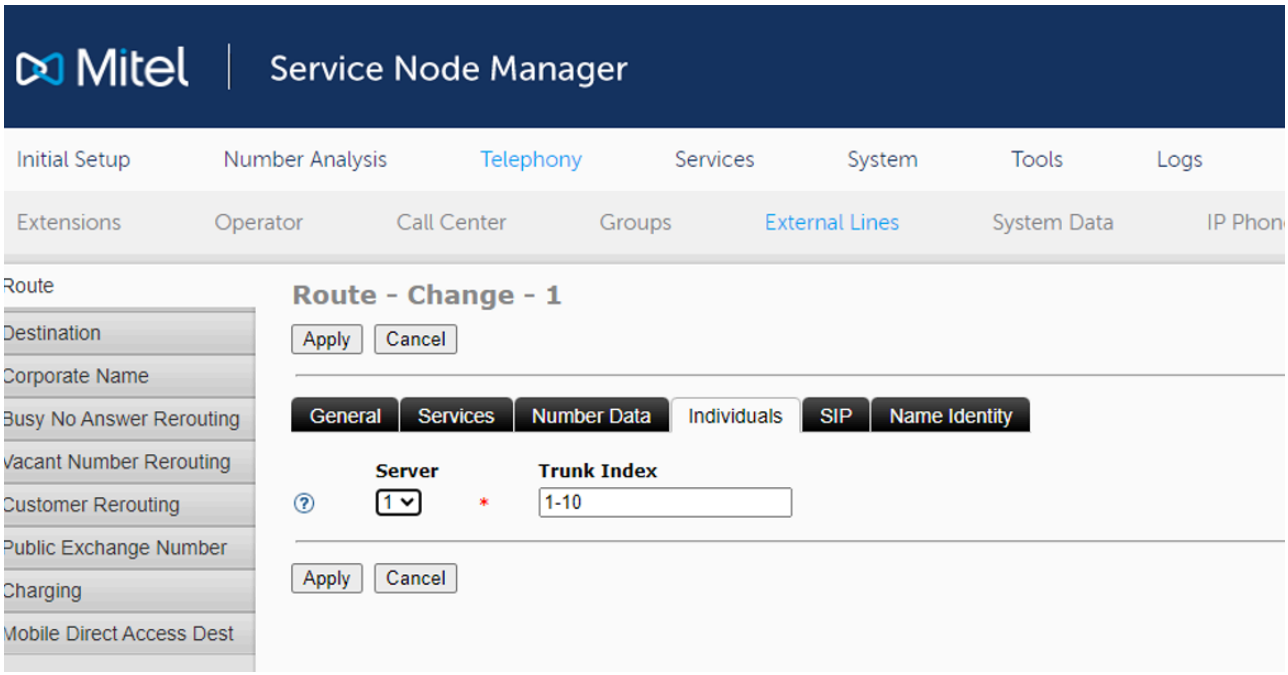


Figure 11: SIP Routing: Individuals Configuration

6. Configure **SIP**.

   a. Set **Password for Trunk Registration** as environment specific value.
   b. Set **Trusted Privacy Domain** as **Asserted Identity**.
   c. Configure **Outgoing Traffic** as follows:

      i. Set **Protocol to Use When Calling** as **TLS**.
      ii. Set **Proxy Address** as environment specific value, which points to OpenScape SBC.
      iii. Set **Proxy Port Number** as **5061**.
      iv. Set **Remote Port** as **5061**.
      v. Set **Remote IP Address for Tel** as environment specific value.
      vi. Set **Remote Extension from URI** as environment specific value.
      vii. Set **Remote Extension String** as environment specific value.
      viii. Set **RouteSet** as environment specific value.
   d. Configure **Invite URI String for** as follows:

      i. Set **Unknown Public Number** as environment specific value, which points to OpenScape SBC.
      ii. Set **International Number** as environment specific value.
      iii. Set **National Number** as environment specific value.
      iv. Set **Network Specific Number** as environment specific value.
      v. Set **Local Public Number** as environment specific value.
      vi. Set **Unknown Private Number** as environment specific value.
      vii. Set **Local Private Number** as environment specific value.
      viii. Set **Level 1 Regional Number** as environment specific value.
   e. Configure **From URI String for** as follows:

      i. Set **Unknown Public Number** as environment specific value, the MX-ONE IP is used.
      ii. Set **International Number** as environment specific value.
      iii. Set **National Number** as environment specific value.
      iv. Set **Network Specific Number** as environment specific value.
      v. Set **Local Public Number** as environment specific value.
      vi. Set **Unknown Private Number** as environment specific value.
      vii. Set **Local Private Number** as environment specific value.
      viii. Set **Level 1 Regional Number** as environment specific value.
   f. Configure **Incoming Traffic** as follows:

      i. Set **Type of Accepted Calls** as **Remote IP**.
      ii. Set **Addresses or Numbers to Match Incoming Call** as environment specific value, which points to the OpenScape SBC.
      iii. Set **Emergency Callback Destination Number** as environment specific value.
      iv. Set **Priority for Incoming Calls** as **255**.
   g. Configure **Context String for A Party** as follows:

      i. Set **Unknown Public Number** as environment specific value.

ii. Set **International Number** as environment specific value.
iii. Set **National Number** as environment specific value.
iv. Set **Network Specific Number** as environment specific value.
v. Set **Local Public Number** as environment specific value.
vi. Set **Unknown Private Number** as environment specific value.
vii. Set **Local Private Number** as environment specific value.
viii. Set **Level 1 Regional Number** as environment specific value.

h. Configure **Context String for B Party** as follows:

i. Set **Unknown Public Number** as environment specific value.
ii. Set **International Number** as environment specific value.
iii. Set **National Number** as environment specific value.
iv. Set **Network Specific Number** as environment specific value.
v. Set **Local Public Number** as environment specific value.
vi. Set **Unknown Private Number** as environment specific value.
vii. Set **Local Private Number** as environment specific value.
viii. Set **Level 1 Regional Number** as environment specific value.

i. Configure **Third Party Registration** as follows:

i. Set **Type of Registration** as **No Registration**.
ii. Set **Number Range to Handle** as environment specific value.
iii. Set **Registration Host Port Number** as environment specific value.
iv. Set **Realm** as environment specific value.
v. Set **Register String** as environment specific value.
vi. Set **Time before Re-registering(s)** as environment specific value.
vii. Set **Local Domain** as environment specific value.
viii. Set **Supervise** as environment specific value.
ix. Set **Supervise Time** as environment specific value.
x. Set **Authname for Trunk Registration** as environment specific value.

j. Configure **Signal Diagram for Common Incoming and Outgoing Traffic** as follows:

i. Set **Crypto offer** as **SAVP**.
ii. Select **May use replaces to update remote end**.
iii. Select **May use early replaces to update remote end**.
iv. Set **Gateway mode** as **Use any gateway to minimize IP hops. Use session timer**.
v. Select **Use SIP-URI parameter user-phone**.
vi. Deselect **Enforce data media pass through, modem and fax**.
vii. Deselect **Service route**.
viii. Deselect **Do not display name received from external party**.
ix. Set **SDP restrictions** as **No restrictions**.
x. Deselect **Request End to End DTMF signaling from other side**.
xi. Deselect **Use inband DTMF instead of INFO when RFC2833 is not used**.

k. Configure **Signal Diagram for Incoming Traffic** as follows:

i. Select **Use history Information from network (RFC4244)**.
ii. Select **Use diversion Information from network (RFC5806)**.
iii. Select **Use Referred-by Information from network (RFC3892)**.
iv. Set **Rva media mode** as **Rva uses early media**.
v. Select **Send 181 'call is being forwarded'**.

l. Configure **Signal Diagram for Outgoing Traffic** as follows:

i. Deselect **Treat 404, 485 and 604 as network congestion**.
ii. Select **Send history information**.
iii. Select **Send diversion information**.
iv. Deselect **Request End to End DTMF Signaling**.
v. Deselect **Use Contact field to update called (answering) information at seizure**.
vi. Deselect **Treat session progress (183) as ringing (180)**.
vii. Set **Number of Seconds before Sending INVITE** as **4**.
viii. Set **Number of Seconds for Answer to INVITE** as **1**.

The following figures depict the sample **SIP** configuration.

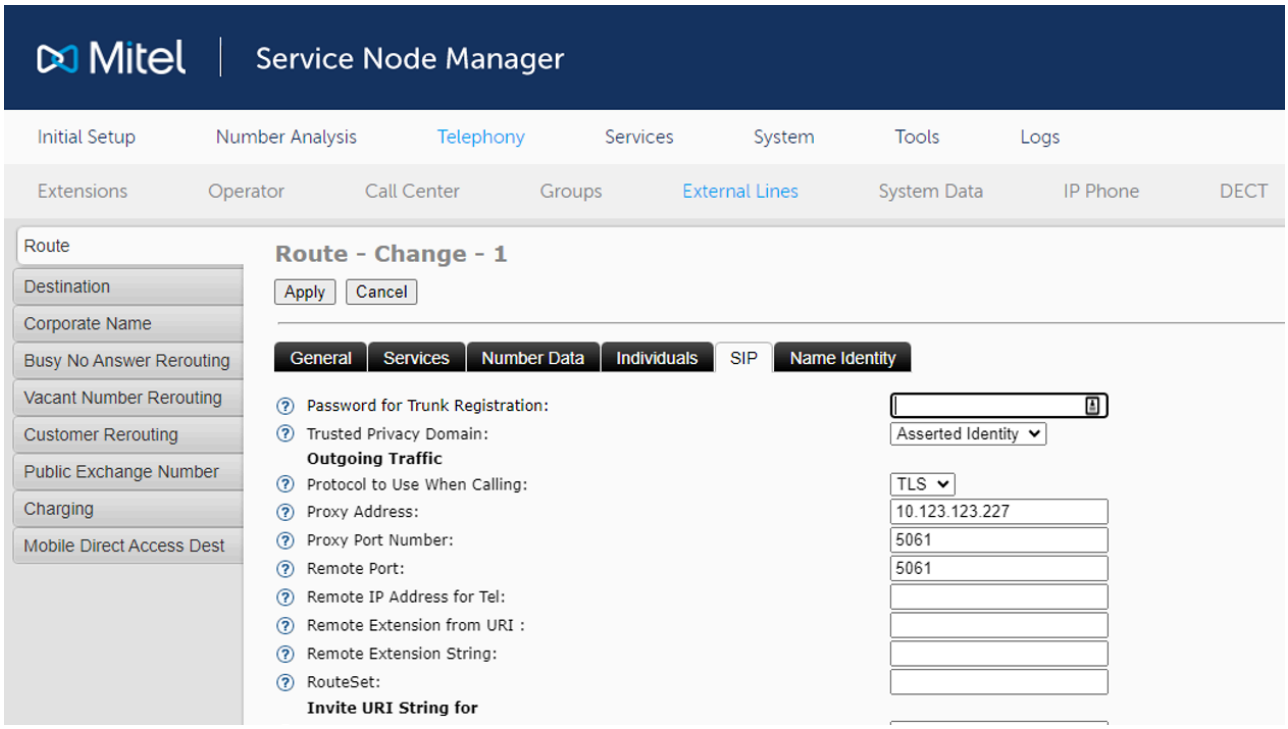


Figure 12: SIP Routing: SIP Configuration (1 of 4)

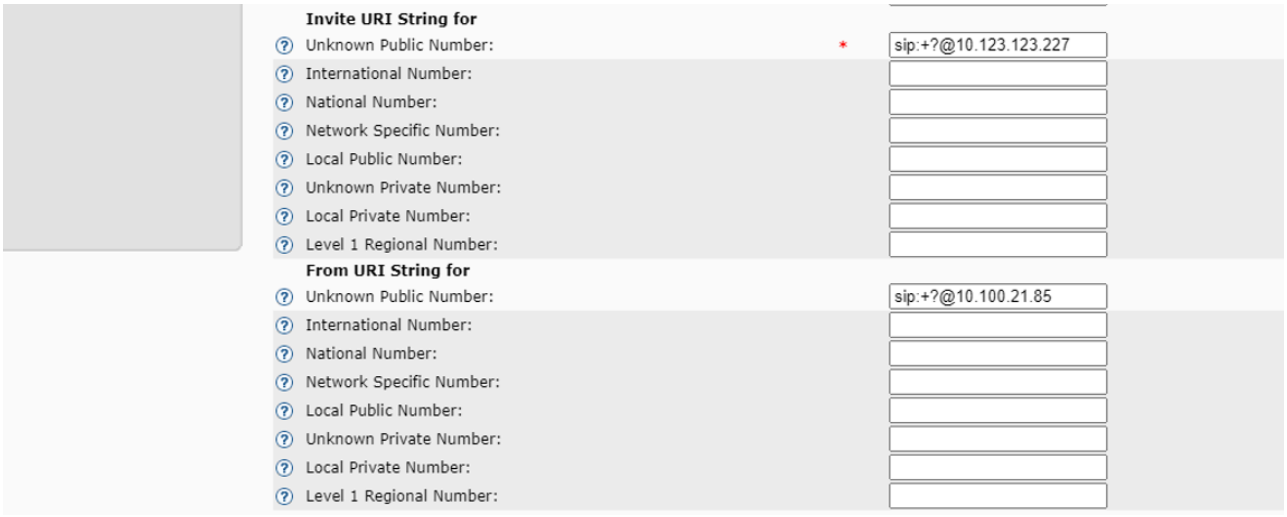


Figure 13: SIP Routing: SIP Configuration (2 of 4)

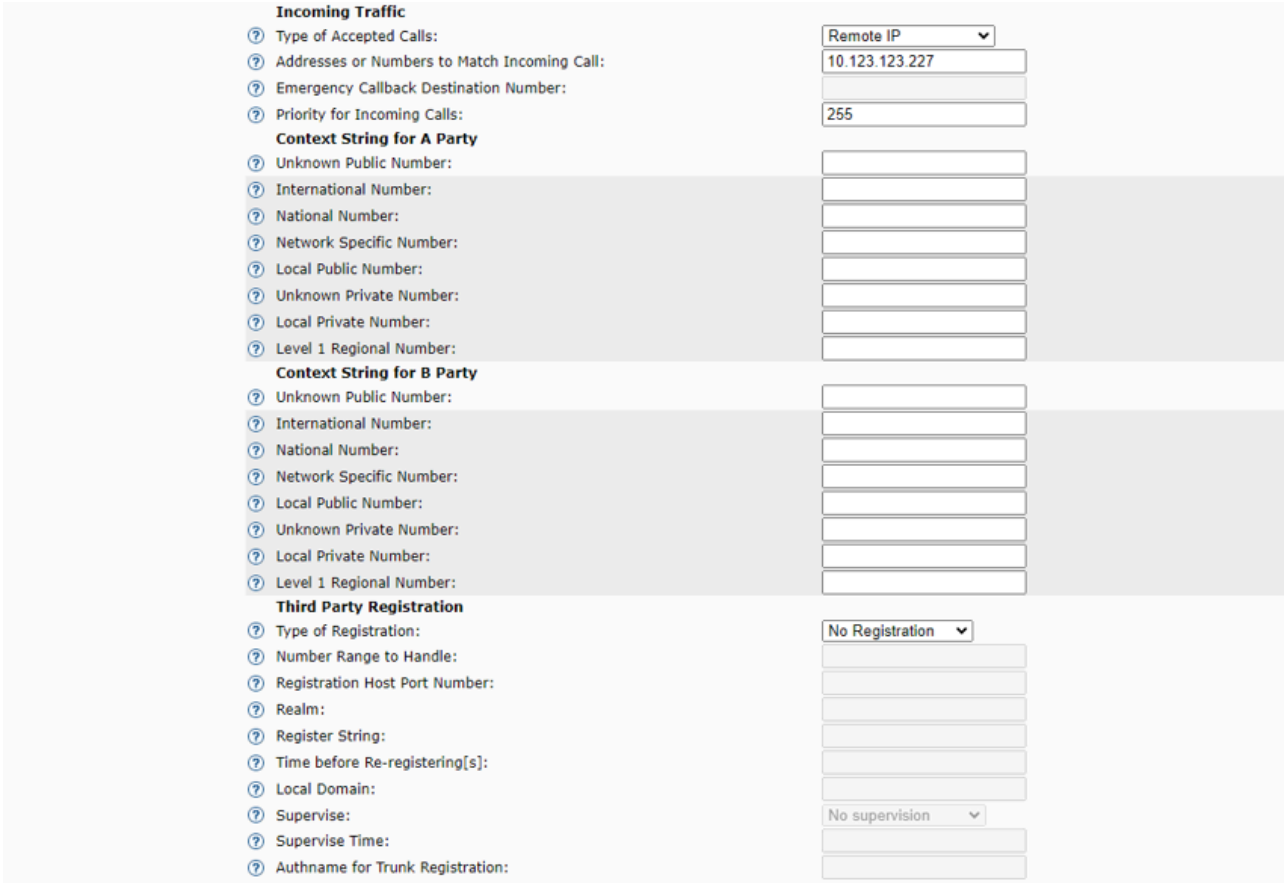


Figure 14: SIP Routing: SIP Configuration (3 of 4)

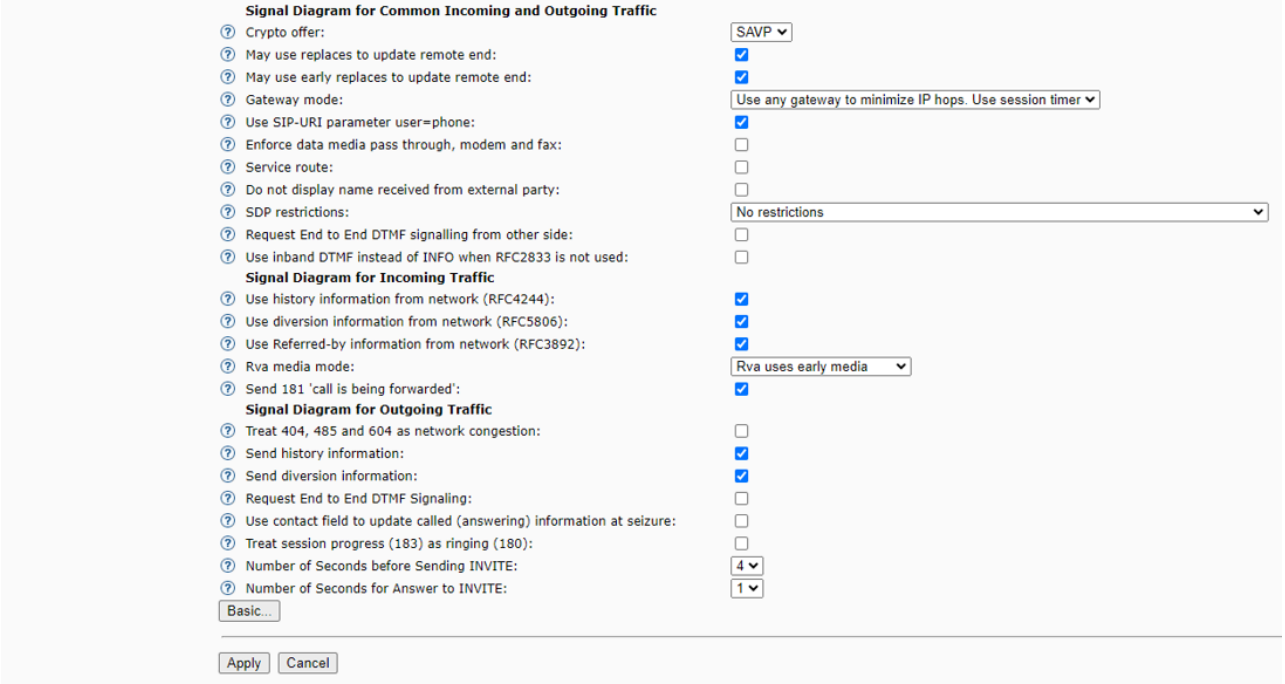


Figure 15: SIP Routing: SIP Configuration (4 of 4)

7. Configure **Name Identity**.

a. Set **First Name** as environment specific value.
b. Set **Last Name** as environment specific value.
c. Set **Name Presentation Order** as **First part of name is presented**.

The following figure depicts the sample **Name Identity** configuration.

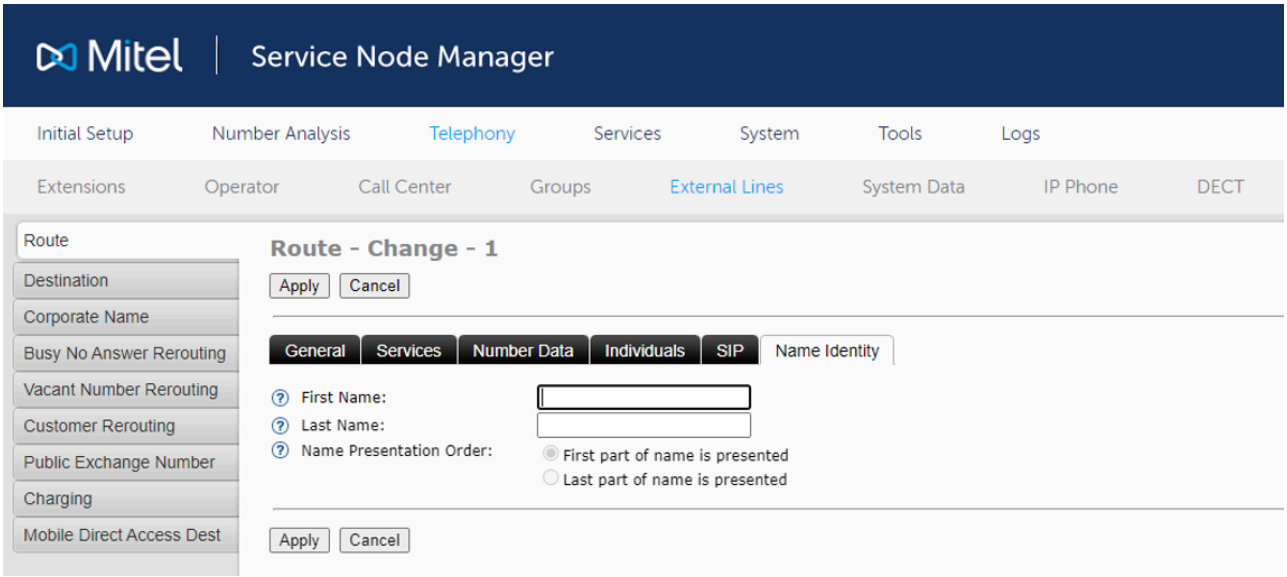


Figure 16: SIP Routing: Name Identity Configuration

8. Click on **Apply** to save the SIP route configuration.

4.6 Configuring SIP Invite Message

This section describes how to configure SIP Invite Messages by adding Session Description Protocol (SDP).

To configure SIP invite messages:

1. Log in to the MX-ONE system.
2. Execute the following command to change the permission to root user.

```
su
```

3. Navigate to the */etc/opt/eri_sn/sip_trunk_profiles* directory.
4. Open the *default.conf* file.
5. Search and update the following value from **no** to **yes** in a *default.conf* file.

```
TrunkProfile:Default:MediaRequiredInFirstProvisional: yes
```

6. Save and close the *default.conf* file.
7. Execute the following command to take the backup of the existing configuration.

```
data_backup
```

8. Execute the following command to start the system.

```
start--system
```

9. Execute the following command to force use the *sip_route* to regenerate the updated profile.

```
sip_route -set -route 1 -protocol tls
```

In this command, the value **1** indicates the route number, and it is environment specific.

4.7 Configuring Secure Real-Time Transport Protocol

This section describes how to configure Secure Real-Time Transport Protocol (SRTP).

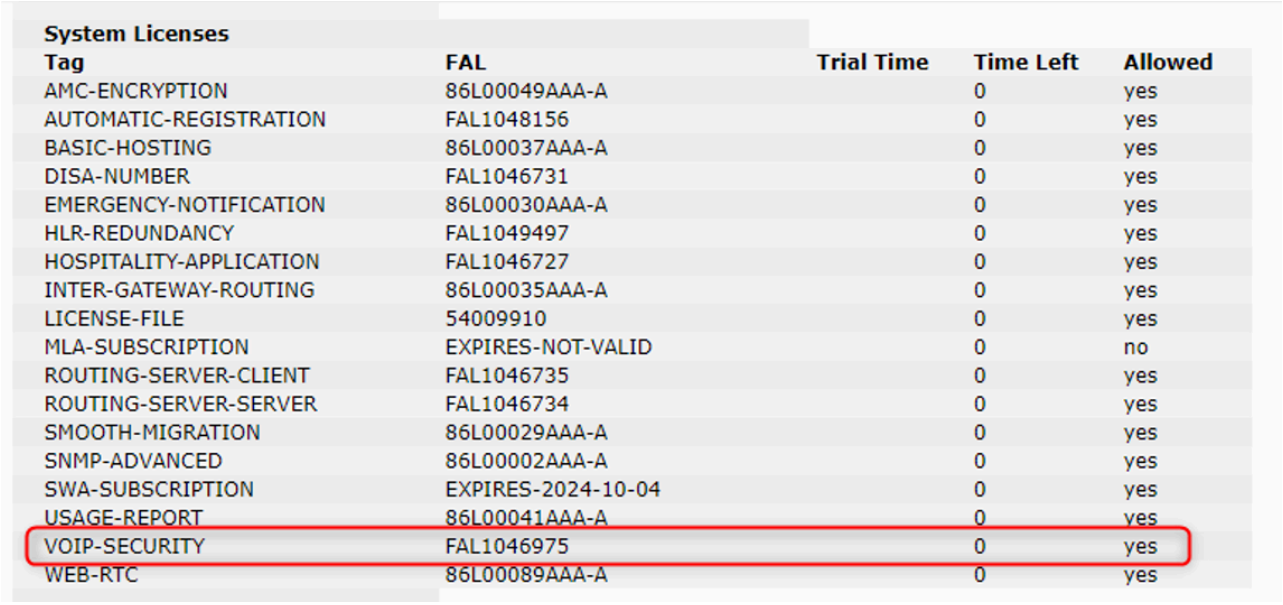
Prerequisites

Ensure that the *VOIP-SECURITY* license is used for the media encryption.

To verify the VoIP security license status:

1. In PM interface, navigate to the **System > Subsystem > License Details**.
2. Click on **Traditional**.

3. Ensure that the *VOIP-SECURITY* license is displayed as depicted in the following figure.



System Licenses

Tag	FAL	Trial Time	Time Left	Allowed
AMC-ENCRYPTION	86L00049AAA-A		0	yes
AUTOMATIC-REGISTRATION	FAL1048156		0	yes
BASIC-HOSTING	86L00037AAA-A		0	yes
DISA-NUMBER	FAL1046731		0	yes
EMERGENCY-NOTIFICATION	86L00030AAA-A		0	yes
HLR-REDUNDANCY	FAL1049497		0	yes
HOSPITALITY-APPLICATION	FAL1046727		0	yes
INTER-GATEWAY-ROUTING	86L00035AAA-A		0	yes
LICENSE-FILE	54009910		0	yes
MLA-SUBSCRIPTION	EXPIRES-NOT-VALID		0	no
ROUTING-SERVER-CLIENT	FAL1046735		0	yes
ROUTING-SERVER-SERVER	FAL1046734		0	yes
SMOOTH-MIGRATION	86L00029AAA-A		0	yes
SNMP-ADVANCED	86L00002AAA-A		0	yes
SWA-SUBSCRIPTION	EXPIRES-2024-10-04		0	yes
USAGE-REPORT	86L00041AAA-A		0	yes
VOIP-SECURITY	FAL1046975		0	yes
WEB-RTC	86L00089AAA-A		0	yes

Figure 17: VOIP-SECURITY License

Configuring SRTP

To configure the Secure Real-Time Transport Protocol (SRTP):

1. Log in to the MX-ONE system as a **mxone_admin** user.
2. Execute the following commands to configure the SRTP.

```
media_encryption_enable -type extension
```

```
media_encryption_enable -type route
```

3. Execute the following command to verify the SRTP status.

```
media_encryption_print
```

4.8 Configuring Destination Number

This section describes the procedure to add the destination number for the external dialed numbers, and to link the destination number for the OpenScape SBC.

Adding Destination Number

To add the destination number:

1. In SNM application, navigate to the **Number Analysis > Number Plan > Number Series**.
2. Set **Select the Number Series Type** as **All**.

3. Click **View**. All the external numbers are displayed.
4. Select the external number and click on edit icon.
5. Configure the **External Destination** as **0**. This parameter is environment specific.
6. Click on **Apply** to add the destination number as depicted in the following figure.

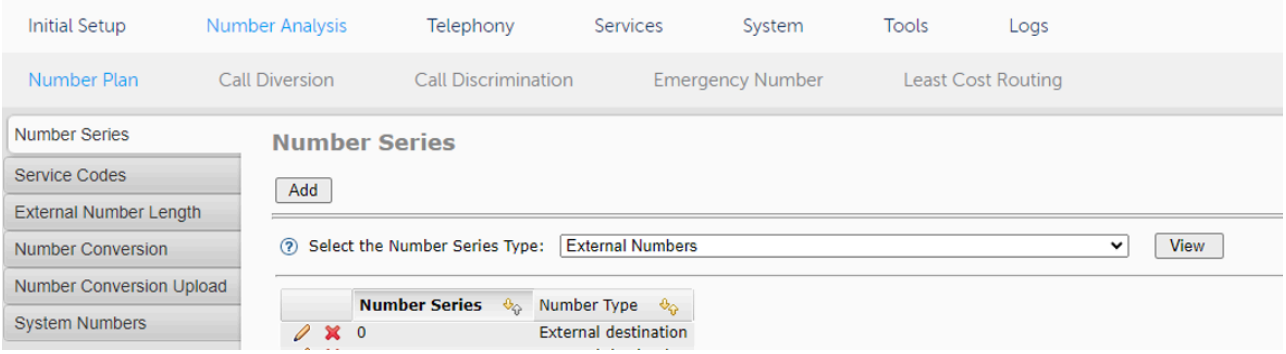


Figure 18: Adding Destination Number

Linking Destination Number

To link the destination number to the OpenScape SBC:

1. In the SNM application, navigate to **Telephony > External Lines**.
2. From the left side navigation tree, click on **Destination**.

3. Click on **Add** to link the exit code created in Adding Destination Number on page 24.

   a. Set **Destination** as **0**.
   b. Set **Route name** as **SBC**.
   c. Set **Start Position for Digit Transmission** as **4**.
   d. Set **Type of Seizure of External Line** as **Seizure when minimum length attained**.
   e. Deselect **Forward Switching**.
   f. Set **Type of Called Number** as **Unknown private**.
   g. Set **Type of Calling Public Number** as **International**.
   h. Set **Type of Calling Private Number** as **Unknown private**.
   i. Deselect **Use as Emergency Destination**.
   j. Set **Pre-digits in order to form a new External Number** as environment specific value.
   k. Set **Truncated Digits in Dialed Number** as **0**.
   l. Set **Type of Signal Seizure** as **Terminating seizure**.
   m. Select **B-Answer Signal Available**.
   n. Deselect **Allow to send Traveling Class Mark**.
   o. Set **Route Type** as **Public**.
   p. Set **Maximum Number of Transit Exchanges** as **25**.
   q. Set **PNR Number Translation Information** as **No Translation**.
   r. Set **Supplementary Services Using User to User Interface** as **Not Allowed**.
   s. Deselect **Use Least Cost Routing for All Calls**.
   t. Deselect **Allow Sending of Expensive Route Warning Tone**.
   u. Set **Type of Protocol to use for Supplementary Service Call Offer** as **User to User Interface(UUI)**.
   v. Set **Type of Protocol for Call Back/Call Completion** as **User to User Interface(UUI)**.
   w. Select **Show Original A-Number**.
   x. Select **Use Original A-Number's Type of Number**.
   y. Select **Enable Enhanced Sent A-Number Conversion**.
   z. Deselect **Use ETSI Diversion Supplementary Service**.

The following figure depicts the sample **Destination** configuration.

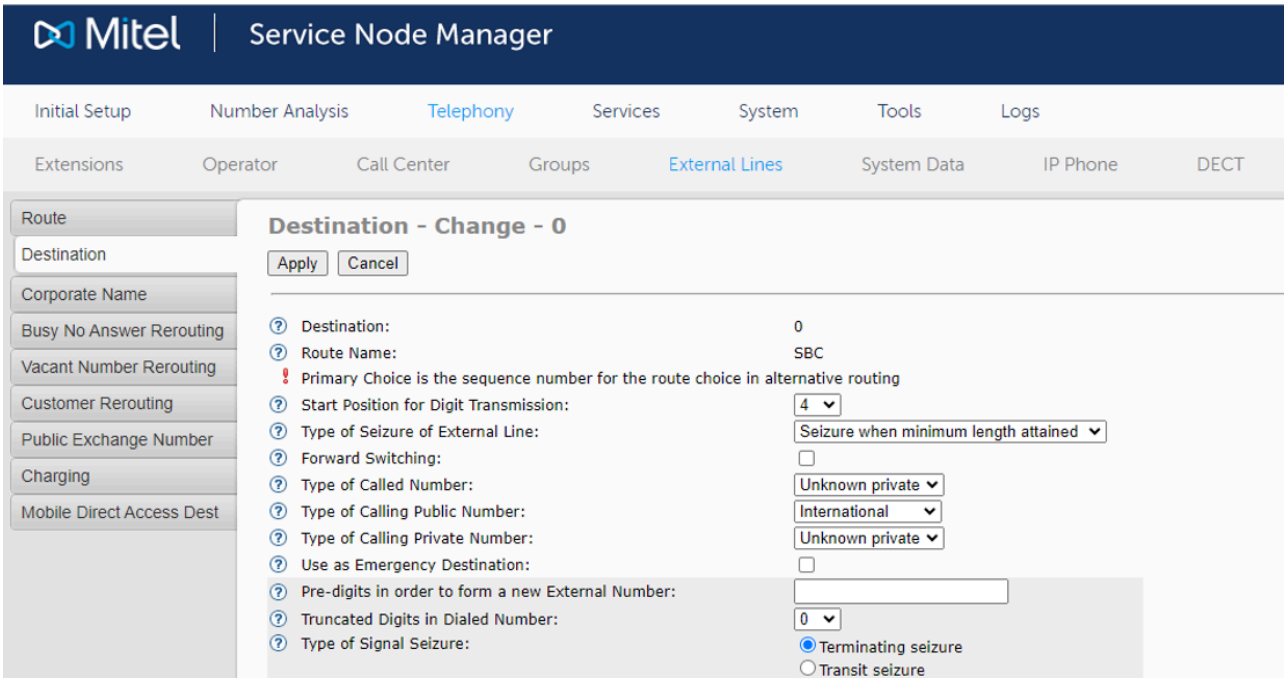


Figure 19: Linking Destination Number (1 of 2)

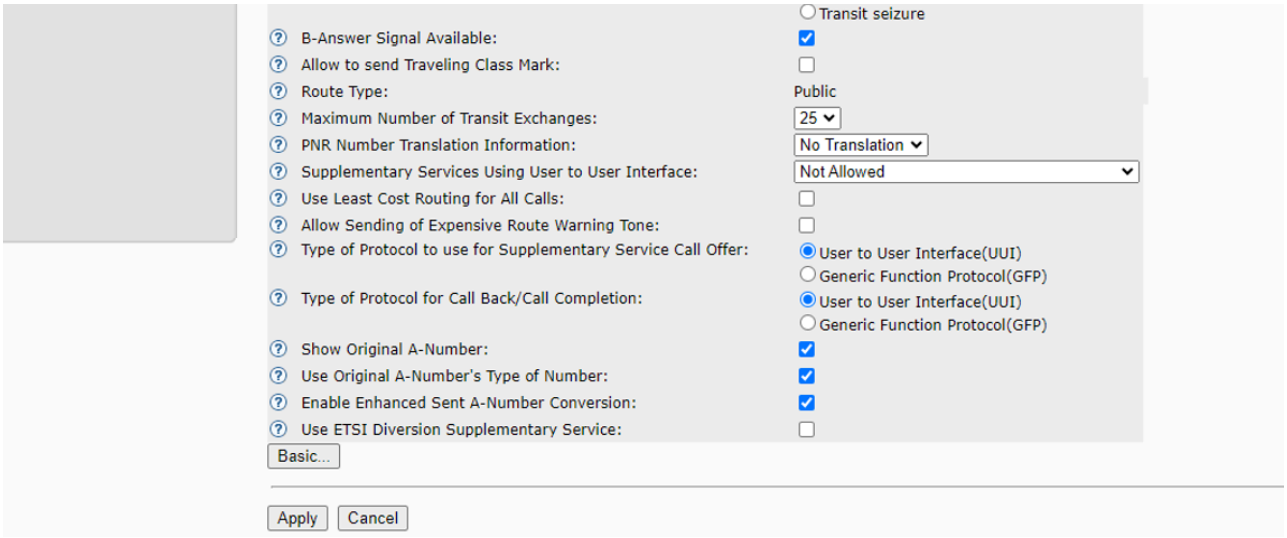


Figure 20: Linking Destination Number (2 of 2)

4. Click **OK**.
5. Click on **Apply** to save the destination configuration.

4.8.1 Example Scenario

Scenario: Make an outbound call by dialing 0 (exit code) followed by 004961513599687 (Microsoft Teams or PSTN international number).

Result: MX-ONE automatically removes first three digits (000) and starts the transmission from fourth digit (4961513599687) to make a call.

Installing OpenScape SBC 5

This chapter contains the following sections:

The following methods are used to install the OpenScape SBC, you can choose either of the following methods to install the OpenScape SBC:

- Using OVA File on page 28 **(recommended)**
- Using OVF Files on page 31

5.1 Using OVA File

This section describes installing the OpenScape SBC on a Virtual Machine using the Open Virtual Appliance (OVA) file.

5.1.1 Prerequisite

Important:
You must use SBC version 11.0 or higher as the minimum requirement.

The following are the prerequisites to install the OpenScape SBC virtual machine:

- Ensure that you have downloaded the latest available *vApps_oss-11.00.XX.YY.zip* package from the Software Download Center.
- The server hardware is installed.
- The VMware and vSphere Host client is operational.

Note:

This section describes the installation steps performed on the **VMWare ESXi Host Client**.

5.1.2 Installing OpenScape SBC Using OVA File

To install the SBC on the Virtual Machine using the OVA file:

1. Log in to the **VMWare ESXi Host Client**.

2. From the left side navigation tree, click on **Virtual Machines**.
3. On the main page, click on **Create / Register VM**.
4. Choose **Select creation Type** as **Deploy a virtual machine from an OVF or OVA file**.
5. Click **NEXT**.
6. Enter the virtual machine name on the **Enter a name for the virtual machine** field.
7. Click on **Click to select files or drag/drop** to upload the OVF file.
8. Select the *image_oss-11.00.XX.YY.ova* file that is downloaded in Prerequisite on page 28.
9. Click **NEXT**.
10. On the **Select Storage** page, select the **datastore** and click on **NEXT**.
11. Configure the **Deployment options**.

    a. Configure Network mappings:

        i. Set **LAN** as an environment-specific value.
        ii. Set **WAN** as an environment-specific value.

    b. Set **Disk provisioning** as **Thick Lazy Zero**.
    c. Select **Power on automatically**.
12. Click **NEXT**.
13. On **Ready to complete** page, verify the configuration details, and click on **FINISH**.

    On **Virtual Machines** page, a new entry is created based on the configuration.
14. Click on the new entry (created for SBC installation) to view the OVA file uploading process. Wait for the OVA file to upload.

    After the OVA file upload is complete, the VM command prompt starts automatically.

5.1.3 Configuring IP Address

Note:
The OVA file is pre-configured with the IP addresses, and it must be reconfigured as per the site environment.

To configure the default IP address:

Note:
In case of a system reboot before completing all configuration steps via the GUI, use the CLI commands again to restore access to the SBC system.

1. Log in to the SBC server as a **root** user. For information on default user name and password, see Appendix B: Default User Name and Password on page 121.

2. Execute the following commands to update the IP address.

```
ip address flush dev eth0
```

```
ip address add 10.10.1.2/24 dev eth0
```

In this command,

- **10.10.1.2** indicates the IP address. This value is environment specific.
- **24** indicates the netmask. This value is environment specific.

3. Execute the following commands to update the default gateway.

```
ip route del default
```

```
ip route add default via 10.10.1.1
```

In this command, 10.10.1.1 indicates the default gateway. This value is environment specific.

4. Log in to the SBC GUI with the IP address configured in **Step 2**. For example, *https://10.10.1.2/*
5. Navigate to the **Network/Net Services > Settings**.

The **Network/Net Services** pop-up window appears.

6. Configure the **Network/Net Services**.

Note:

In **Network/Net Services** configuration, configure the number of interfaces according to the deployment model. The number of interfaces must match the number of virtual cards on virtual machine settings.

The example shown refers to the multi-arm with the firewall in NAT mode. For multi-arm bridged mode or single-arm deployments, please refer to the respective diagrams in Deployment Scenarios on page 5 for comparison with your actual deployment IP addresses.

a. On the **Core realm configuration** panel:

   i. Configure the **IP address** as **10.10.1.2**. This parameter is environment specific.
   ii. Configure the **Subnet mask** as **255.255.255.0**. This parameter is environment specific.

b. On the **Access and Admin realm** configuration panel:

   i. Configure the **IP address** as **176.16.10.102**. This parameter is environment specific.
   ii. Configure the **Subnet mask** as **255.255.255.0**. This parameter is environment specific.

c. On the **Routing** panel, set **Default gateway** address as **176.16.10.1**. This parameter is environment specific.

d. Click **Ok** and then click on **Apply Changes**.

7. A pop-up window appears for the system restart; click **OK** on all the pop-up windows.

5.1.4 Verifying SBC Software Status

To verify the SBC software status, see Verifying SBC Software Status on page 35.

5.2 Using OVF Files

This section describes installing the OpenScape SBC on a Virtual Machine using the Open Virtualization Format (OVF) file.

5.2.1 Prerequisites

The following are the prerequisites to install the OpenScape SBC on a Virtual Machine:

Important:
You must use SBC version 11.0 or higher as the minimum requirement.

- Ensure that you have downloaded the following OVF packages from the Software Download Center.
  - *oss-11.00.XX.YY.zip*
  - *vApps_oss-11.00.XX.YY.zip*
- The server hardware is installed.
- The VMware and vSphere Host client is operational.

> **Note**:
>
> This document describes the installation steps performed on the **VMWare ESXi Host Client**.

- Common Management Platform (CMP) is installed, or local GUI is available.

5.2.2 Generating ISO image with USB stick

This section describes the process of generating an ISO image with USB stick.

> **Note**:
> This configuration applies to a multi-arm deployment (Firewall NAT mode). For more information, refer to Deployment Scenarios on page 5.

To generate the ISO image:

1. Extract the *oss-11.0X.YY.ZZ.zip* SBC package. The *oss-11.0X.YY.ZZ* folder is generated.
2. Open the *oss-11.0X.YY.ZZ* folder and extract the *usbsticksetup_oss-11.0X.YY.ZZ.zip* file. The *usbsticksetup_oss-oss-11.0X.YY.ZZ* folder is generated.
3. Move the *image_oss-11.0X.YY.ZZ.tar* file from the *oss-11.0X.YY.ZZ* folder to the *usbsticksetup_oss-11.0X.YY.ZZ/ob* folder.
4. Navigate to the *usbsticksetup_oss-11.0X.YY.ZZ.zip* folder.
5. Double-click on the *usbsticksetup.exe* file.
6. A pop-up window appears; click **Yes**.

   The **OSS USB Stick Setup** window is displayed.
7. Configure the **OSS USB Stick Setup**.

   a. On the **Configuration database** panel, select **Generate node.cfg** from the drop-down menu.

Important:
For single-arm deployment, it's essential to check the **Single arm** checkbox. Upon doing so, you'll notice that both the access and core realms have the same IPs but different ports. Despite this, in terms of administration, they remain logically separated network realms. Now, your access realm is configured as **SA Main IPv4** type.

b. Configure the **SBC Network Configuration**:

i. From the **Hardware Type** drop-down menu, select **Virtual OSS 20000**.
ii. Set **Hostname** as an environment-specific value.
iii. From the **Interface** dropdown menu, select **LAN Interface.**

Note:
Admin access is configured by default on the **LAN Interface**. You don't have to configure a separate admin interface; you can configure the **Admin Interface** only if you need a separate admin interface.

iv. Set the **IPv4 address** as **10.10.1.2**. This is an environment specific value.
v. Set the **IPv4 netmask** as **255.255.255.0**. This is an environment specific value.
vi. Set the **IPv4 gateway** as **172.16.10.1**. This is an environment specific value.
vii. From the **Interface** dropdown menu, select **WAN Interface.**
viii. Set the **IPv4 address** as **172.16.10.102**. This is an environment specific value.
ix. Set the **IPv4 netmask** as **255.255.255.0**. This is an environment specific value.
x. Click **Ok** to save the ISO image on your system.

After the **Setup Progress** is complete, the ISO image will be saved on your system.

5.2.3 Installing SBC Using OVF File

To install the SBC on the Virtual Machine using the OVF file:

1. Extract the *vApps_oss-11.0X.YY.ZZ.zip* file. The *vApps_oss-11.0X.YY.ZZ* folder is generated.
2. Log in to the **VMWare ESXi Host Client**.
3. From the left side navigation tree, click on **Virtual Machines**.
4. On the main page, click on **Create / Register VM**.
5. Choose **Select creation Type** as **Deploy a virtual machine from an OVF or OVA file**.
6. Click **NEXT**.
7. Enter the virtual machine name on the **Enter a name for the virtual machine** field.
8. Click on **Click to select files or drag/drop** to upload the OVF file.
9. Navigate to the *vApps_oss-11.0X.YY.ZZ/vApps/OSS-20000* folder.
10. Select both the *OSS.ovf* and *OSS-disk1.vmdk* files.
11. Click **NEXT**.
12. On the **Select Storage** page, select the **datastore**.

13. Click **NEXT**.
14. Configure the **Deployment options**.

    a. Configure **Network mappings**:

        i. Set **LAN** as an environment-specific value.
        ii. Set **WAN** as an environment-specific value.

    b. Set **Disk provisioning** as **Thin**.
    c. Deselect **Power on automatically**.
15. Click **NEXT**.
16. On the **Ready to complete** page, verify the configuration details, and click on **FINISH**.

> **Note**:
> The vApps configuration includes CPU and Memory reservations, which you can manually change if desired.

On the **Virtual Machines** page, a new entry is created based on the SBC configuration.

5.2.4 Configuring Virtual Machine Settings

1. On **VMWare ESXi Host Client**, click on the new entry (created for SBC installation) to edit the configuration.
2. Click **Edit** to change the settings for the VM.
3. Configure the following parameters on the **Virtual Hardware**.

> **Note**:
> Do not change the default value of the other parameters that are configured based on the Vapps template (uploaded in Installing SBC Using OVF File on page 33).

    a. Set **CD/DVD Drive 2** as **Datastore ISO file**.

    The **Datastore browser** window is displayed.

    b. Click on **Upload**.
    c. Select the ISO file that is generated in Generating ISO image with USB stick on page 32. It takes a few seconds to upload the ISO file.
    d. After the ISO file is uploaded, select the file and click on **SELECT**.
    e. On **CD/DVD Drive 2**, select both **Connect at power on** and **Connect**.
4. Click **SAVE**.
5. Click **Power on** on top of the VM homepage. The command terminal is displayed and the bootup starts. It takes a few seconds for the host to load the configuration from the CD/DVD Drive 2.

6. Login to the SBC as the **root** user.
7. Navigate to the **osb/bin** directory.
8. Execute the following command to run the installation script.

```
obinstall.sh
```

9. When Option is prompted, type **1** and press **Enter**.
10. When asked for confirmation, type **yes** to continue the installation with 5 (default value) partitions.
11. When asked for reconfirmation, type **yes** to continue the installation.
12. After the partition installation is completed, type **x** on the Options menu to exit the installation.
13. Execute the following command to shut down the VM.

```
shutdown
```

After shutdown, the command prompt window is closed.

14. On **VMWare ESXi Client**, select the new entry (created for SBC installation) and click on **Edit**.
15. On **CD/DVD Drive 2**, deselect the **Connect at power on** and click on **SAVE**.

> **Important**:
> Stabilization for SBC installation takes around 10 minutes. Therefore, it is recommended that any changes to the database must be made after 10 minutes of the SBC installation.

16. Click **Power on** on the Virtual Machine.

5.2.5 Verifying SBC Software Status

> **Note**:
> It is recommended to verify the software status10 minutes after the SBC installation.

To verify the SBC software status:

1. Log in to the SBC server as an **administrator**.
2. Execute the following command to change the permission to **root**:

```
su
```

3. Execute the following command to verify the status of the SBC software:

```
pmc show .
```

4. The status of the software must be as follows:

```
Status: STABLE
```

5. To verify the SBC status in GUI:

    a. Log in to the SBC GUI.
    b. Navigate to the homepage.
    c. The status below **General <user_name>** will be as **SBC aggregated information and data**.

        This indicates that all the data is loaded into the system successfully.

Configuring OpenScape SBC 6

This chapter contains the following sections:

This chapter describes the configuration for connecting the OpenScape SBC with MX-ONE, the PSTN Provider, and Microsoft Teams. For the OpenScape SBC configurations required for Emergency Calls, refer to Configuring an E911 Solution.

The OpenScape SBC can be administered efficiently through a web-based GUI at the local level or the Common Management Platform (CMP) as a unified network element within the internal LAN network. This GUI simplifies its management alongside other OpenScape solution components forming the enterprise network. Additionally, the OpenScape SBC facilitates local management through a web-based GUI using HTTPS. In this solution, the local management portal is used to execute the required configurations.

The following figure depicts the OpenScape SBC login page.

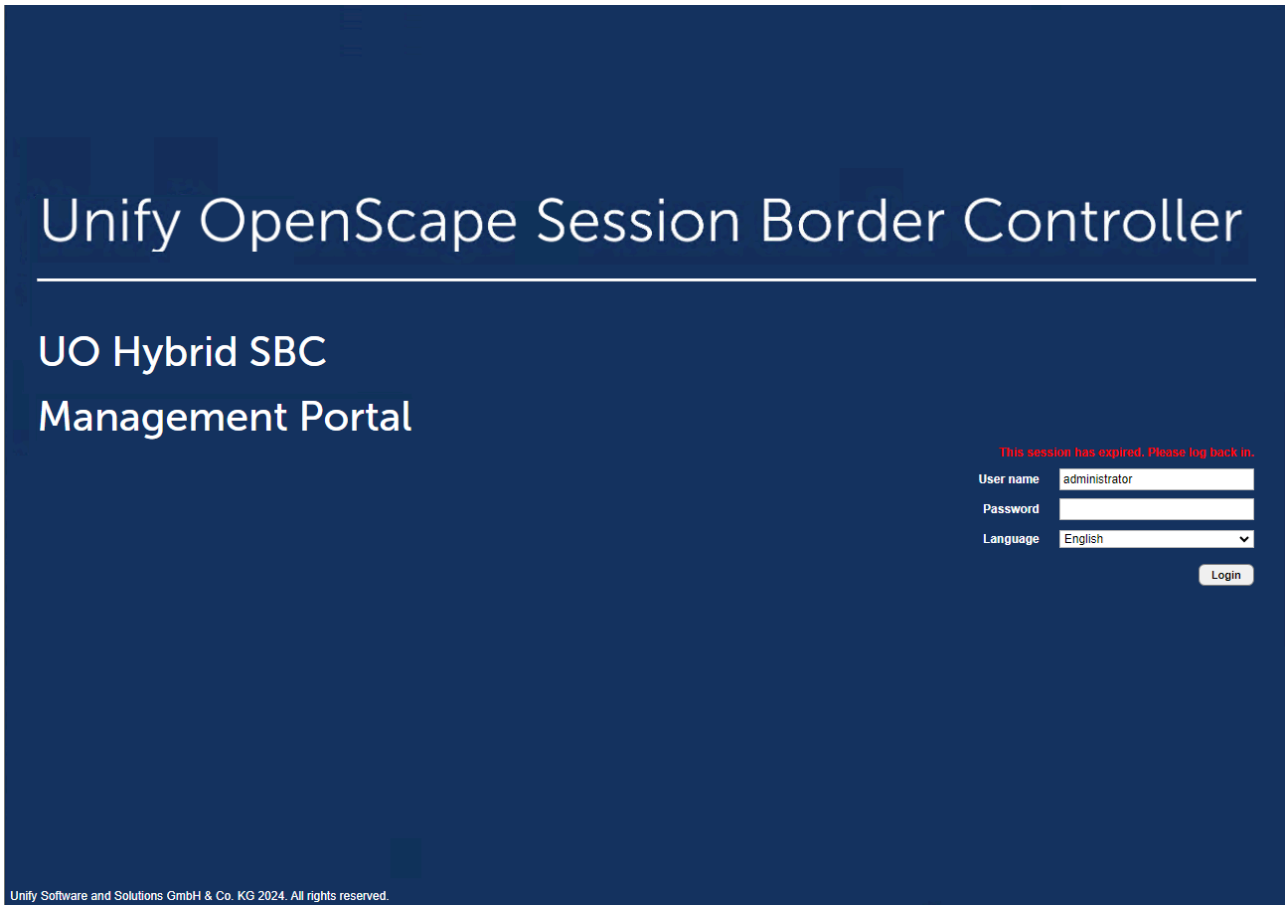


Figure 21: OpenScape SBC Login Page

6.1 Verifying License

This section describes the process of license registration and verification in the OpenScape Session Border Controller (SBC). After the initial SBC installation, the system enters a 29-day grace period. Each concurrent Direct Routing call between the PBX and MS Teams consumes two session licenses. For example, 10 concurrent calls require 20 SBC session licenses.

Note:
After the initial SBC installation, the system is in a grace period of 29 days. You can finalize the licenses later in the configuration process, once network settings and configurations are complete.

Note:
In case you change any of the following SBC parameters, you will also need to make ALI changes:

Hostname Host IP (or any other network chance such as adding a VPN or extra IPs to network interfaces etc.), DNS, Gateway and Timezone.

Prerequisite

To obtain an official license, you need an Advanced Locking ID (ALI). To generate the ALI for the OpenScape SBC, ensure that the DNS server is enabled.

Perform the following procedure to generate the ALI:

1. In the SBC management portal, navigate to the **Network/Net Services > DNS**.
2. Check the **Enable DNS server** checkbox.

Note:
In a fresh installation, the **Enable DNS server** checkbox is selected by default.

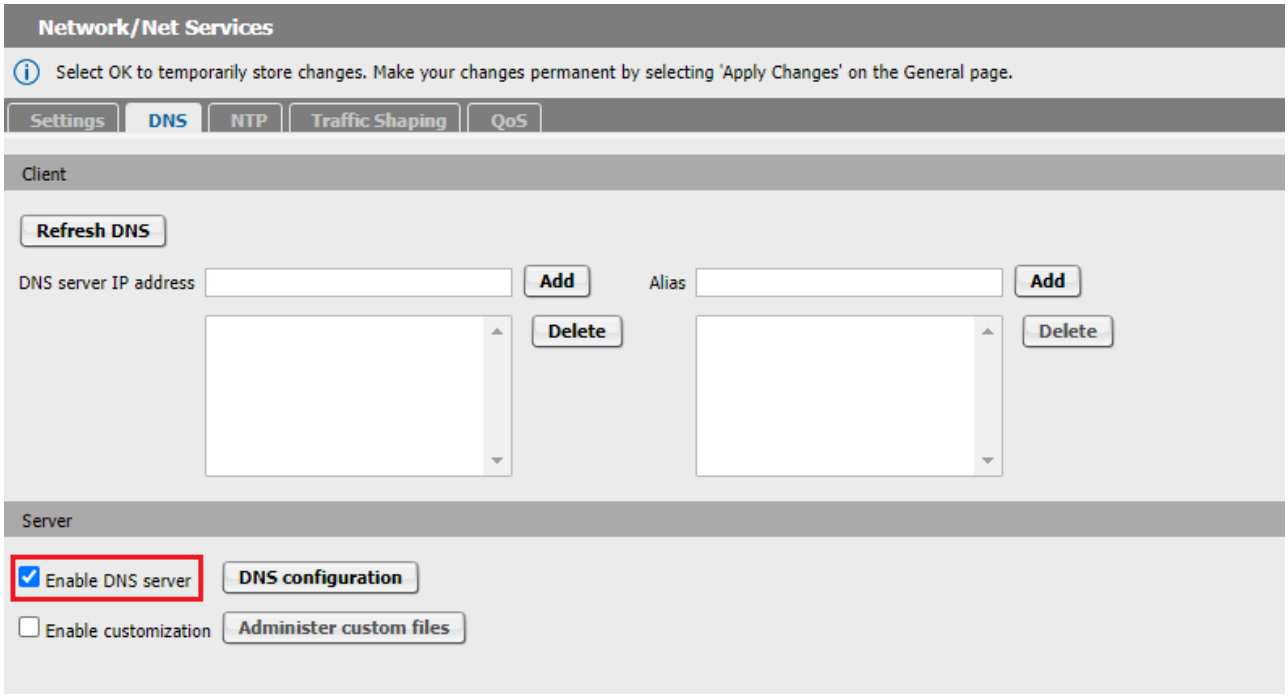


Figure 22: Enabling the DNS Server

3. Click **OK** and then click on **Apply changes**.
4. Navigate to **System > License**.

5. On **Advanced Locking ID**, click on **Refresh** to generate the ALI.

> **Note**:
> It is recommended to note down the Advanced Locking ID (ALI), as you need to provide the ALI upon registration.

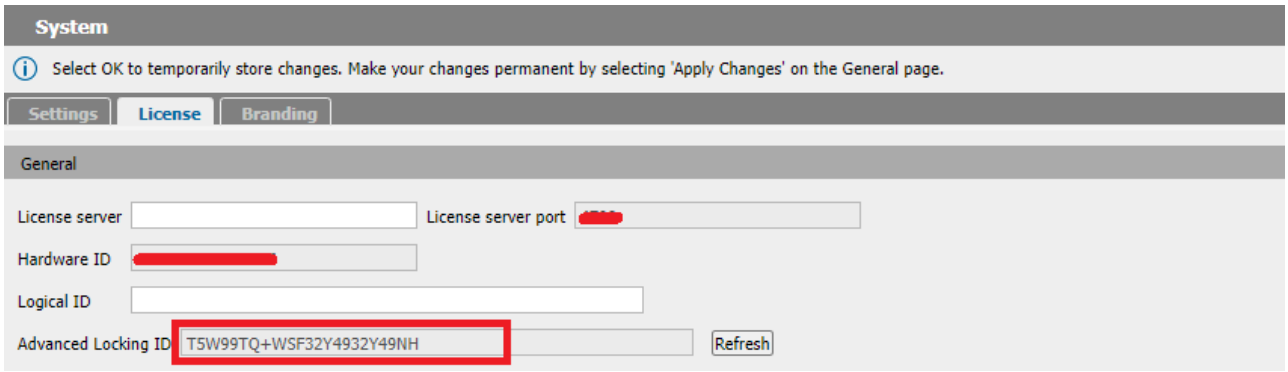


Figure 23: Generating ALI

6. Register your purchased license and SWA parts against your OpenScape SBC locking ID within MiAccess under **Licenses & Services**.

   You will receive the license file to upload for the OpenScape SBC installation. You can also use the application to register add-on licenses, replace locking IDs, and request SWA renewal quotes.

Procedure

To verify the licenses:

1. In SBC management portal, navigate to the **System > License** tab in the navigation tree under **Administration**.

   The **System** window pops up.
2. Under **License Information**, do the following:

   a. Under **Stand alone license file**, click **Choose file** to select the following standalone licenses if the license is not obtained from the license server (CMP):

   - OpenScape SBC Base License
   - Redundancy (if there is an SBC cluster)
   - SBC sessions
   - SBC Microsoft Direct Routing

   b. Click **Upload** to upload the licenses.

3. Ensure that the following licenses are displayed:

- OSS Base
- Redundancy

> **Note**:
> The **Redundancy** license type is optional and applies only to cluster OpenScape SBC.

- SBC Sessions
- Registered Lines
- SBC MS Direct Routing
- MS SBA (Optional)

> **Note**:
> After installation, the default license is valid 29 days. It is recommended to raise an official license request with the ALI which is generated in the Prerequisite on page 39.

License type	License configured	Licenses usage (peak)	Days till license expires
OSS Base	1	1	178 days
Redundancy	1	0	7 days
SBC sessions	100	6	178 days
Registered Lines	1	0	178 days
SBC MS Direct Routing	1	1	178 days

Figure 24: SBC License

> **Note**:
>
> In this OpenScape SBC configuration, the SBC needs a V11 license with one *SBC MS Direct Routing* license to enable Microsoft Teams direct routing configuration. To configure direct routing, see Configuring Direct Routing on page 101.

6.2 Configuring Network/Net Services

To configure interfaces for the Core (LAN), Access (WAN) realms, routing, and redundancy:

1. In SBC management portal, navigate to the **Network/Net Services > Settings** tab in the navigation tree under **Administration**.
2. Configure **Physical Network Interface** for either single-arm or multiple-arm configuration.
   - For single-arm configuration:
     a. **eth0**. Select **Enabled** for the web communication.
     b. Select **Single armed**.
   - For multiple-arm configuration:
     a. **eth0**. Select **Enabled** for the cluster and web interface.
     b. **eth1**. Select **Enabled** for the PSTN provider and Microsoft Teams communication.
     c. **eth2**. Select **Enabled** for the MX-ONE communication.
3. Configure the **Interface Configuration** for **eth0** interface. The **Core realm configuration** for **eth0** is completed during the installation and does not require any configuration.

> **Note**:
> For single-arm configuration, the following ports must configured with unique port values:
> - **SIP-UDP**
> - **SIP-TCP**
> - **SIP-TLS**
> - **SIP-MTLS**

4. Configure **Access and Admin realm configuration**.
   - For single-arm configuration:

     The **Access and Admin realm configuration** for **eth0** is completed during the installation and does not require any configuration.

Note:
For single-arm configuration, the following ports must configured with unique port values:

- **SIP-UDP**
- **SIP-TCP**
- **SIP-TLS**. This port must be configured as **5061** because Microsoft Team uses this port for the communication.
- **SIP-MTLS**

- For multiple-arm configuration:

  a. The **Access and Admin realm configuration** for **eth1** is completed during the installation and does not require any configuration.
  b. Configure **Access and Admin realm configuration** for **eth2**.

     i. Set **Type** as **Non-VLAN IP**.
     ii. Set **Network ID** as **Second-Access-IPv4**.
     iii. Set **Interface** as **eth2**.
     iv. Set **IP address** as environment specific value (IP for connection with MX-ONE).
     v. Set **Subnet mask** as **255.xxx.xxx.xxx**.
     vi. Set **SIP-UDP** as **5060**.
     vii. Set **SIP-TCP** as **5060**.
     viii. Set **SIP-TLS** as **5061**.
     ix. Set **SIP-MTLS** as **5161**.

  The following figure depicts the sample **Interface Configuration**.

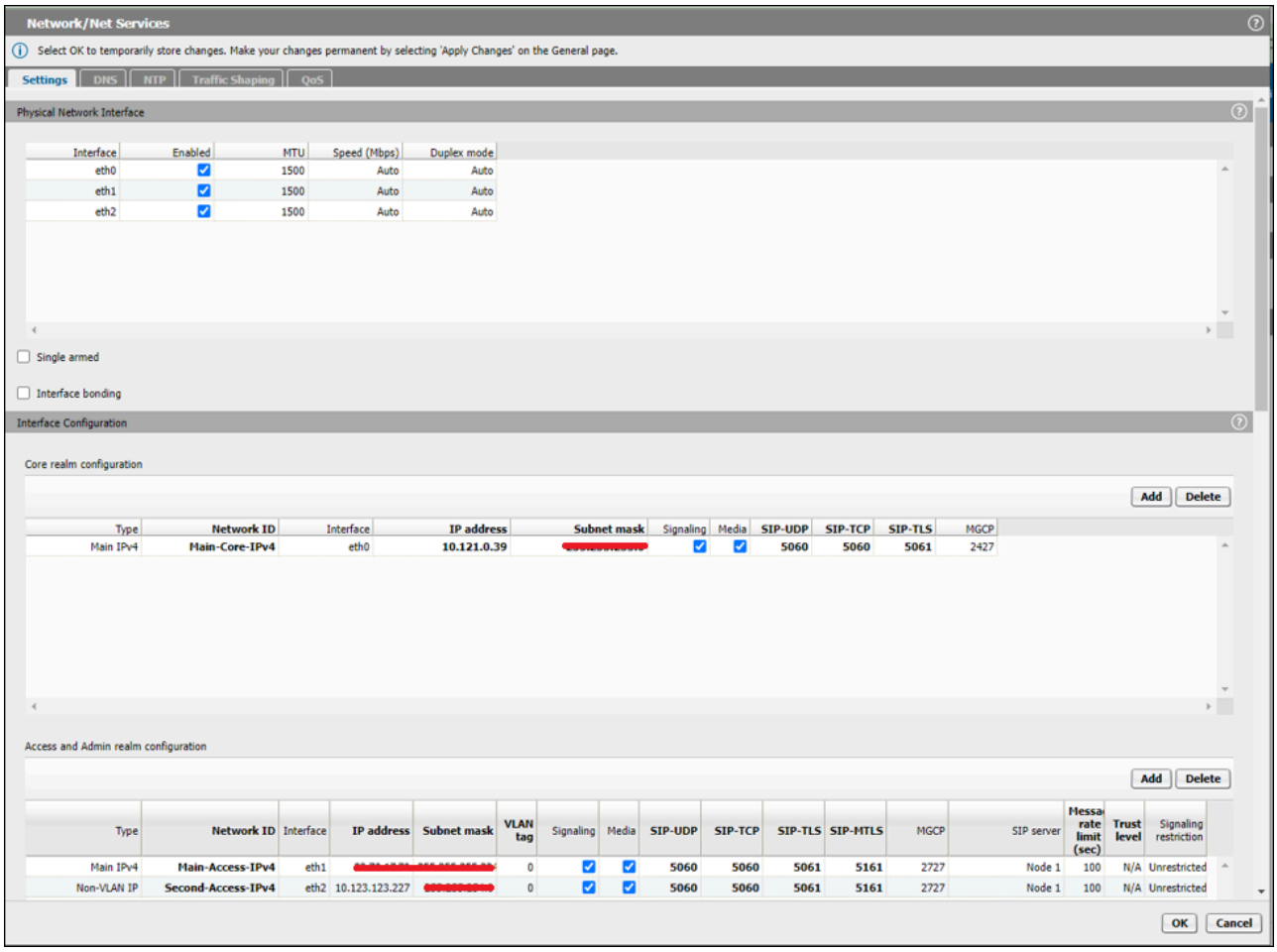


Figure 25: Network/Net Services Settings

5. On **Realm Profile** panel, click on **Add** to configure the realm profile.

- For single-arm configuration:

  a. Configure **Realm Profile** for main core realm ipv4:

     i. **Realm profile**. This parameter is configured by default in the system.
     ii. **Realm**. This parameter is configured by default in the system.
     iii. Set **Signaling network ID** as **Main-Core-ipv4**.
     iv. Set **Media network ID** as **Main-Core-ipv4**.
     v. Set **Forward network ID** as environment specific value.

  b. Configure **Realm Profile** for main access realm ipv4:

     i. Set **Realm profile** as **Main-Access-Realm - ipv4**.
     ii. Set **Realm** as **access**.
     iii. Set **Signaling network ID** as **Main-Access-ipv4**.
     iv. Set **Media network ID** as **Main-Access-ipv4**.
     v. Set **Forward network ID** as environment specific value.

- For multiple-arm configuration:

  a. Configure **Realm Profile** for main core realm ipv4:

     i. **Realm profile**. This parameter is configured by default in the system.
     ii. **Realm**. This parameter is configured by default in the system.
     iii. Set **Signaling network ID** as **Main-Core-ipv4**.
     iv. Set **Media network ID** as **Main-Core-ipv4**.
     v. Set **Forward network ID** as environment specific value.

  b. Configure **Realm Profile** for main access realm ipv4:

     i. Set **Realm profile** as **Main-Access-Realm - ipv4**.
     ii. Set **Realm** as **access**.
     iii. Set **Signaling network ID** as **Main-Access-ipv4**.
     iv. Set **Media network ID** as **Main-Access-ipv4**.
     v. Set **Forward network ID** as environment specific value.

  c. Configure **Realm Profile** for second access realm ipv4:

     i. Set **Realm profile** as **Second-Access-Realm - ipv4**.
     ii. Set **Realm** as **access**.
     iii. Set **Signaling network ID** as **Second-Access-ipv4**.
     iv. Set **Media network ID** as **Second-Access-ipv4**.
     v. Set **Forward network ID** as environment specific value.

The following figure depicts the sample realm profile configuration.

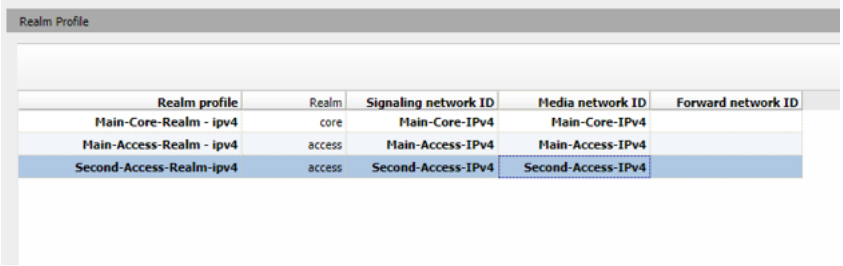


Figure 26: Realm Profile Configuration

6. Click **OK** and then click **Apply Changes** to save the network configuration.

6.2.1 Creating Rule for Network/Net Services Settings Routing

Note:
This section is applicable only if a separate network card is used for a communication with MX-ONE.

To create a new route to a destination other than the default gateway:

1. In SBC management portal, navigate to the **Network/Net Services > Settings** tab in the navigation tree under **Administration**.
2. In **Routing configuration** panel, click on **Add** to create a new rule for network/net services settings.

   a. Create a new rule for network/net services settings for **eth0**.

      i. Set **Destination** as environment specific value.
      ii. Set **Gateway** as environment specific value.
      iii. Set **Netmask** as environment specific value.
      iv. Set **Interface** as **eth0**.

   b. Create a new rule for network/net services settings for **eth2**.

      i. Set **Destination** as environment specific value.
      ii. Set **Gateway** as environment specific value.
      iii. Set **Netmask** as environment specific value.
      iv. Set **Interface** as **eth2**.

3. Configure the Default gateway address as environment specific value for internet connectivity.

Important:
After installation if user wants to change the **Default gateway address**, then the user must configure **Routing configuration** (Step 2) before configuring the default gateway address. Changing the default gateway address before the routing configuration will terminate the connection.

The following figure depicts the sample configuration for **eth0** and **eth2**.

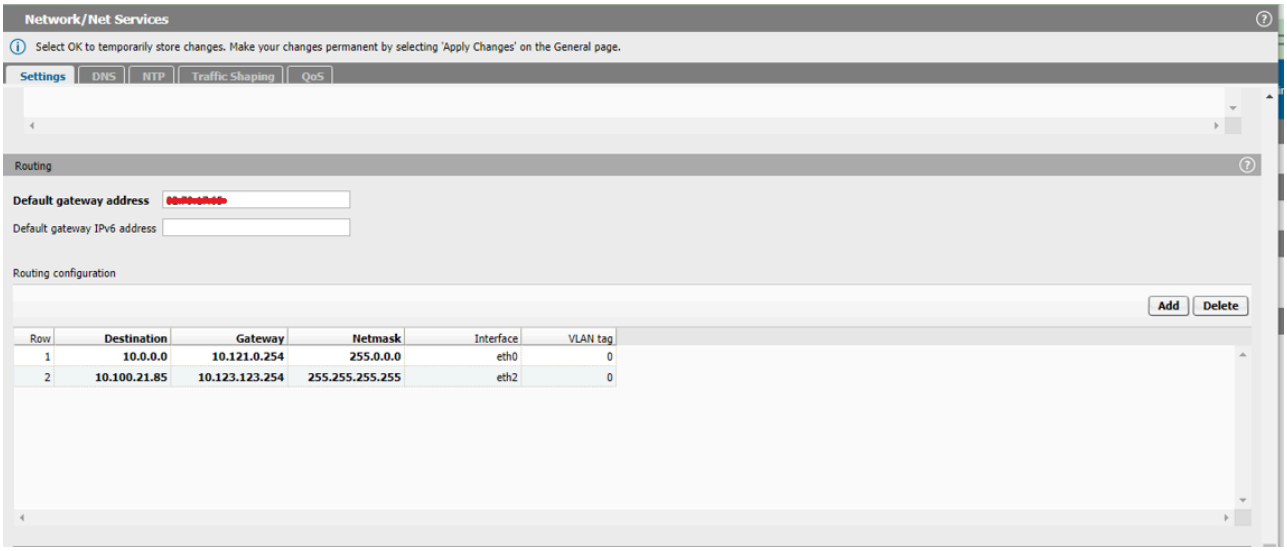


Figure 27: Network/Net Services Settings Routing Configuration

4. Click **OK** and then click **Apply Changes** to save the network configuration.

6.3 Configuring Domain Name System

The Domain Name System (DNS) must be configured to solve Microsoft Teams direct routing FQDNs.

To configure the DNS settings:

1. In the SBC management portal, navigate to **Network/Net Services > DNS** in the navigation tree under **Administration**.
2. Under **Client**, click **Refresh DNS** to manually refresh the DNS client (restarting the service).

3. Configure the **DNS**.

   a. Configure **Client** as follows:

      i. Set **DNS server IP address** as environment specific value. Enter the value and then click on **Add**.

      ii. Set **Alias** as environment specific value. Enter the value and then click on **Add**.

   b. In **Server** select **Enable DNS server**.

The following figure depicts the sample **DNS** configuration.

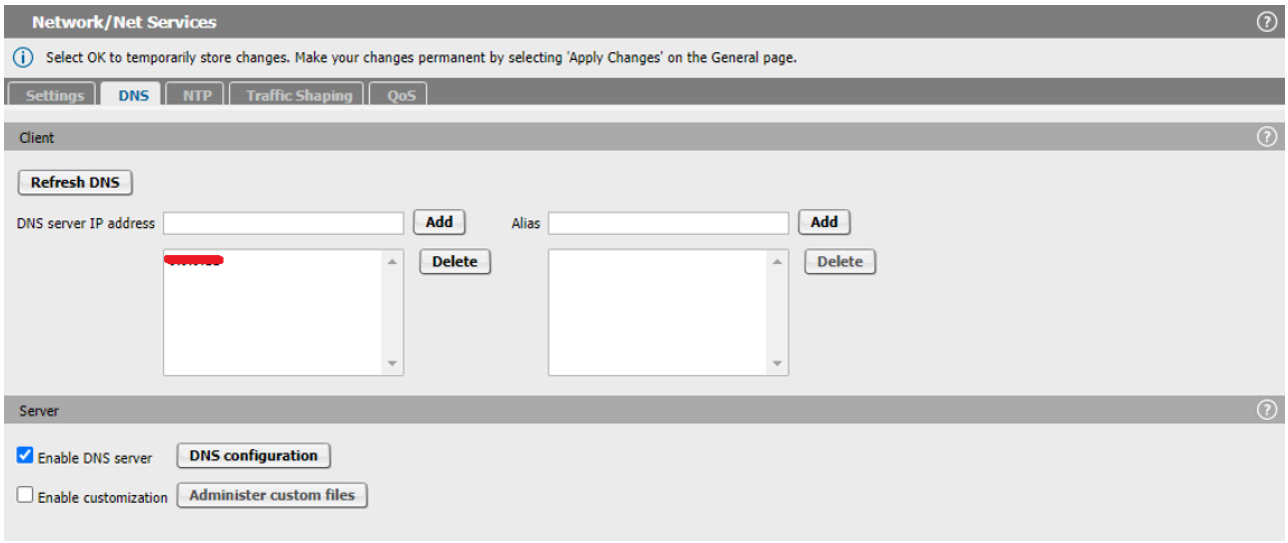


Figure 28: DNS Configuration

4. Click **OK** and then click **Apply Changes** to save the DNS configuration.

6.4 Network Time Protocol Configuration

To configure the Network Time Protocol (NTP) server:

1. In the SBC management portal, navigate to **Network/Net Services > NTP** in the navigation tree under **Administration**.

2. Configure **NTP Settings**.

   a. Set **Region** as an environment specific value.
   b. Set **Timezone** as an environment specific value.
   c. Select **Enable local NTP server**.
   d. Deselect the **Manual configuration**. The parameter has the following subset of parameters.

      i. **Date**
      ii. **Time**

   e. Select **Synchronize with NTP server**.
   f. Set **NTP server** as an environment specific value and click on **Add**. The following figure depicts the sample **NTP Settings** configuration.

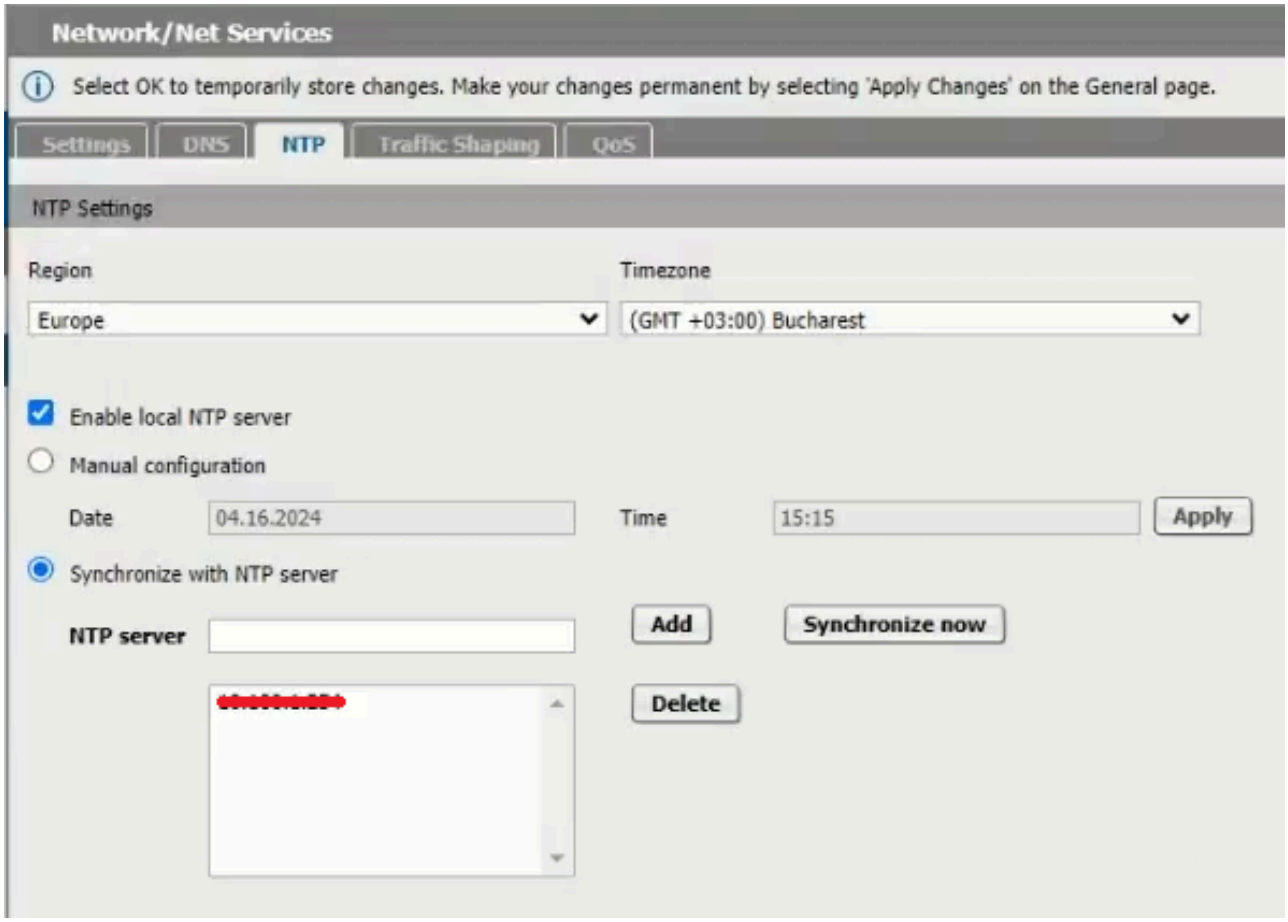


Figure 29: NTP Settings

3. Click **OK** and then click **Apply Changes** to save the NTP configuration.

6.5 Configuring Firewall

Setting up permissions to manage and control network traffic is the initial step in creating firewall rules.This chapter describes the network ports that need to be configured on the external firewall to ensure security and proper functioning of the system.

Depending on the system deployment (single-arm or multi-arm), note the prerequisites for the configuration steps. For more information, refer to Deployment Scenarios on page 5.

6.5.1 Prerequisite

Single-arm Deployment

Proper configuration is required in the Firewall prior configuring the firewall settings for single-arm deployment.

Important:

The following high-level steps should be performed with the support of the IT team:

1. Add a network interface in your firewall for accessing the local network.
2. Create a new DMZ LAN interface, to access the network where MX-ONE is located.
3. Configure network equipment to route the traffic between new DMZ LAN interface and the local network (MX-ONE).
4. Allow traffic between the DMZ LAN interface and the local network, and vice versa.
5. Create firewall rules to allow traffic between MX-ONE– SBC and vice versa for the TLS port assigned (i.e., 5061) and the RTP port range. The TLS ports depends on the configuration of SIP ports used by MX-ONE (see Configuring Media Profiles on page 54). RTP ports depends on configuration of RTP ranges (see Configuring Port and Signaling Settings on page 62). The default ports are 20000-49999.
6. Allow TCP/UDP traffic between Microsoft Teams servers (sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com and sip3.pstnhub.microsoft.com) and the WAN interface of DMZ and SBC. The TCP ports depend on configuration of SIP ports used by Microsoft Teams (usually 5061) (see Configuring Remote Endpoints on page 79) and by access realm SIP ports of SBC (see Configuring Network/Net Services on page 42). The RTP ports depend on the configuration of RTP ranges; (see Configuring Port and Signaling Settings on page 62). The default ports are 20000-49999. The range can be reduced to minimize the number of ports to be opened. The range of RTP ports must be wide enough to allow the maximal expected simultaneous calls.

Multi-arm Deployment

Proper configuration is required in the Firewall prior configuring the firewall settings for multi-arm deployment.

Important:
The following high-level steps should be performed with the support of the IT team:

1. Allow TCP/UDP traffic between Microsoft Teams servers (sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com and sip3.pstnhub.microsoft.com) and the WAN interface of DMZ and SBC. The TCP ports depend on the configuration of SIP ports used by Microsoft Teams, which usually is 5061 (please refer to Configuring Remote Endpoints on page 79 and by access realm SIP ports of OpenScape SBC (see Configuring Network/Net Services on page 42).
2. The RTP ports depend on the configuration of RTP ranges (see Configuring Port and Signaling Settings on page 62). The default ports are 20000-49999. The range can be reduced to minimize the number of ports to be opened. The range of RTP ports must be wide enough to allow the maximal expected simultaneous calls.

6.5.2 Configuring Firewall Settings

To configure firewall settings:

1. In SBC management portal, navigate to the **Security > Firewall** tab in the navigation tree under **Administration**.

2. On **Firewall Settings**, click on **Add** to add the internal firewall configuration for either single-arm or multiple-arm configuration:

   - For single-arm configuration. The **Main** access interface is configured by default and does not require any configuration.
   - For multiple-arm configuration:

     a. The **Main** access interface is configured by default and does not require any configuration.
     b. Click on **Add**, and configure firewall settings for **Second-Access-IPv4** access interface.

        i. Set **Network ID** as **Second-Access-IPv4**.
        ii. **Access IP address**: **10.xxx.xxx.xxx**. This parameter is configured automatically by the system.
        iii. Set **DNS** as **Block**.
        iv. Set **SNMP** as **Block**.
        v. Set **FTP** as **Block**.
        vi. Set **HTTPS** as **Block**.
        vii. Set **SSH** as **Block**.
        viii. Set **ICMP** as **Block**.
        ix. Set **Telnet** as **Block**.
        x. Set **NTP** as **Block**.
        xi. Set **SIP** as **Allow**.
        xii. Set **TLS** as **Allow**.
        xiii. Set **RTP/sRTP** as **Allow**.
        xiv. Set **MGCP** as **Allow**.

   The following figure depicts the sample **Firewall Settings** configuration.

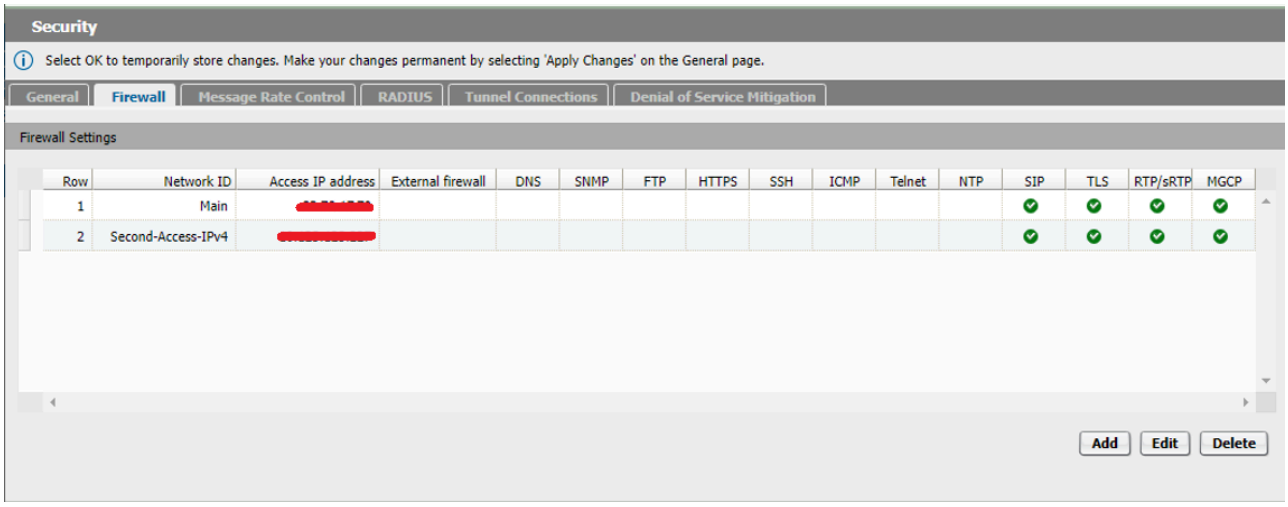


Figure 30: Firewall Configuration

3. Click **OK** and then click **Apply Changes** to save the firewall configuration.

6.5.2.1 External Firewall Configuration

When an external firewall is used, it can be configured in the **External Firewall** panel as depicted in the following figure.

> **Note**:
> For the DMZ deployments, the external firewall IP should be configured with the firewall's WAN IP.

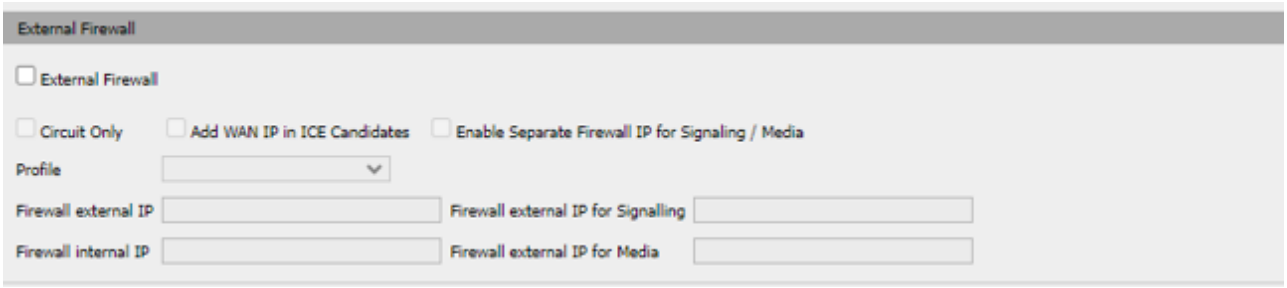


Figure 31: External Firewall Configuration

6.6 Configuring SIP Server

> **Note**:
> Assumption for the SIP server configuration:
>
> - Routing configuration is applied for PSTN and Microsoft Teams.
> - It is assumed that the OpenScape SBC operates in a standalone mode.

To configure SIP server settings:

1. In the SBC management portal, navigate to **VoIP > SIP Server Settings** in the navigation tree under **Administration**.
2. In the **General** settings, set **Comm System Type** as **Standalone with Internal SIP Stack** as depicted in the following figure.

Important:
For the OpenScape SBC V11 R0.6.0, when you select **Standalone with internal SIP stack**, you must set the SIP-TCP and SIP-TLS ports in the core realm configuration to **0**. For more information, refer to Configuring Network/Net Services on page 42.

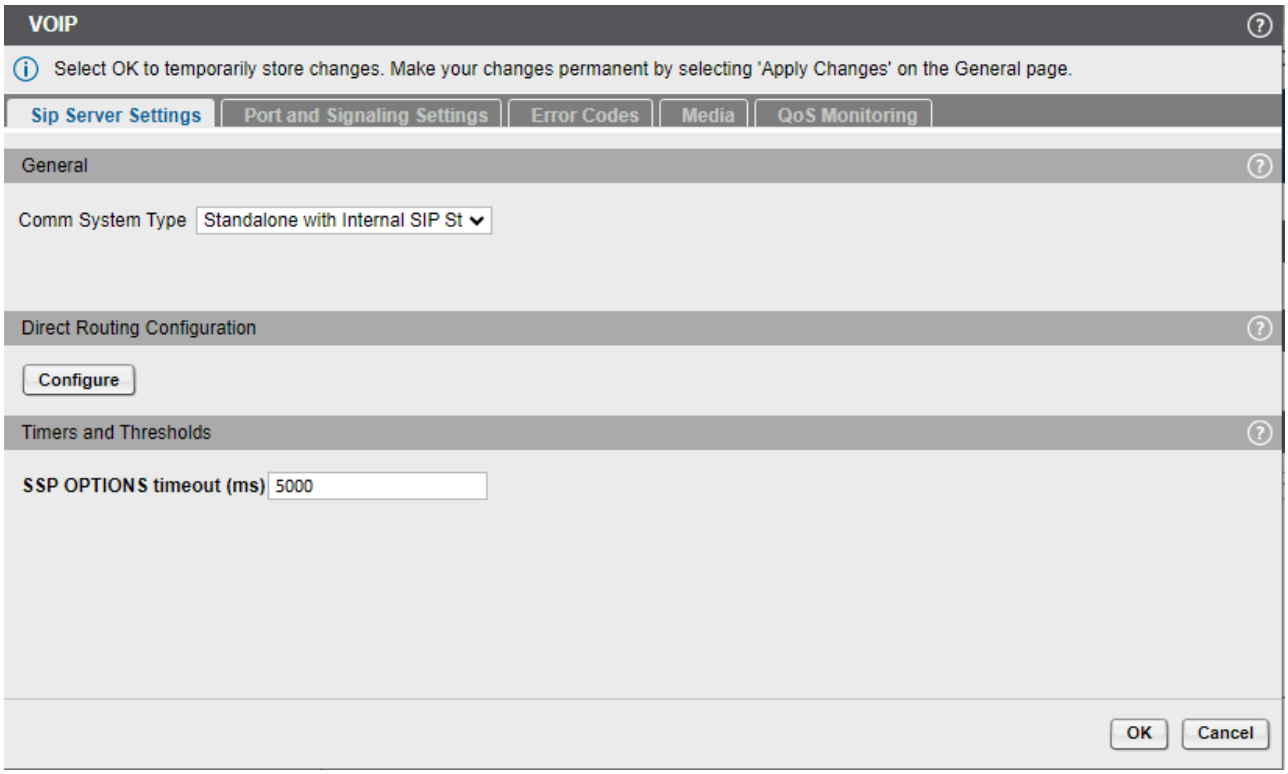


Figure 32: VOIP, SIP Server Settings

Note:
In **Timers and Thresholds** panel, the **SSP OPTIONS timeout (ms)** can be set to **5000** to avoid network delays.

3. When a setup is already existed and used, click on **Configure** to perform the additional configuration (see Configuring Direct Routing on page 91).
4. Click **OK** and then click **Apply Changes** to save the SIP server configuration.

6.7 Configuring Media Profiles

You need to enable the default media profile and create a media profile for each of the following:

- Microsoft Teams
- MiVoice MX-One

- PSTN

> **Important**:
> This PSTN profile is not required if the MBG is used for the SSP connection.

To configure media profile:

1. In the SBC management portal, navigate to **VoIP > Media** in the navigation tree under **Administration**.

2. Under **Media Profile**, select the **default** profile entry and click on **Edit**. Configure media profile for the core interface as follows:

   a. In **General** configuration, set **Media Protocol** as **RTP only**.
   b. Configure **SRTP configuration** as follows:

      i. Set **SRTP crypto context negotiation** as follows:

      - **MIKEY**. Deselect the check box.
      - **SDES**. Deselect the check box.

      ii. Deselect **Mark SRTP Call-leg as Secure**.
   c. Set **Codec** as environment specific value.
   d. Click **OK** to save the core interface configuration.

The following figure depicts the default media profile configuration.

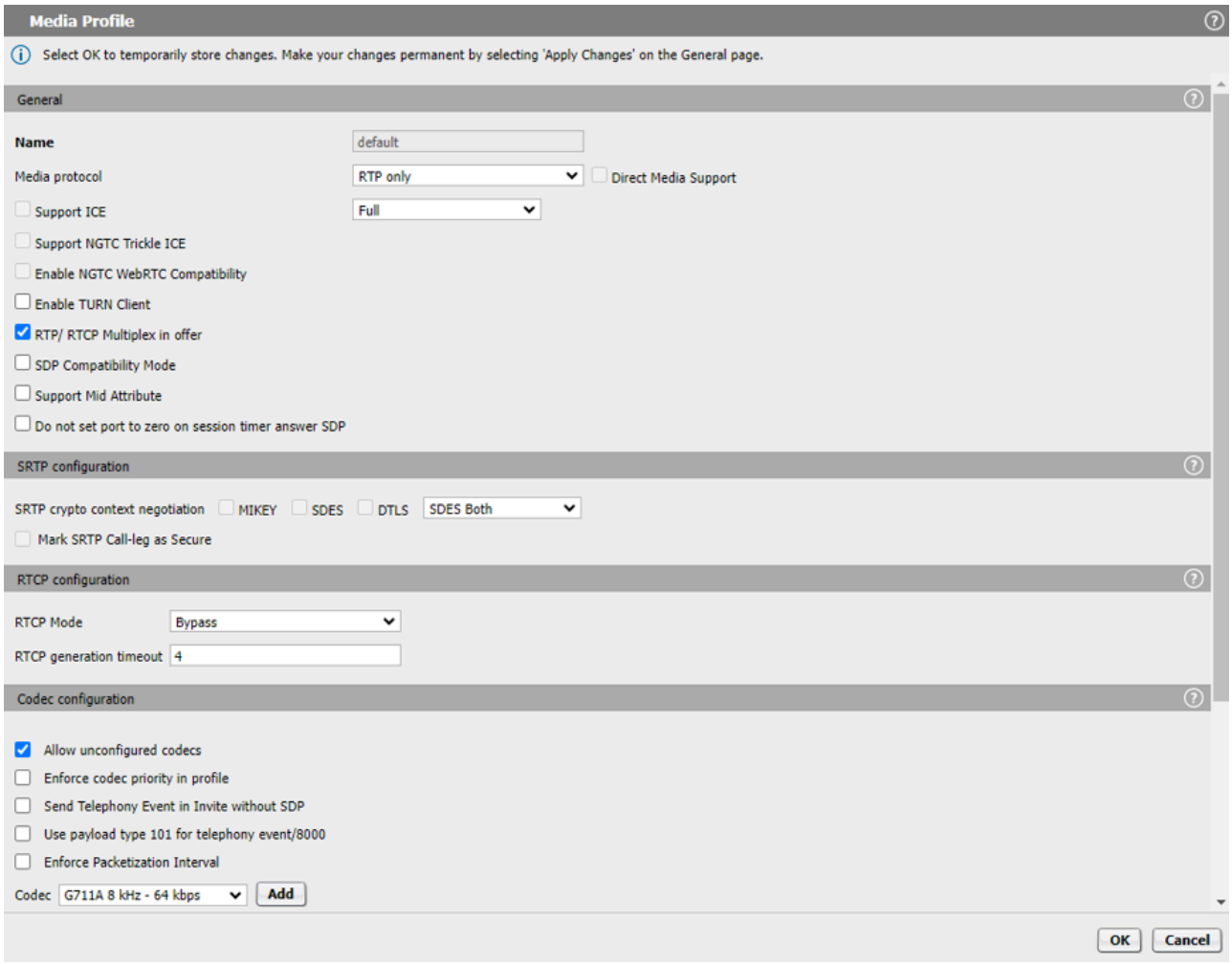


Figure 33: Default Media Profile

3. Click **Add** under **Media Profile** to configure the media profile for **PSTN**. These parameters are only for example, and it might change depending on the service provider.

Important:
This step is not required if the MBG is used for the SSP connection.

a. Configure **General** as follows:

   i. Set **Name** as **DT_TLS**.
   ii. Set **Media Protocol** as **SRTP only**.

b. In **SRTP configuration**, configure **SRTP crypto context negotiation** as follows:

   i. **MIKEY**. Deselect the check box.
   ii. Select **SDES AES-128 only** from drop-down menu.

c. In **Codec configuration**, set **Codec** as environment specific value.

d. Click **OK** to save the core interface configuration.

The following figure depicts the sample **Media Profile** configuration for **PSTN**.

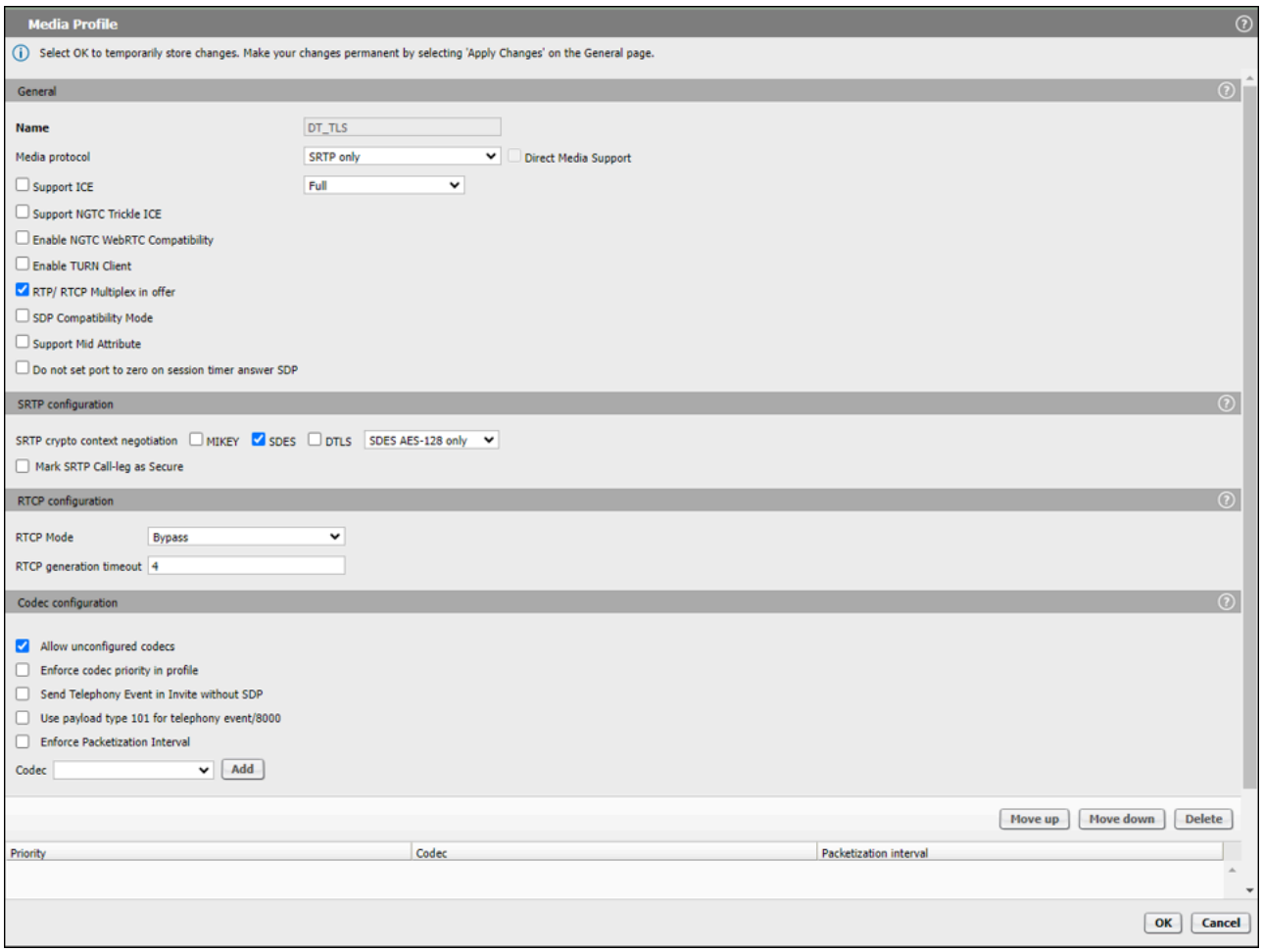


Figure 34: PSTN Provider Media Profile

4. Click **Add** under **Media Profile** to configure the media profile for **Microsoft Teams**.

   a. Configure **General** as follows:

      i. Set **Name** as **Teams**.
      ii. Set **Media Protocol** as **SRTP only**.
      iii. Configure **Support ICE** based on the deployment type being used, see Deployment Scenarios on page 5.

   b. Configure **SRTP configuration** as follows:

      i. Set **SRTP crypto context negotiation** as follows:

      - **MIKEY**. Deselect the check box.
      - **SDES**. Select the check box.
      - **DTLS**. Deselect the check box.
      - **SDES AES-128 only**. Select the value from drop-down menu.

   c. Configure **Codec configuration** as follows:

      i. Set **Codec** as environment specific value.

   d. Click **OK** to save the core interface configuration.

The following figure depicts the sample **Media Profile** configuration for **Microsoft Teams**.

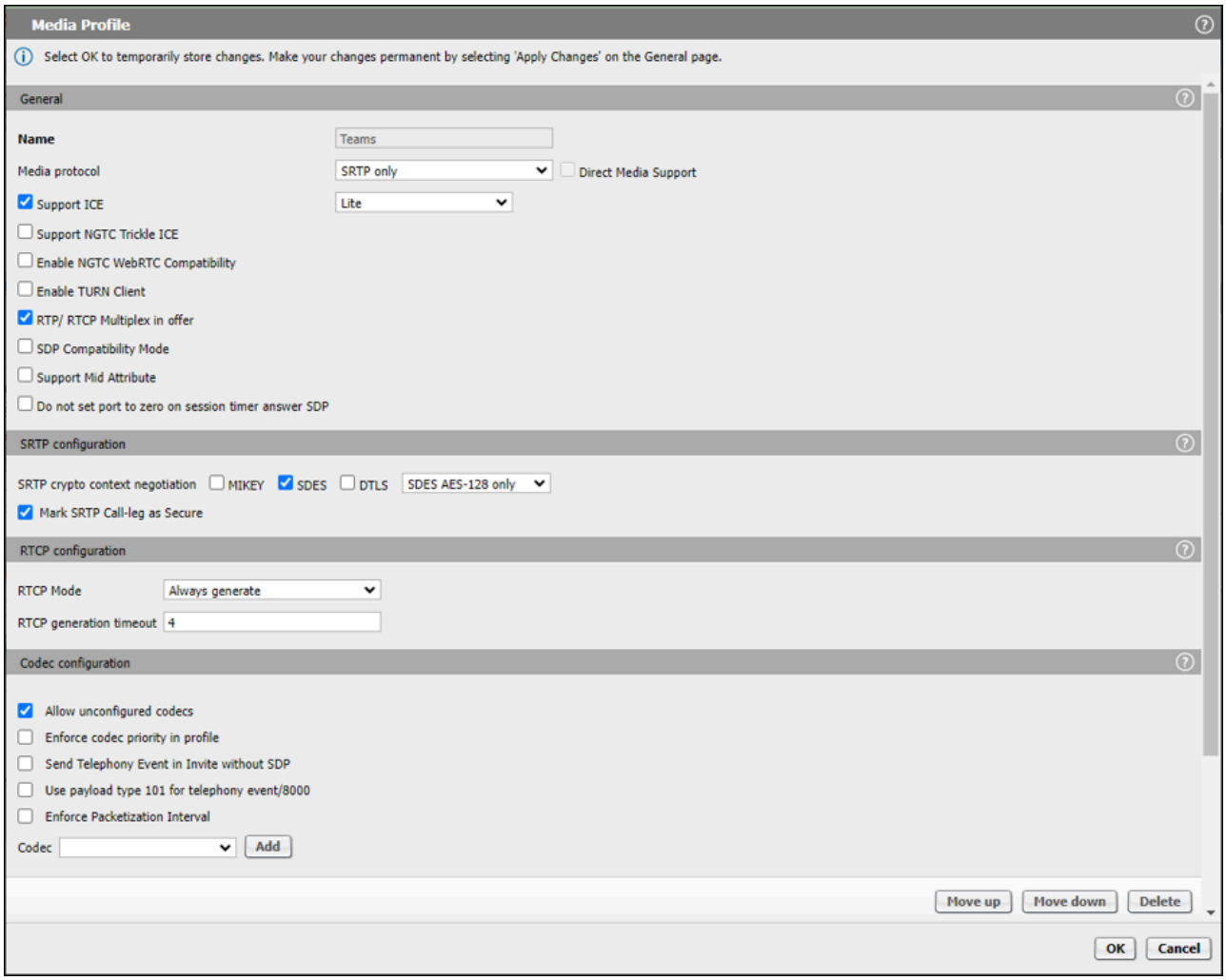


Figure 35: Microsoft Teams Media Profile

5. Click **Add** under **Media Profile** to configure the media profile for **MX-ONE**.

   a. Configure **General** as follows:

      i. Set **Name** as **Mitel**.
      ii. Set **Media Protocol** as **SRTP only**.

Note:

- If OpenScape SBC is configured as SRTP only then the **Media Protocol** must be configured as **SRTP only**.
- If OpenScape SBC is configured as RTP only then the **Media Protocol** must be configured as **RTP only**.

iii. Deselect **RTP/RTCP Multiplex in offer**.

b. In **SRTP configuration**, under **SRTP crypto context negotiation**:

i. Deselect **MIKEY**.

ii. Select **DTLS**.

c. In **Codec configuration**, set **Codec** as environment specific value.

d. Click **OK** to save the core interface configuration.

The following figure depicts the sample **Media Profile** configuration for **MX-ONE (SRTP Only)**.

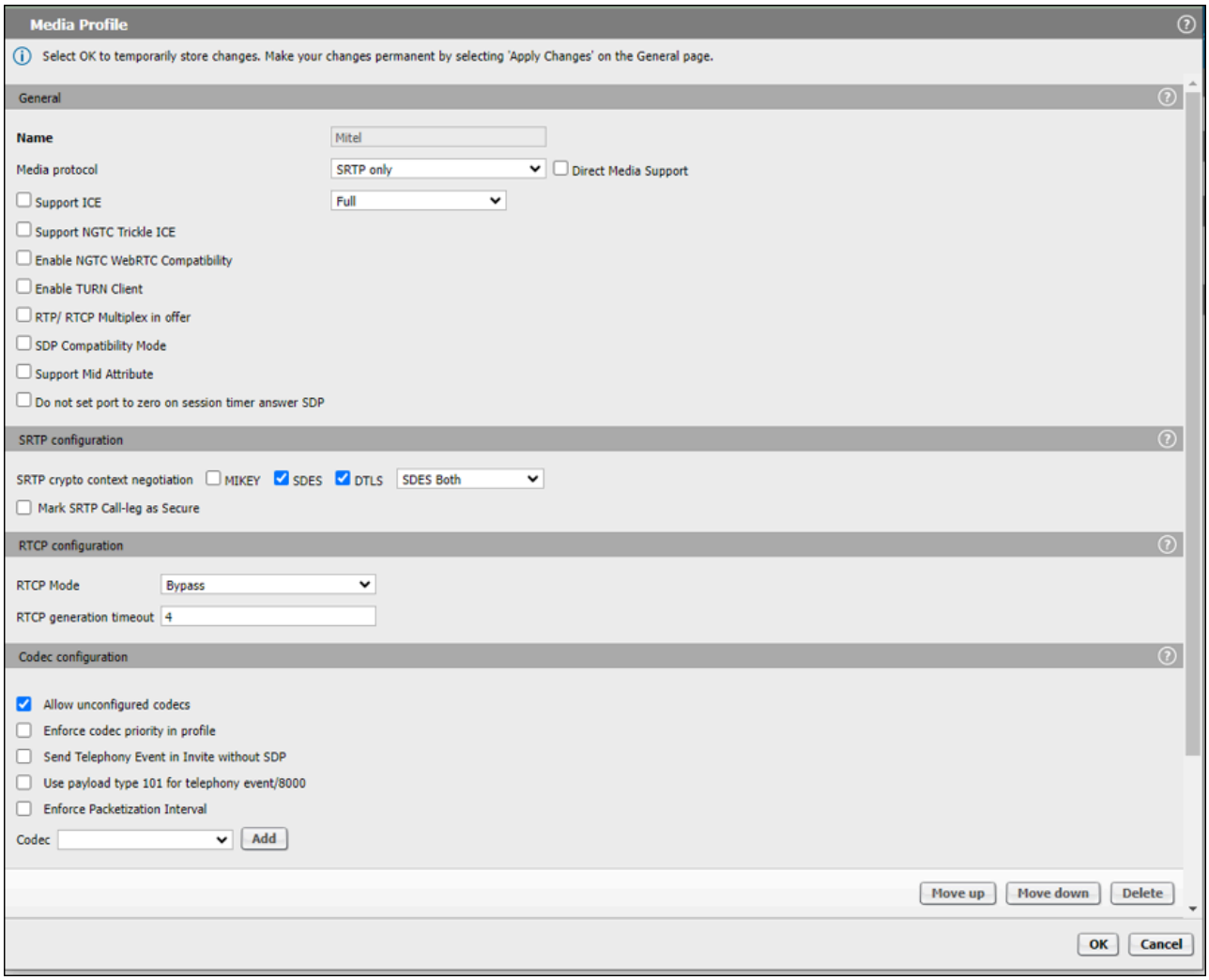


Figure 36: MX-ONE Media Profile with SRTP Only

The following figure depicts the sample **Media Profile** configuration for **MX-ONE (RTP Only)**.

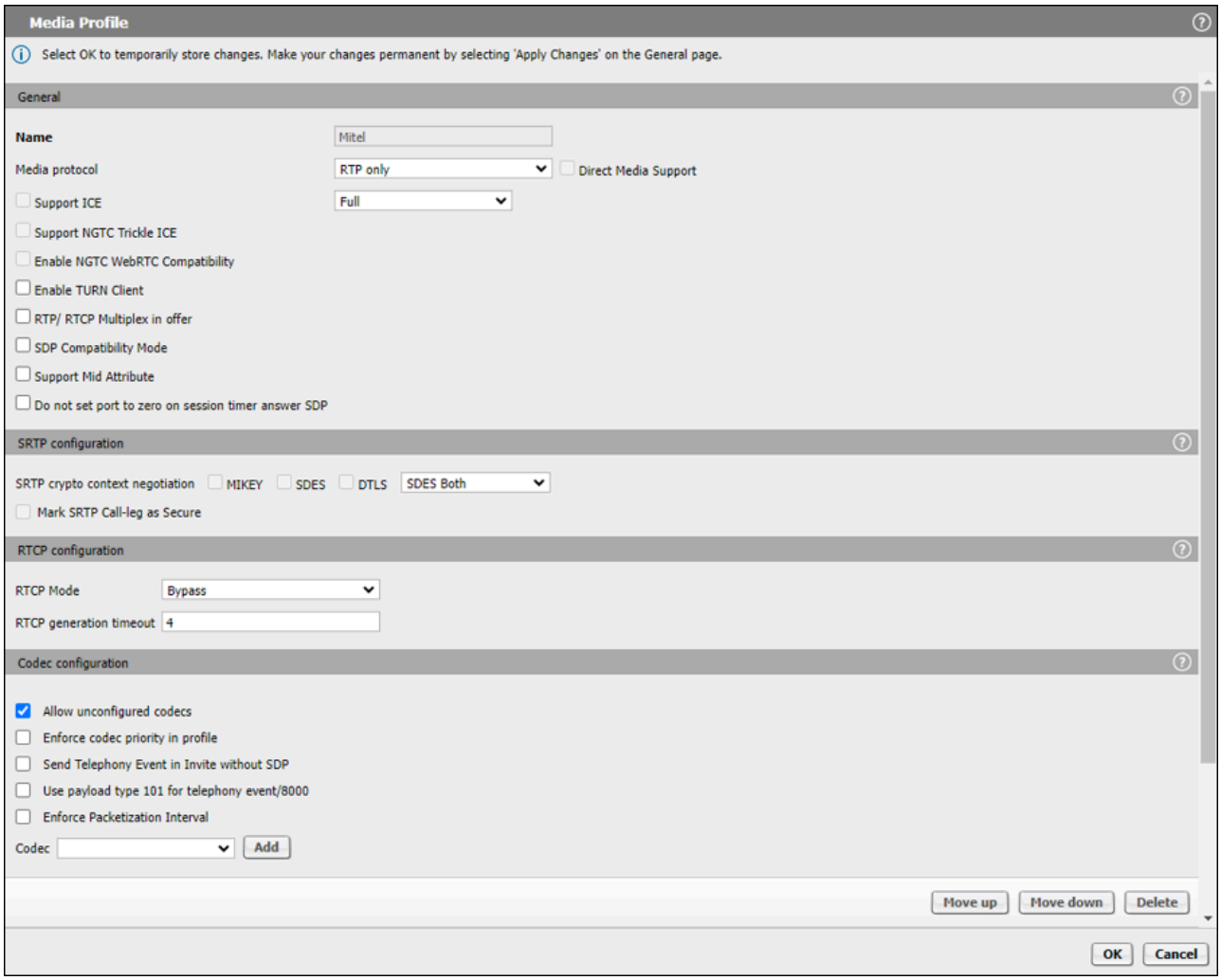


Figure 37: MX-ONE Media Profile with RTP only

6. Under **Cloud Support**, select the **Support OpenScape Cloud** checkbox to remove the core IP from the list of ICE candidates. This is because the core IP address is not accessible from access, resulting in connectivity checks failure.
7. Click **OK** and then click **Apply Changes** to save the media profile configuration.

6.8 Configuring Port and Signaling Settings

To configure the port and signaling settings:

1. In SBC management portal, navigate to the **VoIP > Port and Signaling Settings** tab in the navigation tree under **Administration**.

2. Configure **Port and Signaling Settings**.

   a. Configure **Port Range**.

      i. Set **Port min** as **10000**.
      ii. Set **Port max** as **49999**.
      iii. Set **Time to live (sec)** as **180**.

   b. Configure **Subscribers dynamic SIP ports**.

> **Note**:
> Port range must not overlap with other ranges, such as dynamic SIP ports for subscribers.

      i. Set **Port min** as **10000**.
      ii. Set **Port max** as **49999**.

The following figure depicts the sample **Port and Signaling Settings** configuration.

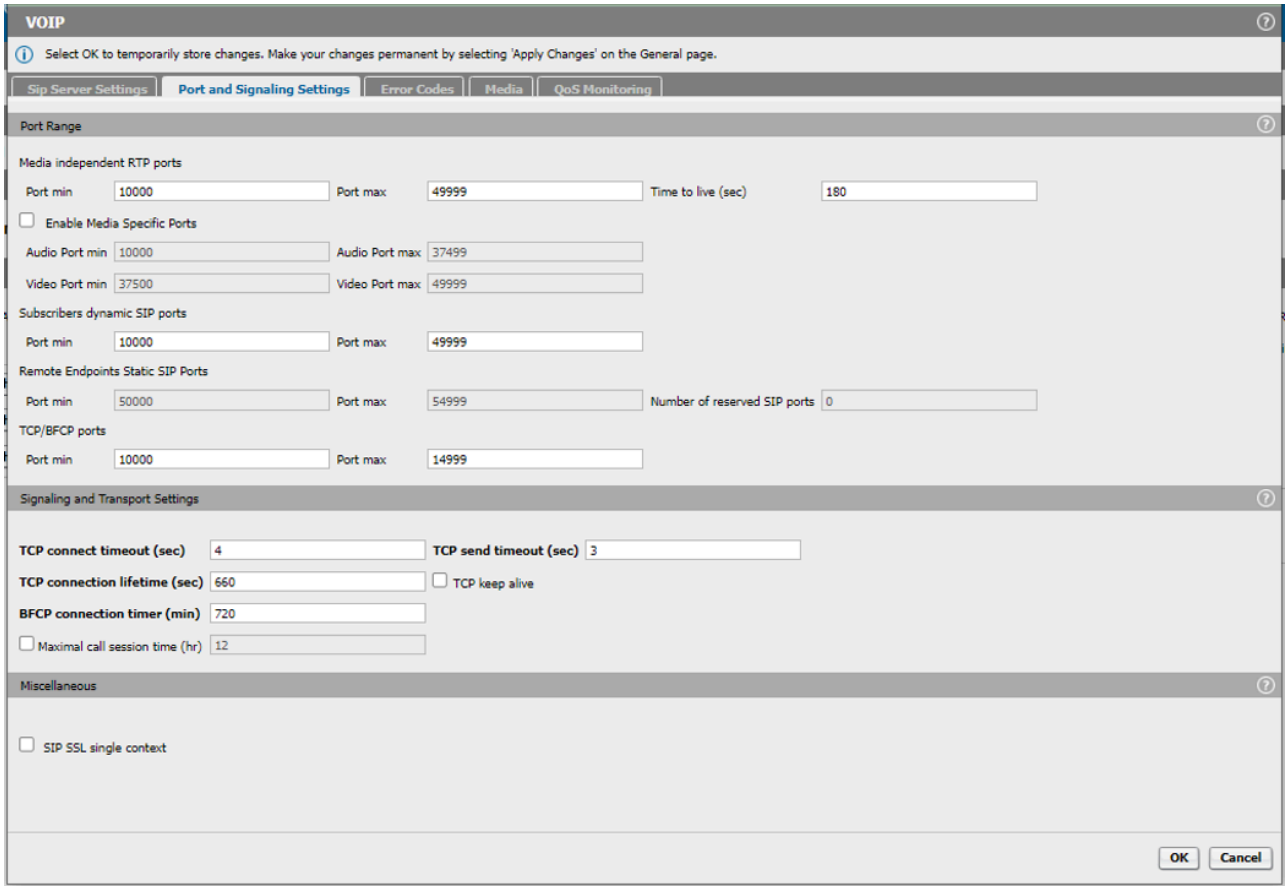


Figure 38: Port and Signaling Settings

3. Click **OK** and then click **Apply Changes** to save the port and signaling settings configuration.

6.9 Configuring Certificates

6.9.1 Prerequisites

Ensure the following before configuring the certificates:

- Ensure that all the OpenScape SBC certificates are in *.pem* format before uploading to the system.
- The certificates used for communication with Microsoft Teams must be signed by a Certificate Authority (CA) that is part of the Microsoft trusted root certificate program. For more information refer to the https://learn.microsoft.com/en-us/security/trusted-root/participants-list. The server certificate should have the SBC FQDN in the Common Name or Subject Alternative Name that is signed by a CA.
- If communication with MX-ONE is configured through TLS protocol, then the related certificates must be generated and uploaded. In this case, TLS must be enabled on MX-ONE, see Appendix D: Generating Certificates for MX-ONE in .pem Format on page 123.
- If PSTN connectivity is configured over TLS protocol, then related certificates are required. The SSP provider should be contacted for information about the needed certificates for PSTN connectivity.

Important:
This step is not required if the MBG is used for the SSP connection.

6.9.2 Importing OpenScape SBC Certificates

To import OpenScape SBC certificates:

1. In SBC management portal, navigate to the **Security > General** tab in the navigation tree under **Administration**.
2. Click **Certificate management**. The **Certificate Management** page is displayed.
3. On **Certificates Upload** panel, import the certificates as listed in the following table.

Certificate Type	Certificate Sample Name
CA certificates. Click on **Choose File** to upload the certificates.	*CA.pem*
	LasT-TeleSec_GlobalRoot_Class_2.pem
	SSL_COM_ROOT_CERTIFICATION_AUTHORITY
	sbcCA.pem

Certificate Type	Certificate Sample Name
X.509 Certificates. Click on **Choose File** to upload the certificates.	*ipserver.pem*
	sbcbyot_tksst_com_new.pem
	sbccert.pem
Key Files. Click on **Choose File** to upload the certificates.	*ipserverkey.pem*
	sbcbyot_privatekey.pem

Certificate Type	Certificate Sample Name
	sbckey.pem

The following figures depict the sample **CA Certificates**, **X.509 Certificates**, and **Key Files**.

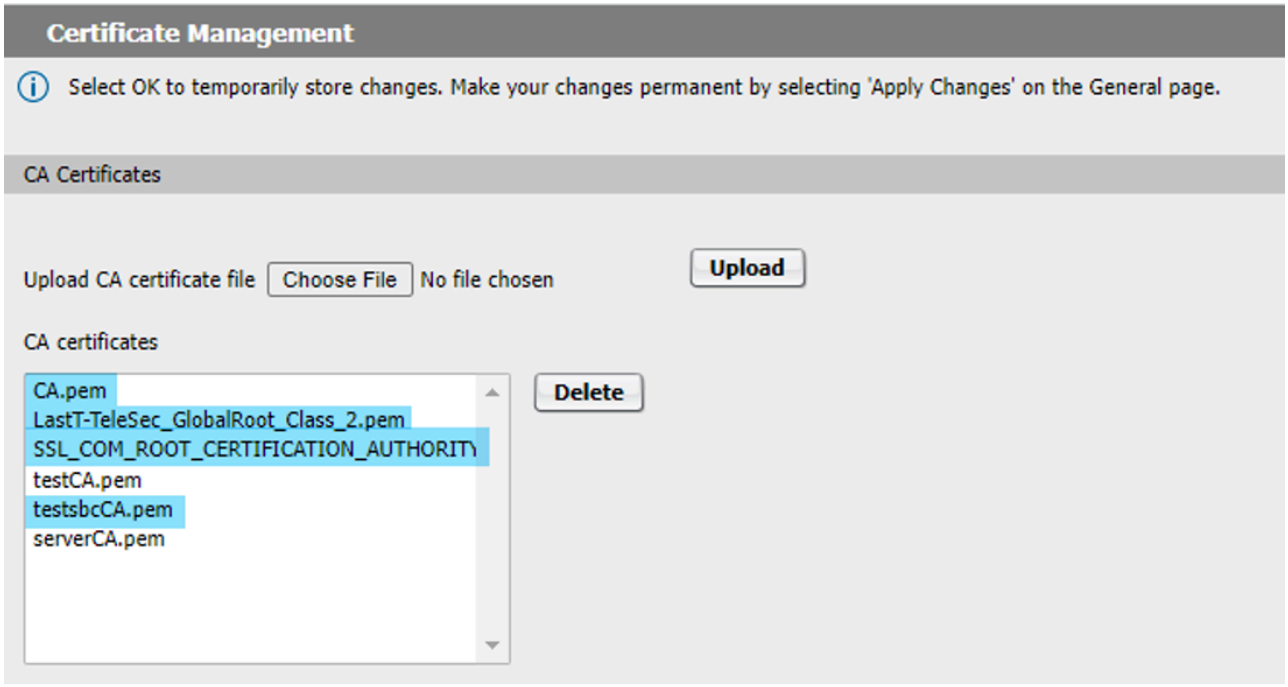


Figure 39: Uploading Certificates (1 of 2)

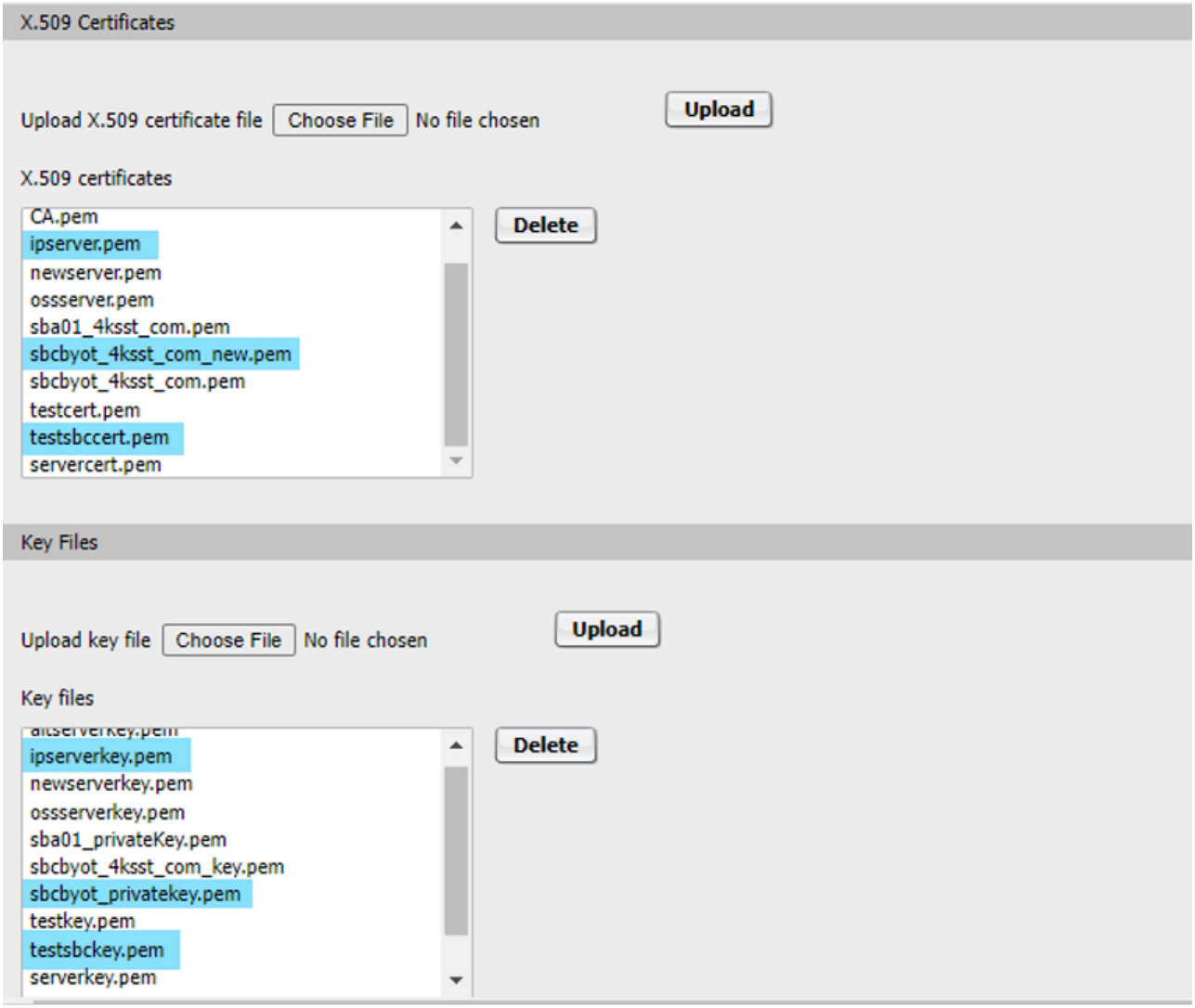


Figure 40: Uploading Certificates (2 of 2)

6.9.3 Creating Certificate Profiles

Create certificate profiles for the following scenarios:

- **PSTN Connectivity Certificate Profile.** This profile must be mapped to the PSTN certificates if PSTN connectivity is configured over the TLS protocol. The SSP provider should be contacted for information about the needed certificates for PSTN connectivity.

> **Important**:
> This PSTN certificate profile is not required if the MBG is used for the SSP connection.

- **Microsoft Teams Certificate Profile.** This profile must be mapped to the Microsoft Teams certificates. Certificates used for communication with Microsoft Teams should be generated and uploaded to OpenScape SBC for TLS communication with Microsoft Teams in port 5061.

- **MX-ONE Certificate Profile.** This profile must be mapped to the MX-ONE certificates. If communication with MX-ONE is configured through TLS protocol then the certificates related to TLS protocol should be generated and uploaded.

> **Note**:
> This MX-ONE certificate profile is only needed if TLS is active in MX-ONE and TLS connectivity is desired between MX-ONE and OpenScape SBC.

To create certificate profiles:

1. In SBC management portal, navigate to **Security > General > Certificate Management**.
2. On **Certificate Profiles**, click on **Add** to configure the certificate profile.

3. In the **Certificate Profile** window that opens, create certificate profile for **Microsoft Teams**.

   a. Configure **Certificate Profile configuration** as follows:

      i. Set **Certificate profile name** as **Teams_Cert_Profile**.
      ii. Set **Local client certificate file** as environment specific value.
      iii. Set **Local server certificate file** as environment specific value.
      iv. Set **Local CA file** as environment specific value.
      v. Set **Remote CA file** as environment specific value.
      vi. Set **Local key file** as environment specific value.

   b. Click **OK** to save the configuration.

The following figures depict the sample **Certificate Profiles** for **Microsoft Teams**.

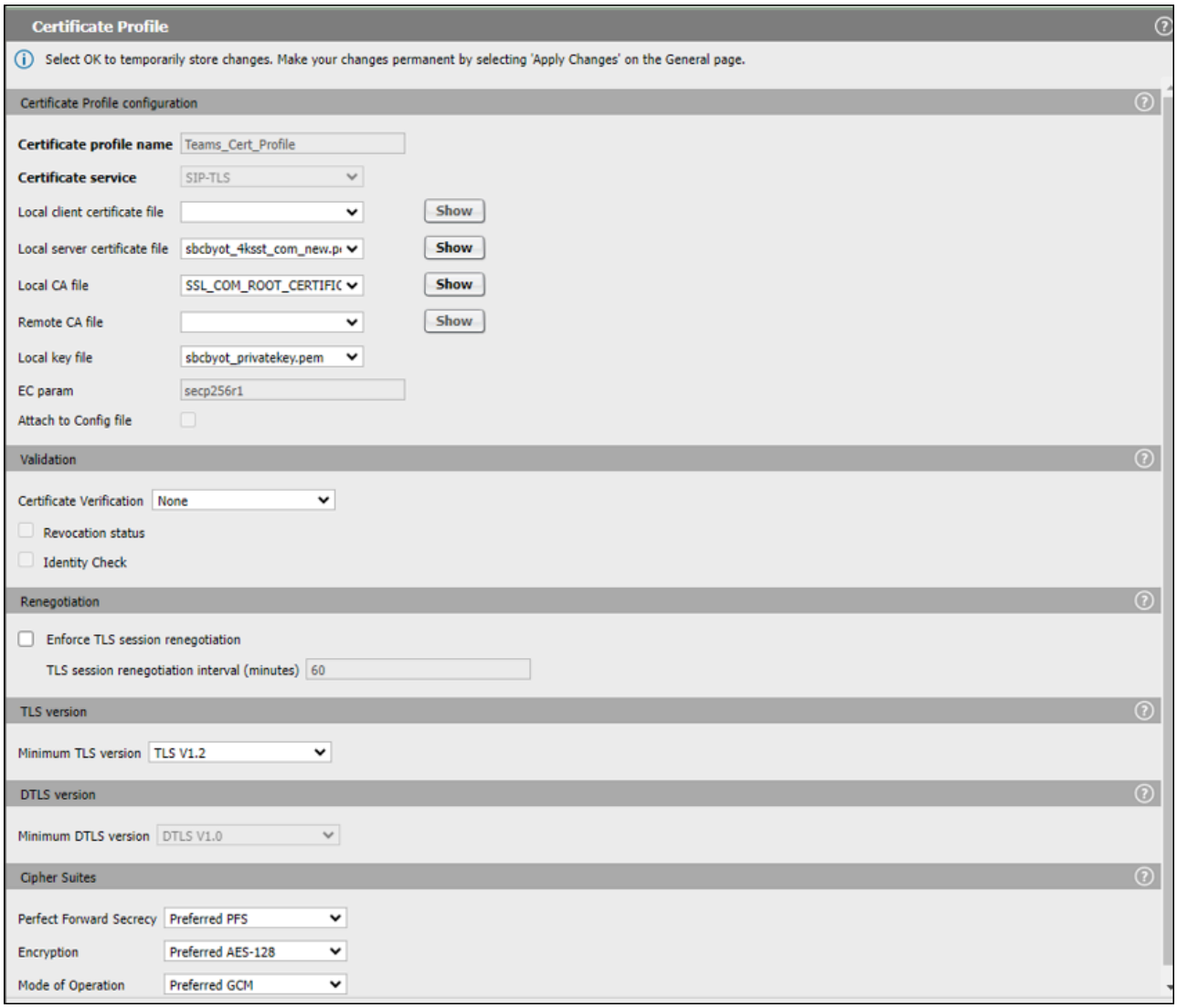


Figure 41: Microsoft Teams Certificate Profile Configuration

4. Create certificate profile for **MX-ONE**.

Note:
The following configurations are only for reference. The MX-ONE certificate profile must be configured as per the site environment.

a. Configure **Certificate Profile configuration** as follows:

   i. Set **Certificate profile name** as **MXONE**.
   ii. Set **Certificate service** as **SIP-TLS**.
   iii. Set **Local client certificate file** as environment specific value.
   iv. Set **Local server certificate file** as environment specific value.
   v. Set **Local CA file** as environment specific value.
   vi. Set **Remote CA file** as environment specific value.
   vii. Set **Local key file** as environment specific value.

b. Configure **Validation** as follows:

   i. Set **Certificate Verification** as **None**.
   ii. Deselect **Revocation status**.
   iii. Deselect **Identity Check**.

c. Configure **Renegotiation** as follows:

   i. Deselect **Enforce TLS session renegotiation**.
   ii. Set **TLS session renegotiation interval (minutes)** as **60**.

d. Set **Minimum TLS version** as **TLS V1.2**.
e. Set **Minimum DTLS version** as **DTLS V1.0**.
f. Configure **Cipher Suites** as follows:

   i. Set **Perfect Forward Secrecy** as **Preferred PFS**.
   ii. Set **Encryption** as **Preferred AES-128**.
   iii. Set **Mode of Operation** as **Preferred GCM**.

g. Click **OK** to save the configuration.

The following figures depict the sample **Certificate Profiles** for **MX-ONE**.

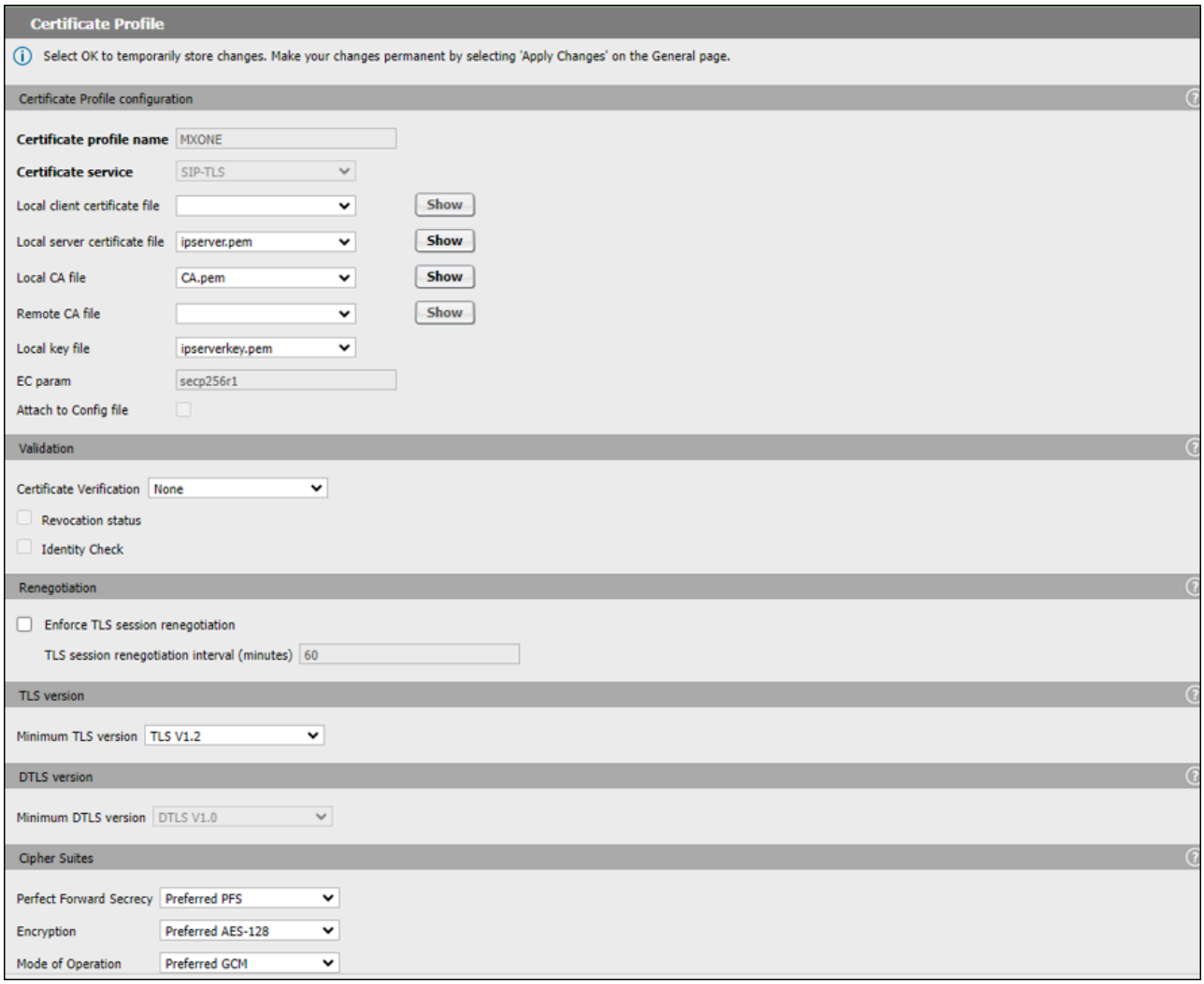


Figure 42: MX-ONE Certificate Profile Configuration

5. Click **OK**.
6. In the **Certificate Management** page that opens, click **OK** and then click **Apply Changes** to save the certificate configuration.

6.10 Configuring SIP Service Provider Profiles

To configure SIP service provider profiles:

1. In SBC management portal, navigate to the **Features**.
2. Select **Enable Remote Endpoints** and click on **Configure**. The **Remote Endpoints** window is displayed.
3. Click **Add** under **SIP Service Provider Profile** to configure the SIP service provider profile for **PSTN** based on your SIP Service Provider. The following are the example configuration for DTAG/Company Flex.

Important:
This step is not required if the MBG is used for the SSP connection.

a. Configure General as follows:

i. Set **Name** as **CompanyFlex**.
ii. Set **Default SSP profile** as **DTAG/Company Flex**.

b. Configure **SIP Privacy** as follows:

i. Set **Privacy support** as **Full**.

The following figure depicts the SIP Service Provider Profile for **PSTN**.

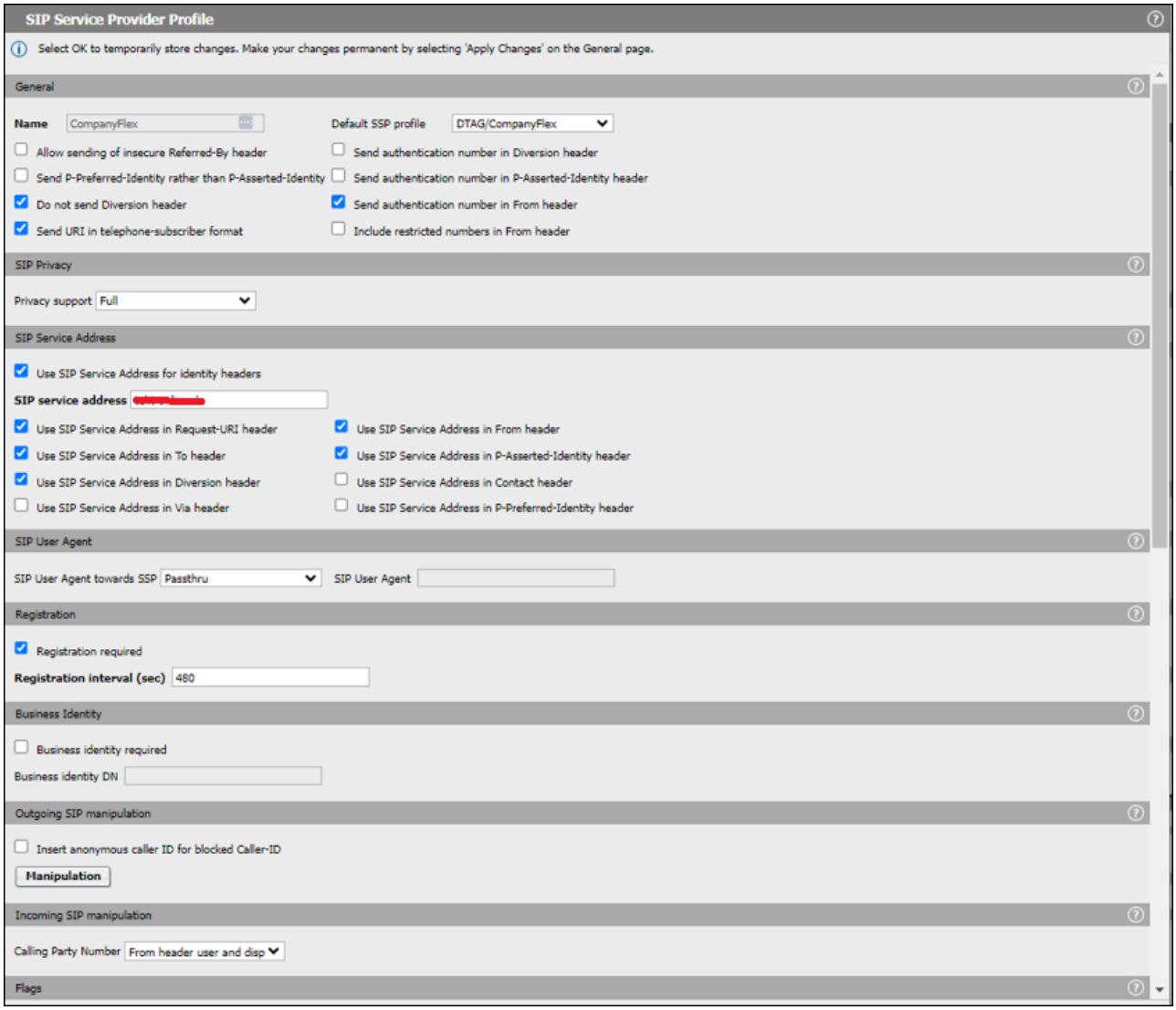


Figure 43: PSTN SIP Service Provider Profile (1 of 2)

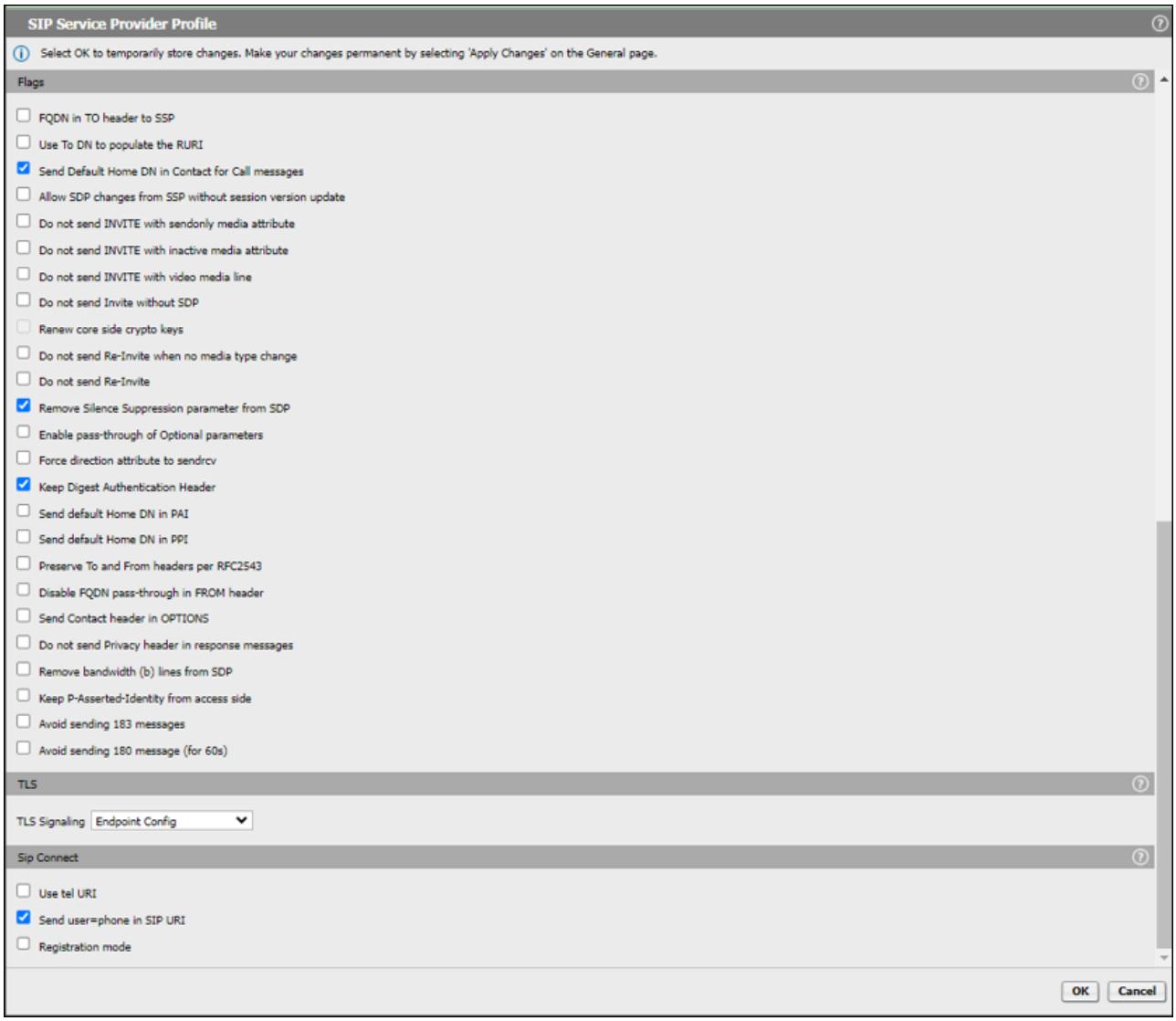


Figure 44: PSTN SIP Service Provider Profile (2 of 2)

a. Click **OK** to save the configuration.

4. Click **Add** under **SIP Service Provider Profile** to configure the SIP service provider profile for **Microsoft Teams** as listed in the following table.

   a. Configure **General** as follows:

      i. Set **Name** as **4Teams**.
      ii. Set **Default SSP profile** as **MS Teams**.

   b. Configure **SIP Service Address** as follows:

      i. Set **SIP service address** as **SBC FQDN**.

The following figure depicts the SIP Service Provider Profile for **Microsoft Teams**.

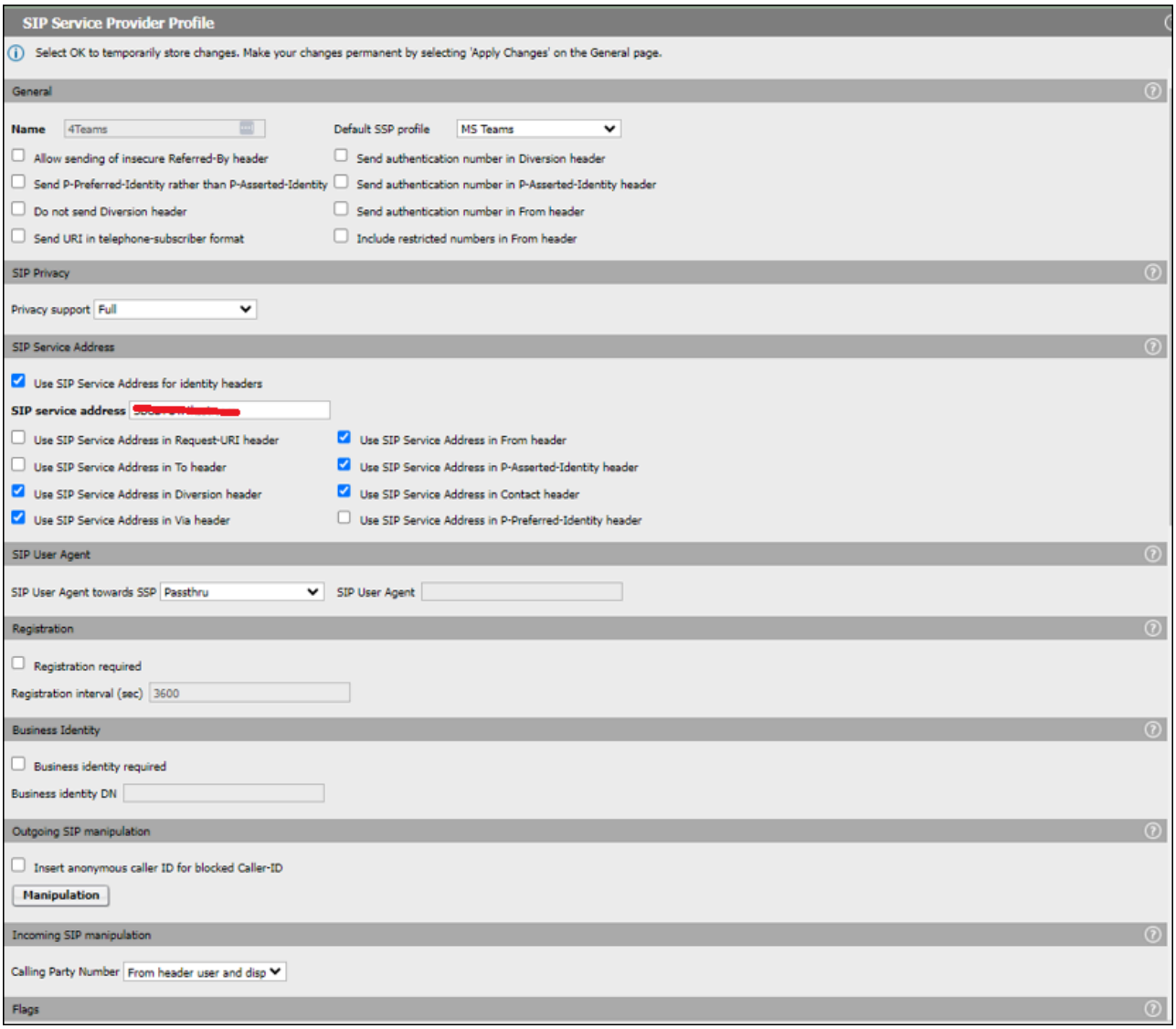


Figure 45: Microsoft Teams SIP Service Provider Profile (1 of 2)

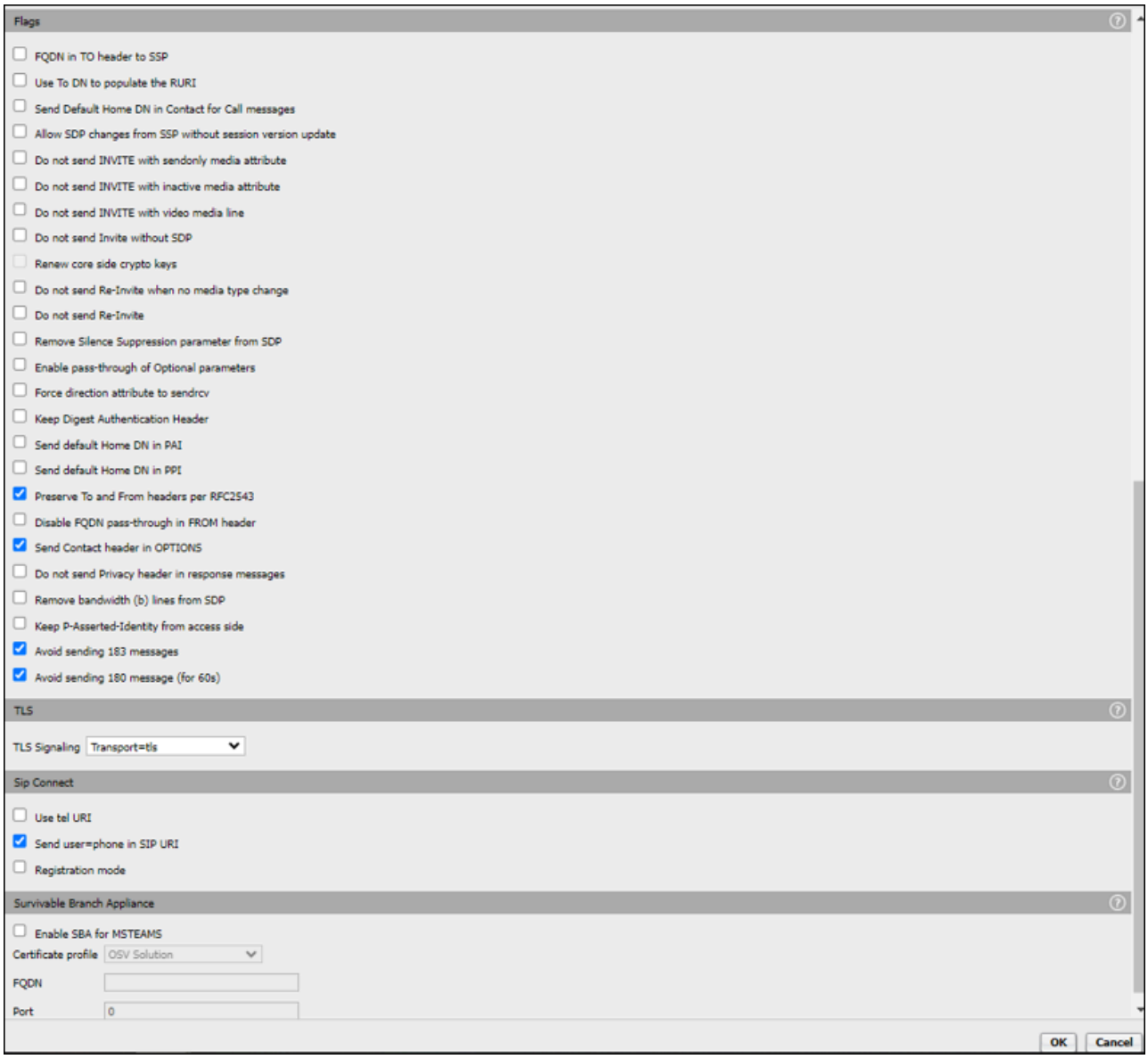


Figure 46: Microsoft Teams SIP Service Provider Profile (2 of 2)

a. Click **OK** to save the configuration.

5. Click **Add** under **SIP Service Provider Profile** to configure the SIP service provider profile for **MX-ONE Profile 1** as listed in the following table.

   a. Configure **General** as follows:

      i. Set **Name** as **MXONE**.
      ii. Do not configure **Default SSP profile** field. Keep it as an empty value.

The following figure depicts the SIP Service Provider Profile for **MX-ONE Profile 1**.

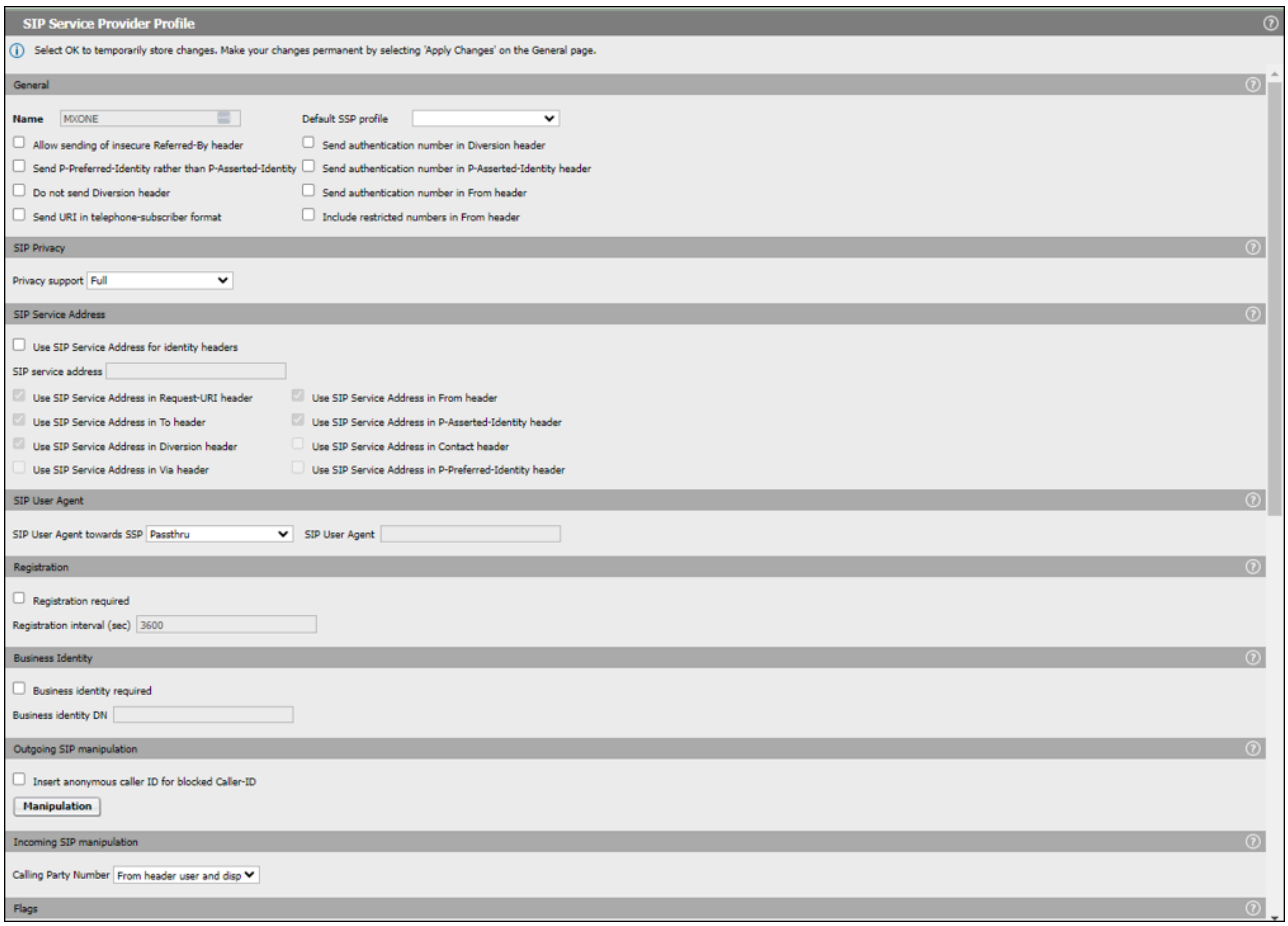


Figure 47: MX-ONE SIP Service Provider Profile 1 (1 of 2)

Figure 48: MX-ONE SIP Service Provider Profile 1 (2 of 2)

a. Click **OK** to save the configuration.

6. Click **Add** under **SIP Service Provider Profile** to configure the SIP service provider profile for **MX-ONE Profile 2** as listed in the following table.

Important:
This step is not required (MX-ONE Profile 2) if the MBG is used for the SSP connection.

a. Configure **General** as follows:

i. Set **Name** as **UOffice**.
ii. Set **Default SSP profile** as **UOffice**.

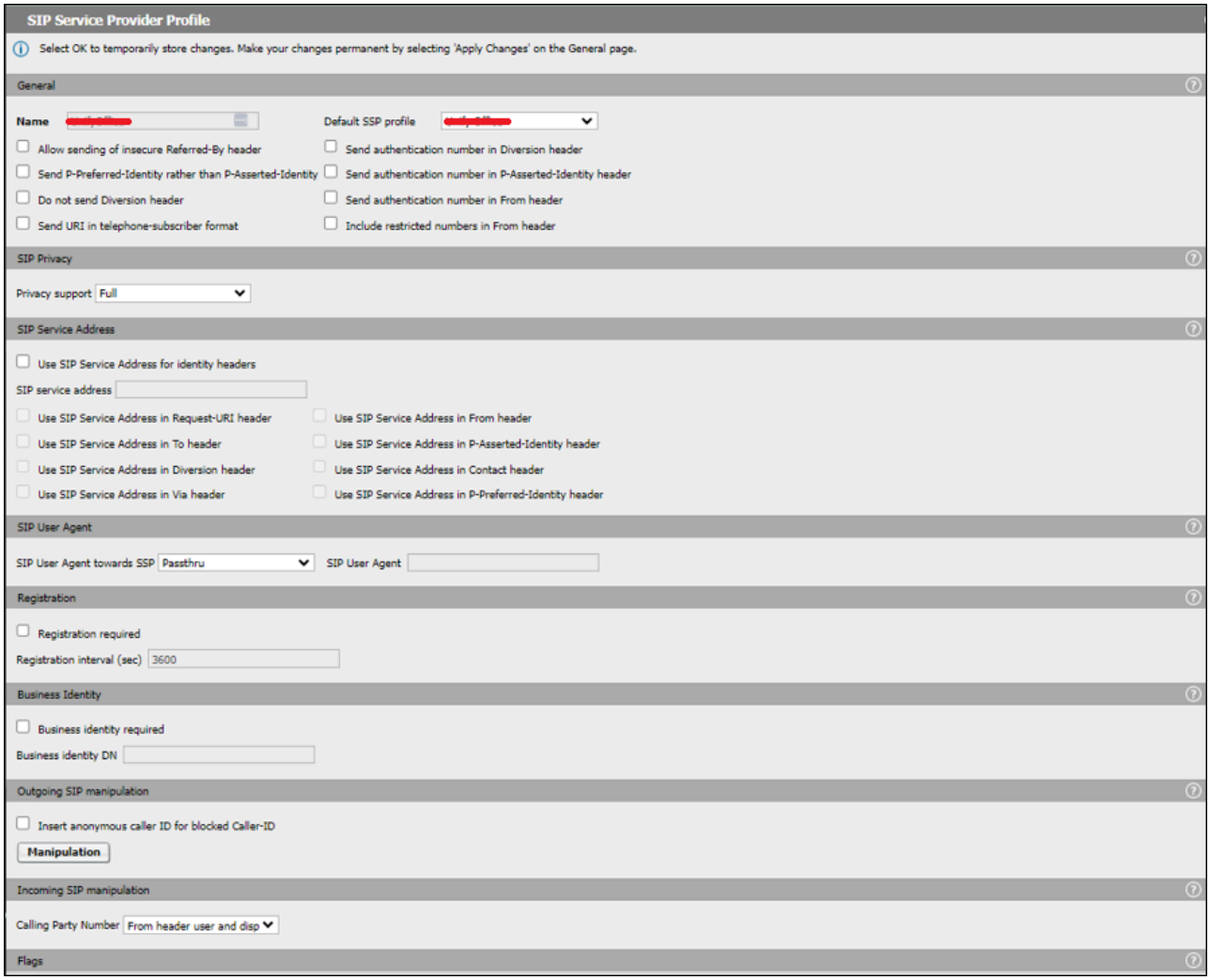


Figure 49: MX-ONE SIP Service Provider Profile 2 (1 of 2)

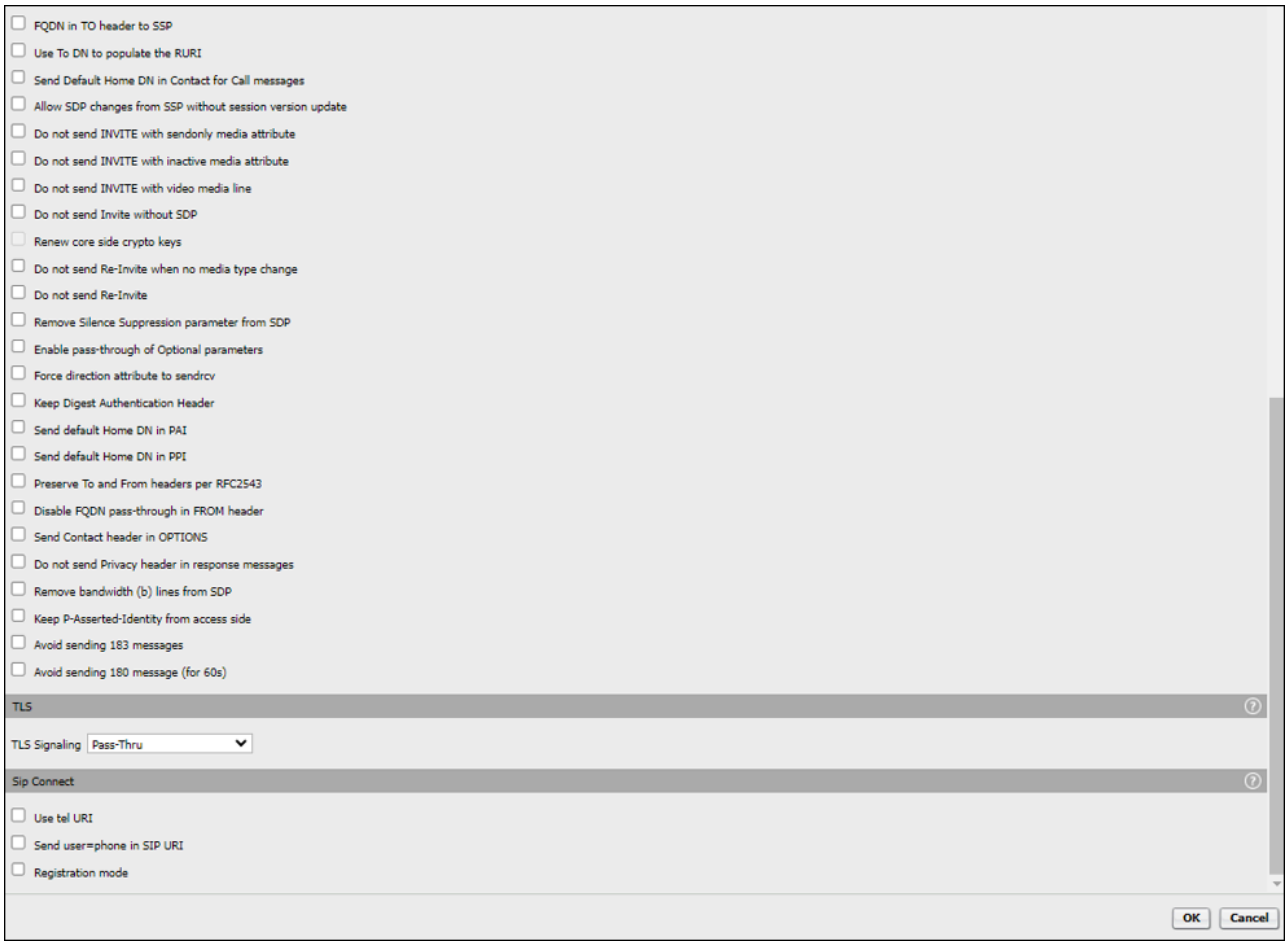


Figure 50: MX-ONE SIP Service Provider Profile 2 (2 of 2)

a. Click **OK** to save the configuration.

7. Click **OK** and then click **Apply Changes** to save the configuration.

6.11 Configuring Remote Endpoints

An endpoint refers to a remote computing device engaged in bidirectional communication with a connected network. After Configuring SIP Service Provider Profiles on page 71, configure remote endpoints:

1. In SBC management portal, navigate to the **Features > Enable Remote Endpoints > Configure Remote Endpoints** tab in the navigation tree under **Administration**.
2. Click **Add** on **Remote endpoint configuration** to configure remote endpoint for **PSTN**. The following are the example configuration for the **CompanyFlex**.

Important:
This step is not required if the MBG is used for the SSP connection.

a. Configure **Remote Endpoint Settings**:

   i. Set **Name** as **CompanyFlex**.
   ii. Set **Type** as **SSP**.
   iii. Select **Profile** as **CompanyFlex** from the drop down menu.
   iv. Set **Access realm profile** as **Main-Access-Realm - ipv4**.
   v. Set **Core realm profile** as **Main-Core-Realm - ipv4**.

b. Configure **Remote Location Information**:

   i. Set **Signaling address type** as **DNS SRV**.

c. Configure **Remote Location domain list**. Click on **Add** to create an entry for remote location domain list.

   i. Configure **General**:

      a) Set **Remote URL** as environment specific value indicated by your SIP service provider.
      b) Set **Remote port** as **0**.
      c) Set **Remote transport** as **TLS**.

   ii. Configure **TLS**:

      a) Set **TLS mode** as **Mutual authentication**.
      b) Set **Certificate profile** as **SSP_TELEKOM**.
      c) Select **TLS keep-alive**.
      d) Set **Keep-alive interval (seconds)** as **60**.
      e) Set **Keep-Alive timeout** as **10**.

   iii. Configure **Media Configuration**:

      a) Set **Media profile** as **DT_TLS**.
      b) Set **Media realm subnet IP address** as environment specific value.

   iv. Configure **Outbound Proxy Configuration**:

      a) Set **Outbound Proxy** as environment specific value.
      b) **Outbound Proxy Port: 0**. This parameter is configured automatically by the system.

   v. Configure **Registrar Server Configuration**:

      a) Set **Registrar Server** as environment specific value.
      b) Set **Registrar Server Port** as **0**.

   vi. Click **Ok** to save the configuration.

d. Configure **Remote Location Identification/Routing**:

i. Set **Core realm port** as **51999**.
ii. Set **Default home DN** as environment specific value.

e. Configure **Digest Authentication**:

i. Select **Digest authentication supported**.
ii. Set **Digest authentication realm** as environment specific value.
iii. Set **Digest authentication user ID** as environment specific value.
iv. Set **Digest authentication password** as environment specific value.

f. Configure **Miscellaneous**:

i. Select **Open external firewall pinhole**.

g. Click **OK** to save the configuration.

The following figure depicts the remote endpoint configuration for **PSTN**.

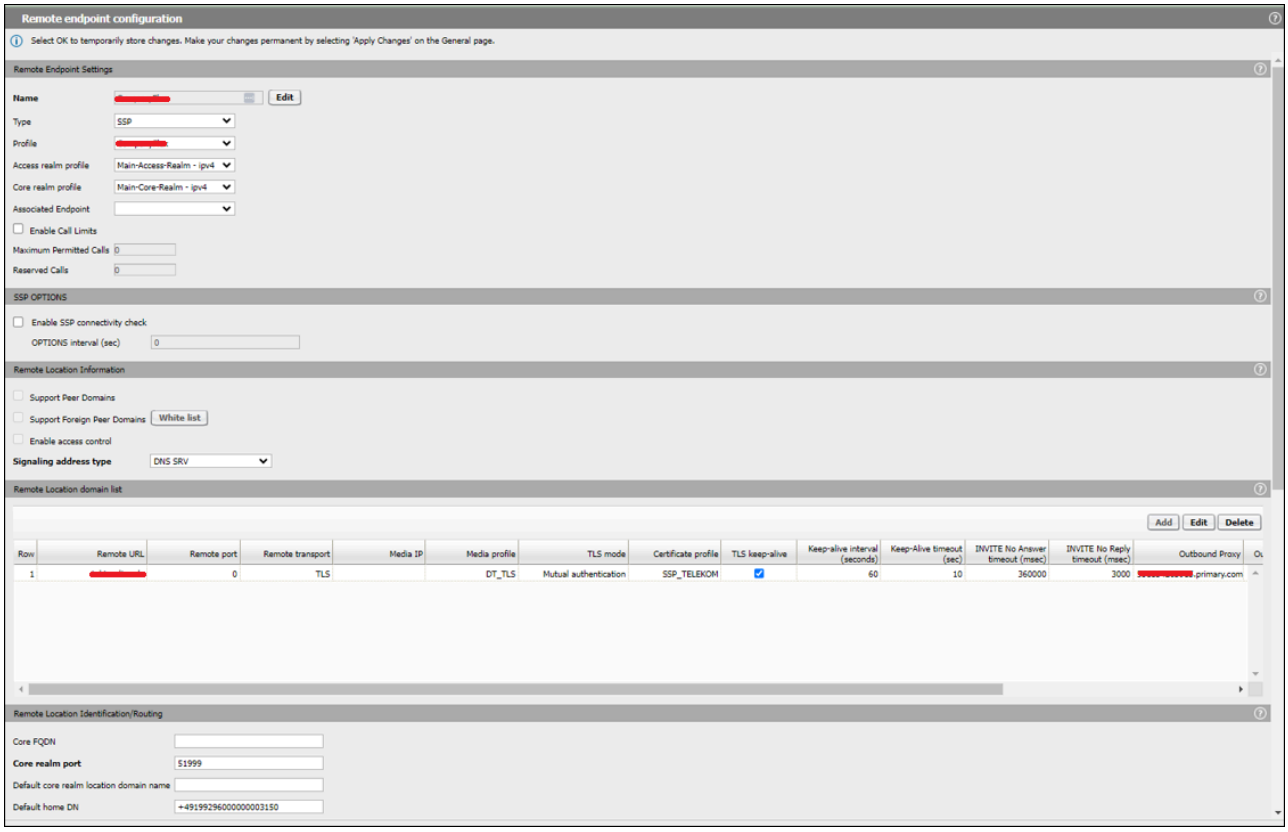


Figure 51: PSTN Remote Endpoint Configuration (1 of 3)

Figure 52: PSTN Remote Endpoint Configuration (2 of 3)

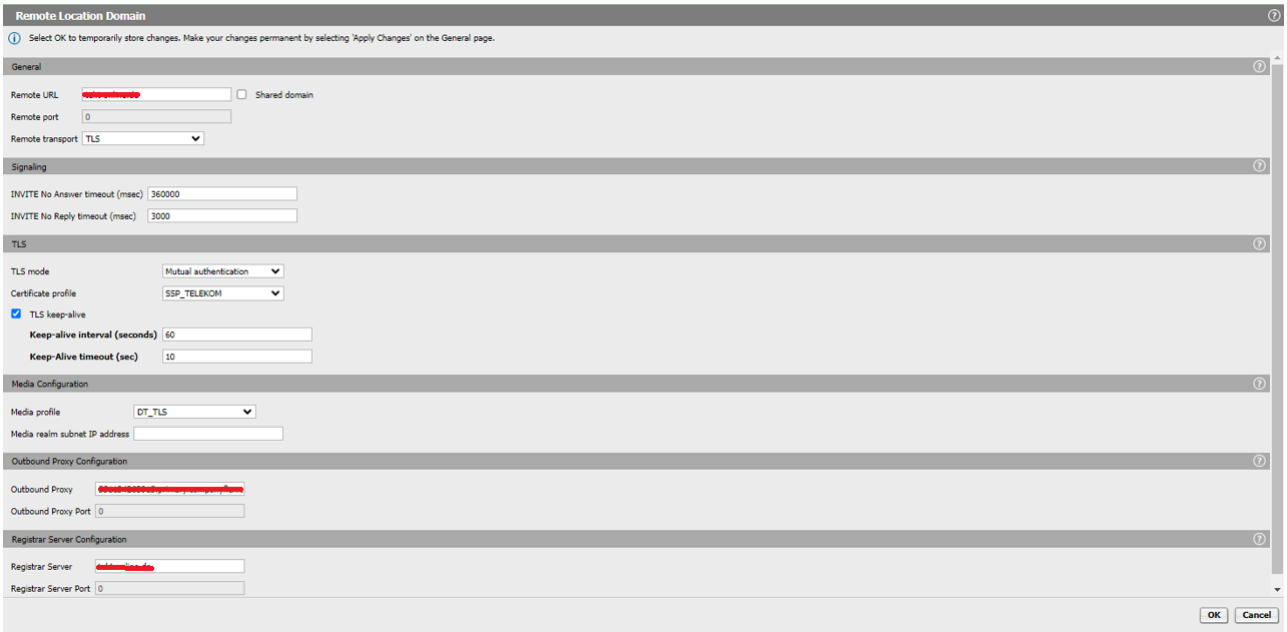


Figure 53: PSTN Remote Endpoint Configuration (3 of 3)

3. Click **Add** on **Remote endpoint configuration** to configure three remote endpoint for **Microsoft Teams**.

Note:
Three remote endpoints must be created for Microsoft Teams. The following configuration lists the sample entry for *Teams_SP1* (sip.pstnhub.microsoft.com). In same way create other two entries for *Teams_SP2* (sip2.pstnhub.microsoft.com) and *Teams_SP3* (sip3.pstnhub.microsoft.com).

a. Configure **Remote Endpoint Settings**:

   i. Set **Name** as **Teams_SP1**.
   ii. Set **Type** as **SSP**.
   iii. Set **Profile** as **4Teams**.
   iv. Set **Access realm profile** as **Main-Access-Realm - ipv4**.
   v. Set **Core realm profile** as **Main-Core-Realm - ipv4**.

b. Configure **SSP OPTIONS**:

   i. Select **Enable SSP connectivity check**.

c. Configure **Remote Location domain list**. Click on **Add** to create an entry for remote location domain list.

   i. Configure **General**:

      a) Set **Remote URL** as **sip.pstnhub.microsoft.com**.
      b) Set **Remote port** as **5061**.
      c) Set **Remote transport** as **TLS**.

   ii. Configure **TLS**:

      a) Set **TLS mode** as **Mutual authentication**.
      b) Set **Certificate profile** as **Teams_Cert_Profile**.

   iii. Configure **Media Configuration**:

      a) Set **Media profile** as **Teams**.

   iv. Click **Ok** to save the configuration.

d. Configure **Remote Location Identification/Routing**:

   i. Set **Core realm port** as **51000**.

Note:

Configure **Core realm port** as follows:

- 51000 for Teams_SP1.
- 51001 for Teams_SP2.
- 51002 for Teams_SP3.

e. Click **OK** to save the configuration.

The following figure depicts the remote endpoint configuration for **Microsoft Teams**.

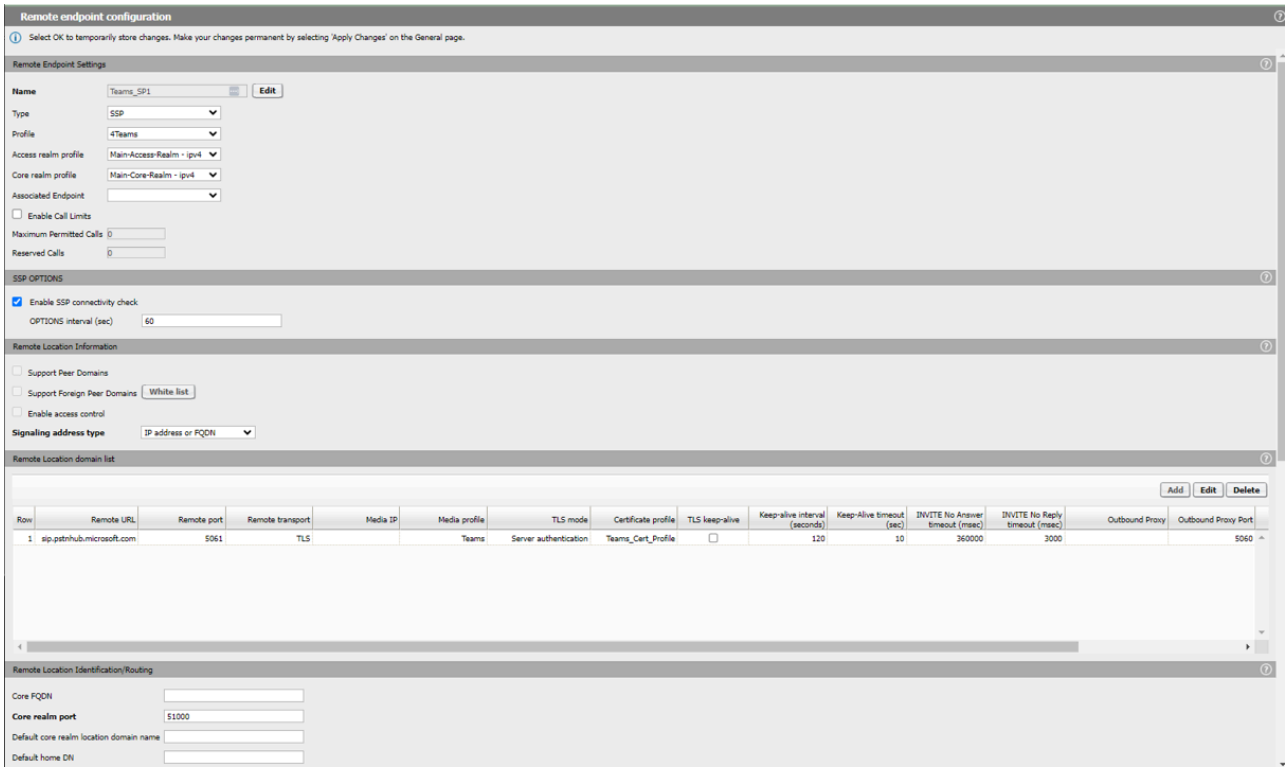


Figure 54: Microsoft Teams Remote Endpoint Configuration (1 of 3)

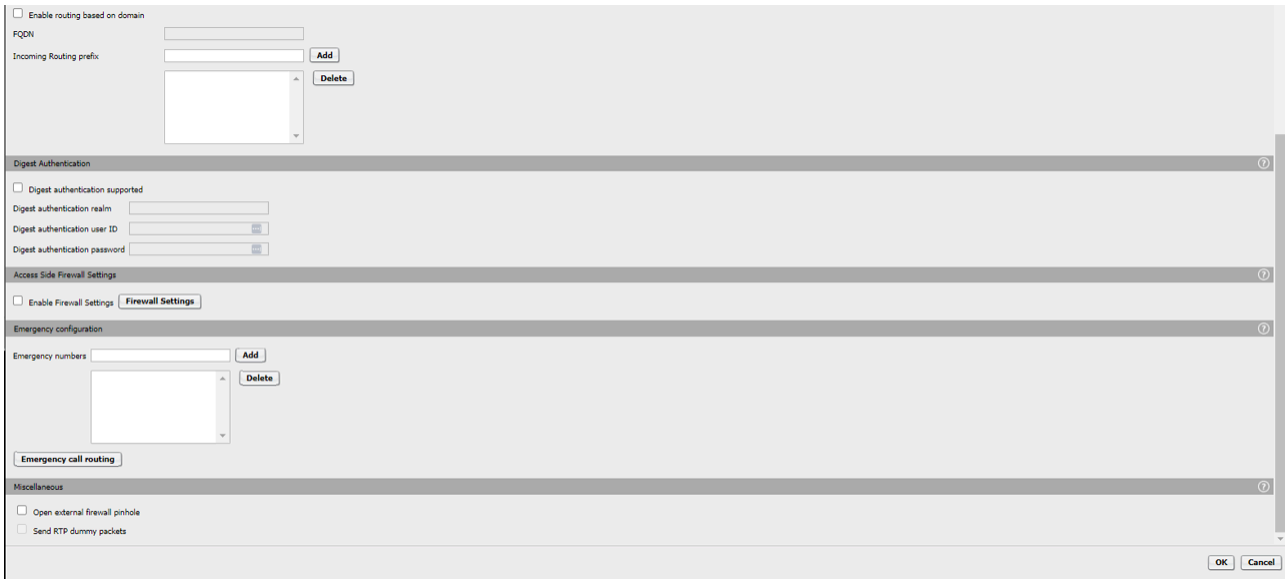


Figure 55: Microsoft Teams Remote Endpoint Configuration (2 of 3)

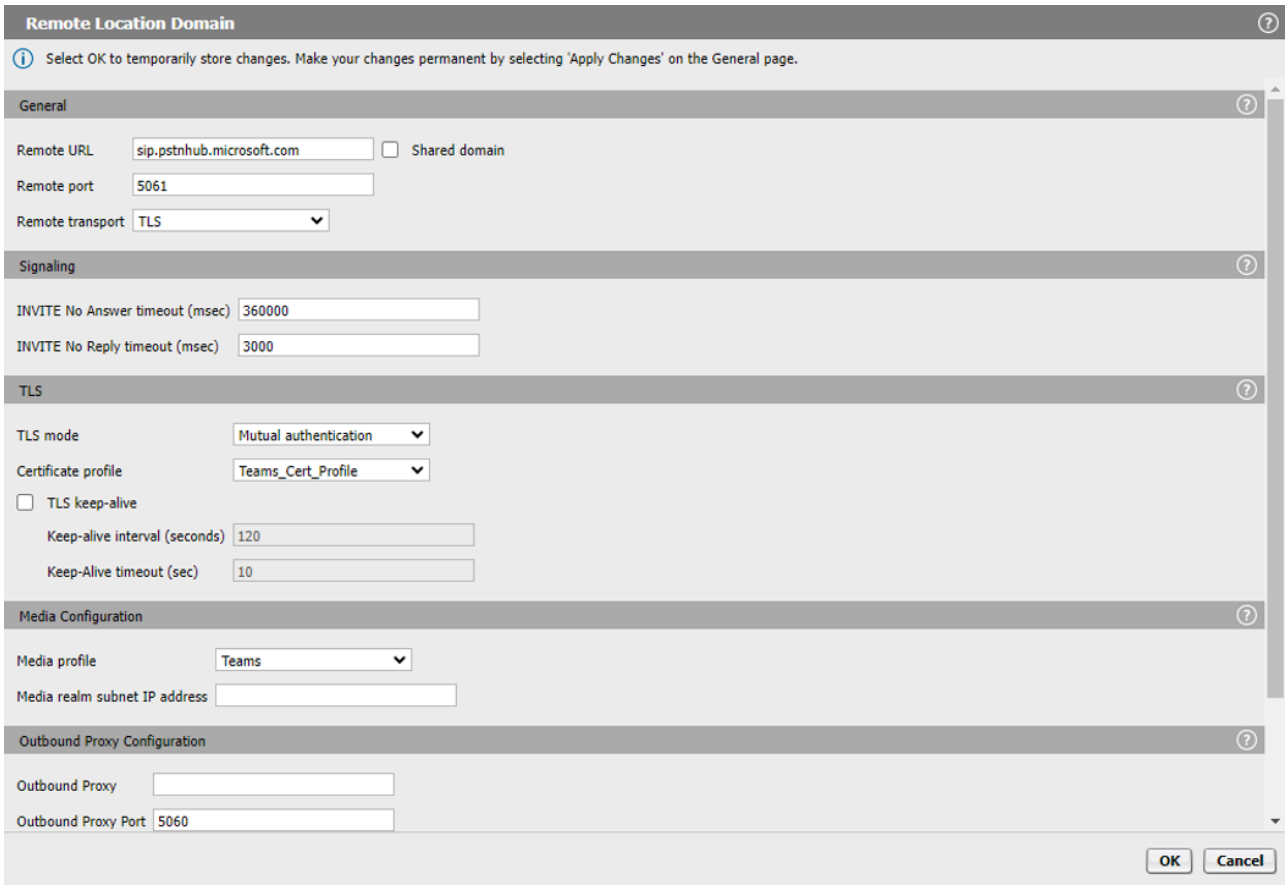


Figure 56: Microsoft Teams Remote Endpoint Configuration (3 of 3)

4. Click **Add** on **Remote endpoint configuration** to configure remote endpoint for **MX-ONE to PSTN**.

Important:
This step is not required if the MBG is used for the SSP connection.

a. Configure **Remote Endpoint Settings**:

i. Set **Name** as **MX-ONEtoSSP**.
ii. Set **Type** as **SSP**.
iii. Set **Profile** as **UOffice**.
iv. Configure **Access realm profile**:

- For single-arm configuration, select **Second-Access-Realm - ipv4**.
- For multiple-arm configuration, select **Main-Access-Realm - ipv4**.

v. Set **Core realm profile** as **Main-Core-Realm - ipv4**.

b. Configure **SSP OPTIONS**:

i. Select **Enable SSP connectivity check**.

c. Configure **Remote Location domain list**. Click on **Add** to create an entry for remote location domain list.

i. Configure **General**:

a) Set **Remote URL** as environment specific value (MX-ONE IP address).
b) Set **Remote port** as **5061**.
c) Set **Remote transport** as **TLS**.

ii. Configure **TLS**:

a) Set **TLS mode** as **Server authentication**.
b) Set **Certificate profile** as **MXONE**.

iii. Configure **Media Configuration**:

a) Set **Media profile** as **Mitel**.

iv. Click **Ok** to save the changes.

d. Configure **Remote Location Identification/Routing**:

i. Set **Core realm port** as **54000**.

> **Note**:
> Two remote endpoints should be created due to the limitation of OpenScape SBC to route calls from SSP-to-SSP media type. Therefore, two similar remote endpoints for MX-ONE should be created. In addition, the first MX-ONE is used to route calls to PSTN, and as a result, an Incoming Routing Prefix must be configured.

ii. Set **Incoming Routing prefix** as environment specific value (enter the value and then click on **Add**). This value must be the prefix for the PSTN numbers.

e. Click **OK** to save the configuration.

The following figure depicts the remote endpoint configuration for **MX-ONE to PSTN**.

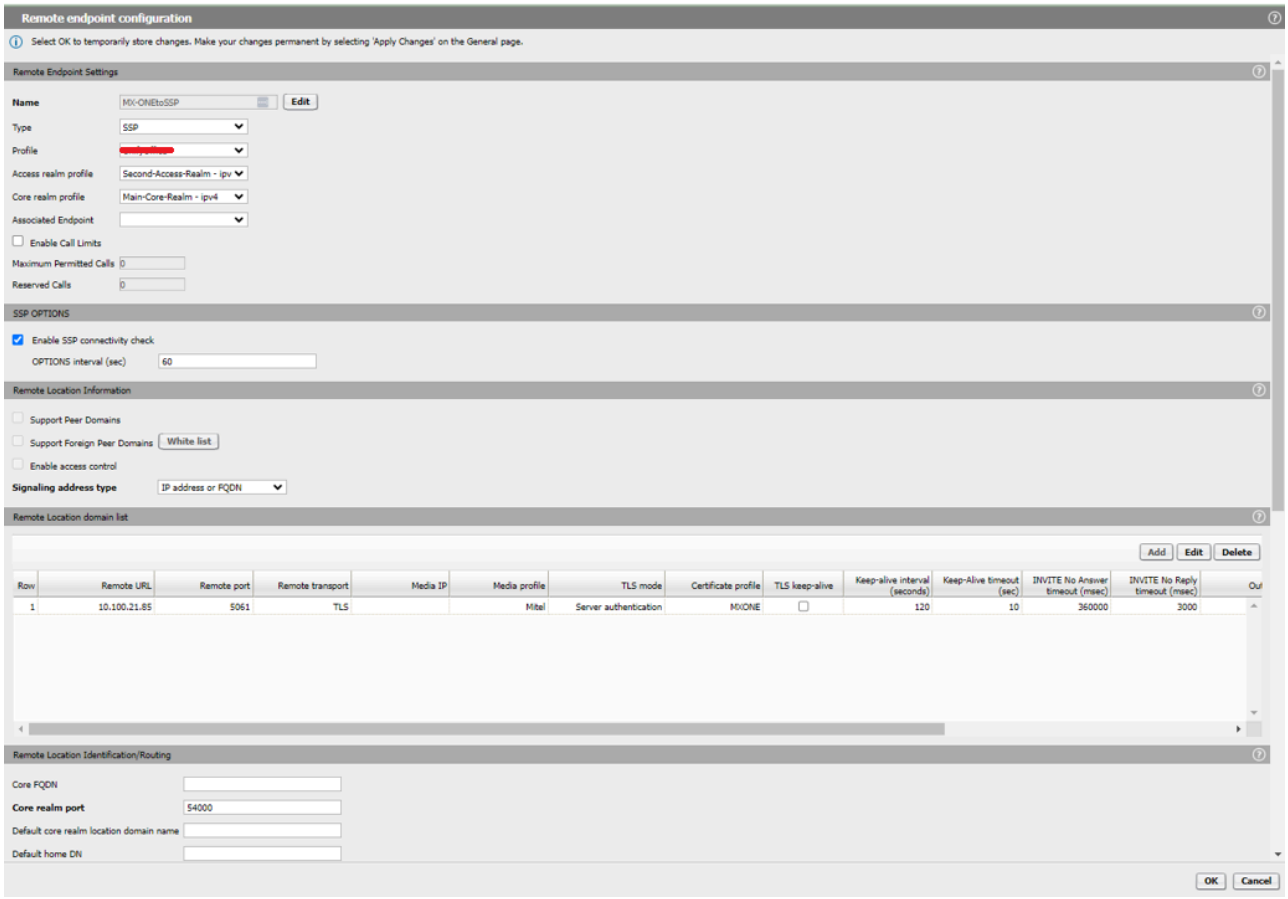


Figure 57: MX-ONE Remote Endpoint Configuration 1 for PSTN (1 of 3)

Figure 58: MX-ONE Remote Endpoint Configuration 1 for PSTN (2 of 3)

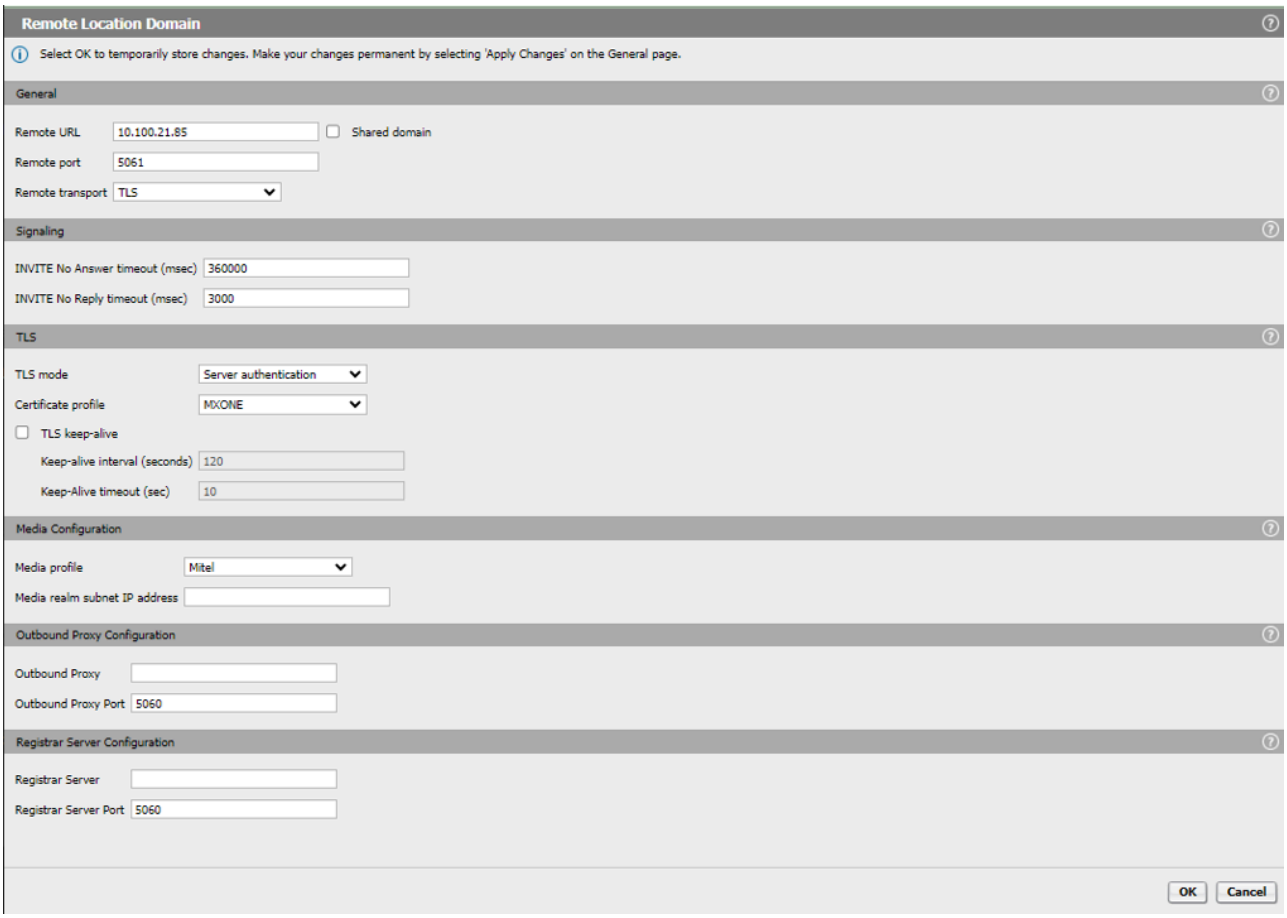


Figure 59: MX-ONE Remote Endpoint Configuration 1 for PSTN (3 of 3)

5. Click **Add** on **Remote endpoint configuration** to configure remote endpoint for **MX-ONE to Microsoft Teams**.

   a. Configure **Remote Endpoint Settings**:

      i. Set **Name** as **MX-ONEtoTeams**.
      ii. Set **Type** as **SSP**.
      iii. Set **Profile** as **MXONE**.
      iv. Set **Access realm profile** as **Second-Access-Realm - ipv4**.
      v. Set **Core realm profile** as **Main-Core-Realm - ipv4**.

   b. Configure **SSP OPTIONS**:

      i. Select **Enable SSP connectivity check**.

   c. Configure **Remote Location domain list**. Click on **Add** to create an entry for remote location domain list.

      i. Configure **General**:

         a) Set **Remote URL** as environment specific value (MX-ONE IP address).
         b) Set **Remote port** as **5061**.
         c) Set **Remote transport** as **TLS**.

      ii. Configure **TLS**:

         a) Set **TLS mode** as **Server authentication**.
         b) Set **Certificate profile** as **MXONE**.

      iii. Configure **Media Configuration**:

         a) Set **Media profile** as **Mitel**.

   d. Configure **Remote Location Identification/Routing**:

      i. Set **Core realm port** as **50010**.

   e. Click **OK** to save the configuration.

The following figure depicts the remote endpoint configuration for **MX-ONE to Microsoft Teams**.

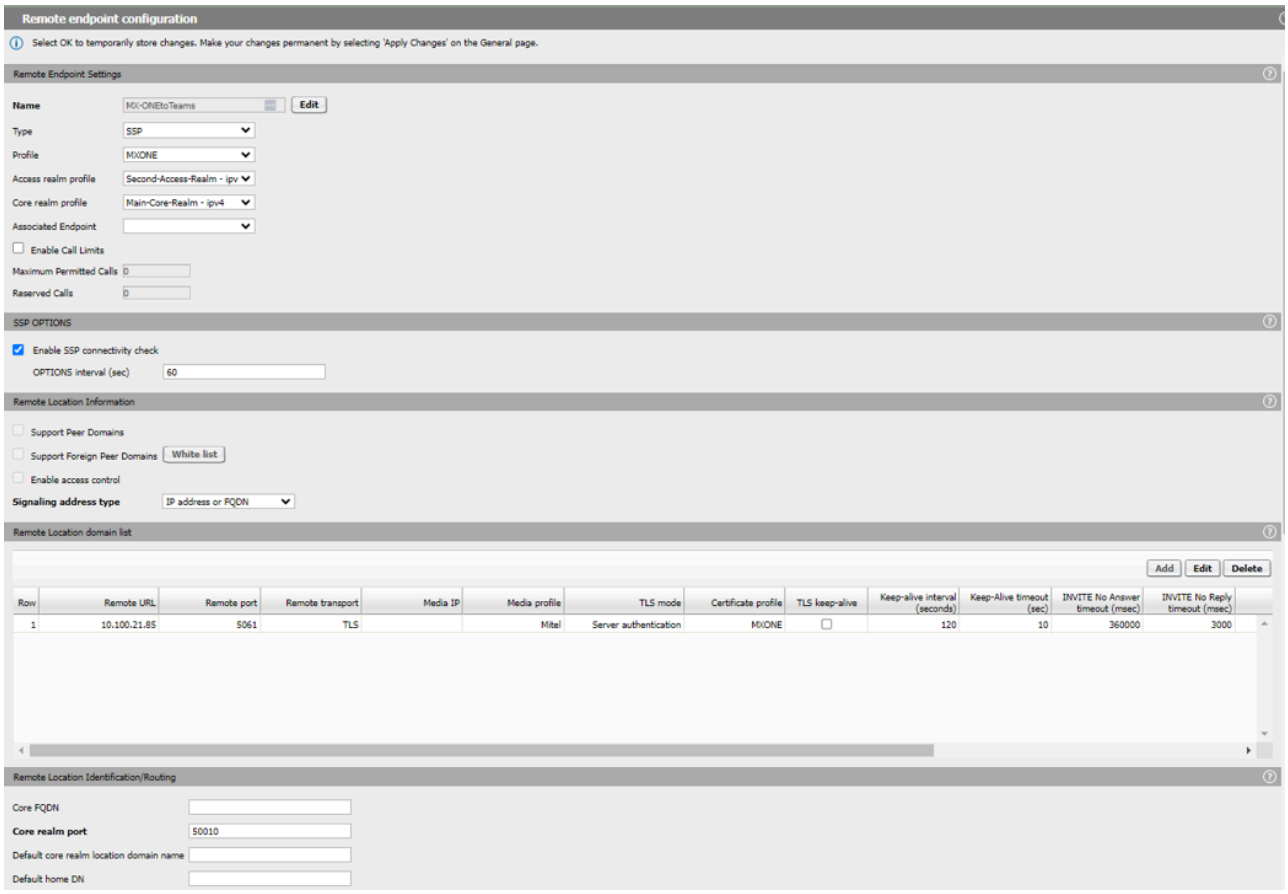


Figure 60: MX-ONE Remote Endpoint Configuration 2 for Microsoft Teams (1 of 3)

Figure 61: MX-ONE Remote Endpoint Configuration 2 for Microsoft Teams (2 of 3)

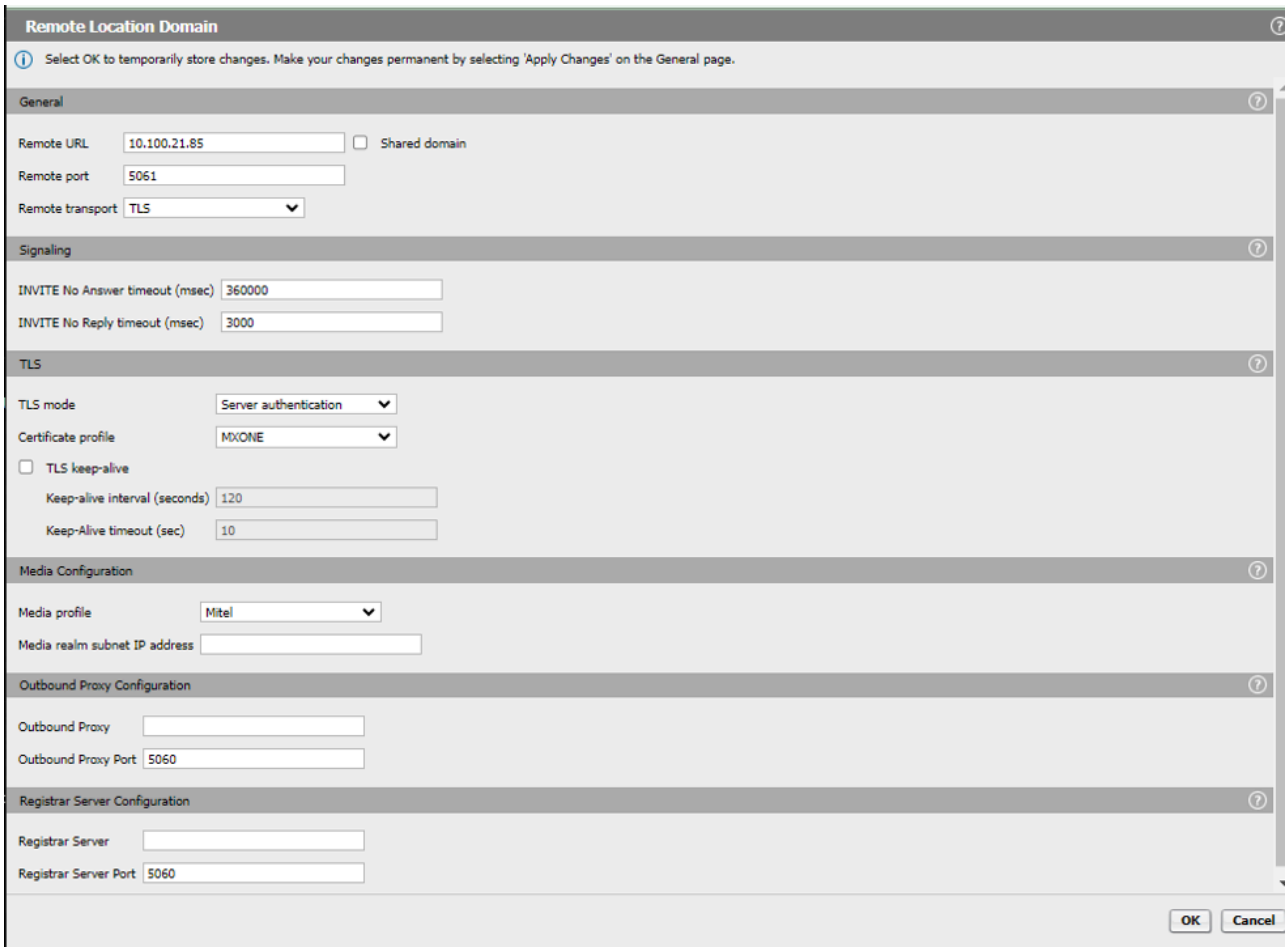


Figure 62: MX-ONE Remote Endpoint Configuration 2 for Microsoft Teams (3 of 3)

6. Click **OK** on all the pop-up windows.
7. Click **Apply Changes** to save the remote endpoint configuration.

6.12 Configuring Direct Routing

A routing table must be created to interconnect the remote endpoints configured in OpenScape SBC. To accomplish this, a group must be created for each SIP Server Provider (SSP) profile, and then relate them as described in this section.

To configure direct routing:

1. In the SBC management portal, navigate to **VoIP > SIP Server Settings** in the navigation tree under **Administration**.

2. Configure the **Comm System Type** as **Standalone with Internal SIP Stack** as depicted in the following figure.

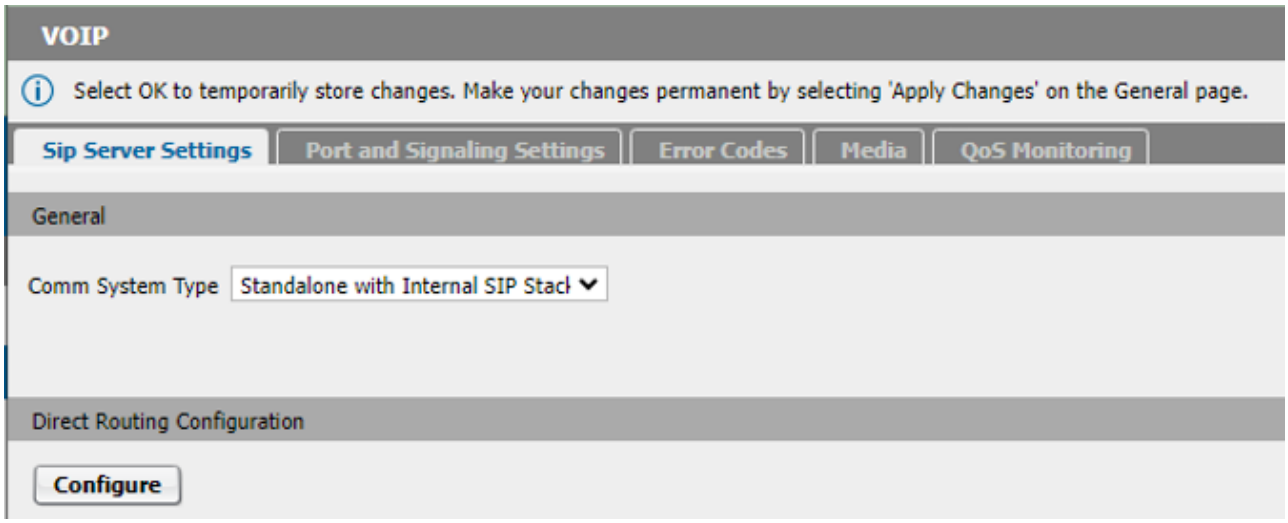


Figure 63: Access Direct Routing Configuration

3. On **Direct Routing Configuration** panel, click on **Configure** to perform the additional configuration.

4. Create the groups and configure endpoints.

   a. Create **MXONE1** group and link to the respective endpoints:

      i. On **Group settings**, configure **Group name** as **MXONE1**.
      ii. Click on **Add group**. The **Group selected** automatically configured as **MXONE1**.
      iii. Select **Group for** as **SSP** endpoints.
      iv. On **Endpoints for group "MXONE1"** panel navigate to the **Endpoints**.
      v. Select **MX-ONEtoTeams** from the drop down menu.
      vi. Click on **Add**.

      The following figure depicts the sample **MXONE1** endpoints configuration.

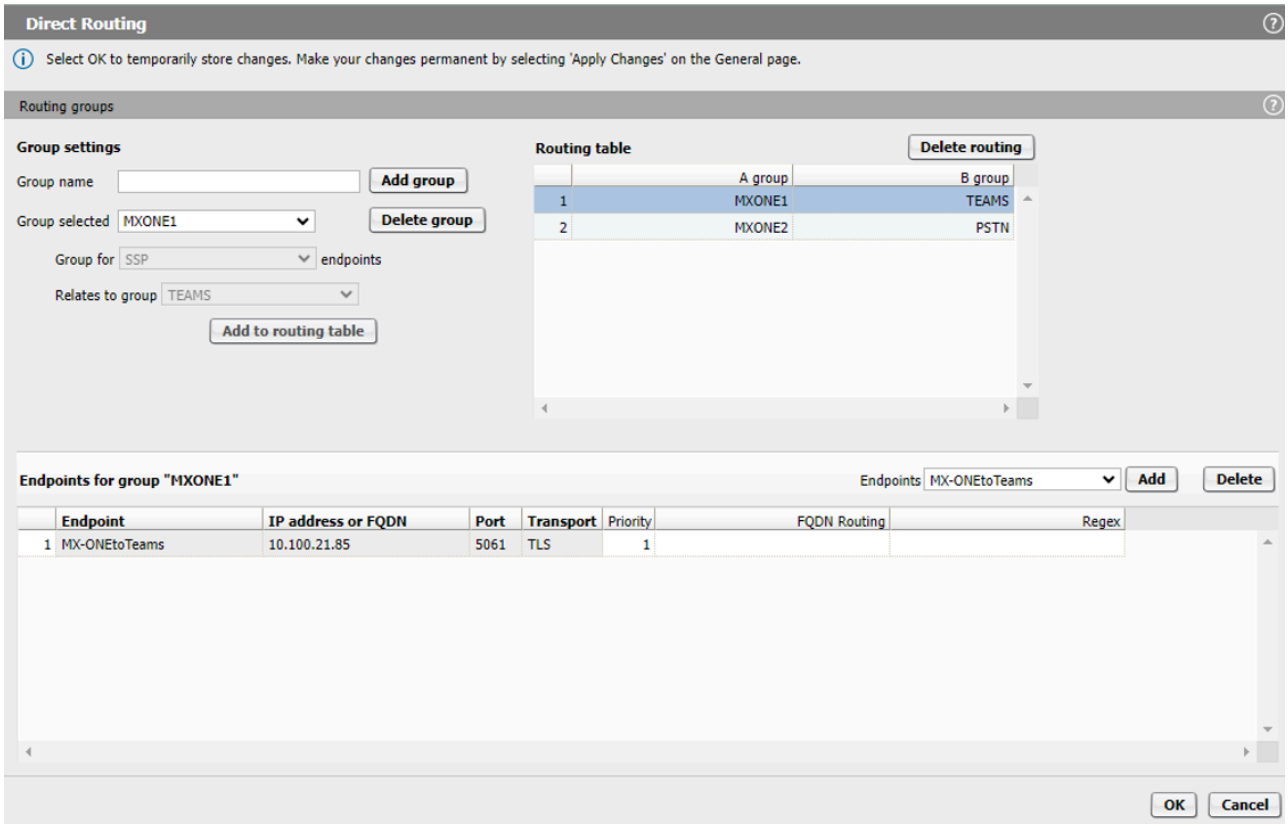


Figure 64: Direct Routing Configuration (MXONE1)

   b. Create **MXONE2** group and link to the respective endpoints:

Important:
This step is not required if the MBG is used for the SSP connection.

i. On **Group settings**, configure **Group name** as **MXONE2**.
ii. Click on **Add group**. The **Group selected** automatically configured as **MXONE2**.
iii. Select **Group for** as **Uoffice**.
iv. On **Endpoints for group "MXONE2"** panel navigate to the **Endpoints**.
v. Select **MX-ONEtoSSP** from the drop down menu.
vi. Click on **Add**.

The following figure depicts the sample **MXONE2** endpoints configuration.

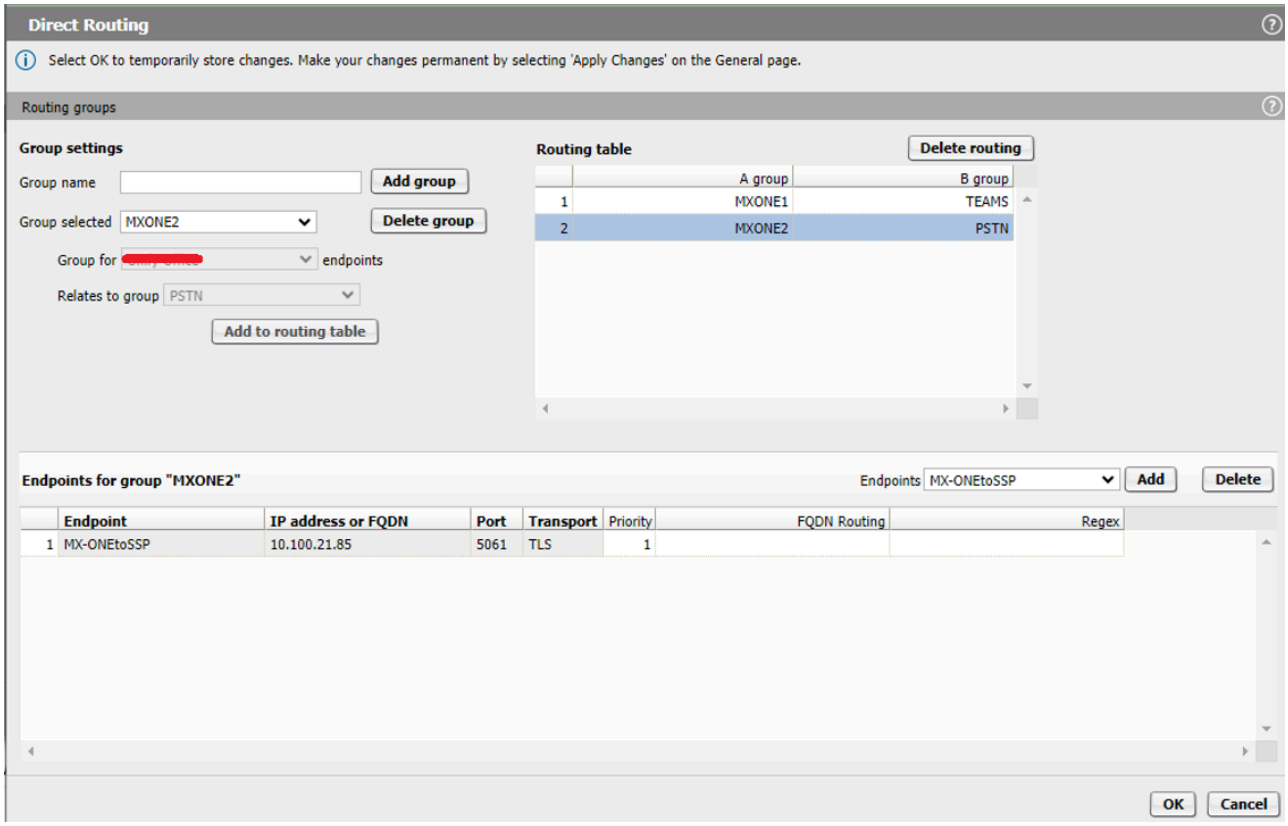


Figure 65: Direct Routing Configuration (MXONE2)

c. Create **PSTN** group and link to the respective endpoints:

Important:
This step is not required if the MBG is used for the SSP connection.

i. On **Group settings**, configure **Group name** as **PSTN**.
ii. Click on **Add group**. The **Group selected** automatically configured as **PSTN**.
iii. Select **Group for** as **SSP** endpoints.
iv. On **Endpoints for group "MXONE1"** panel navigate to the **Endpoints**.
v. Select **CompanyFlex** from the drop down menu.
vi. Click on **Add**.

The following figure depicts the sample **PSTN** endpoints configuration.

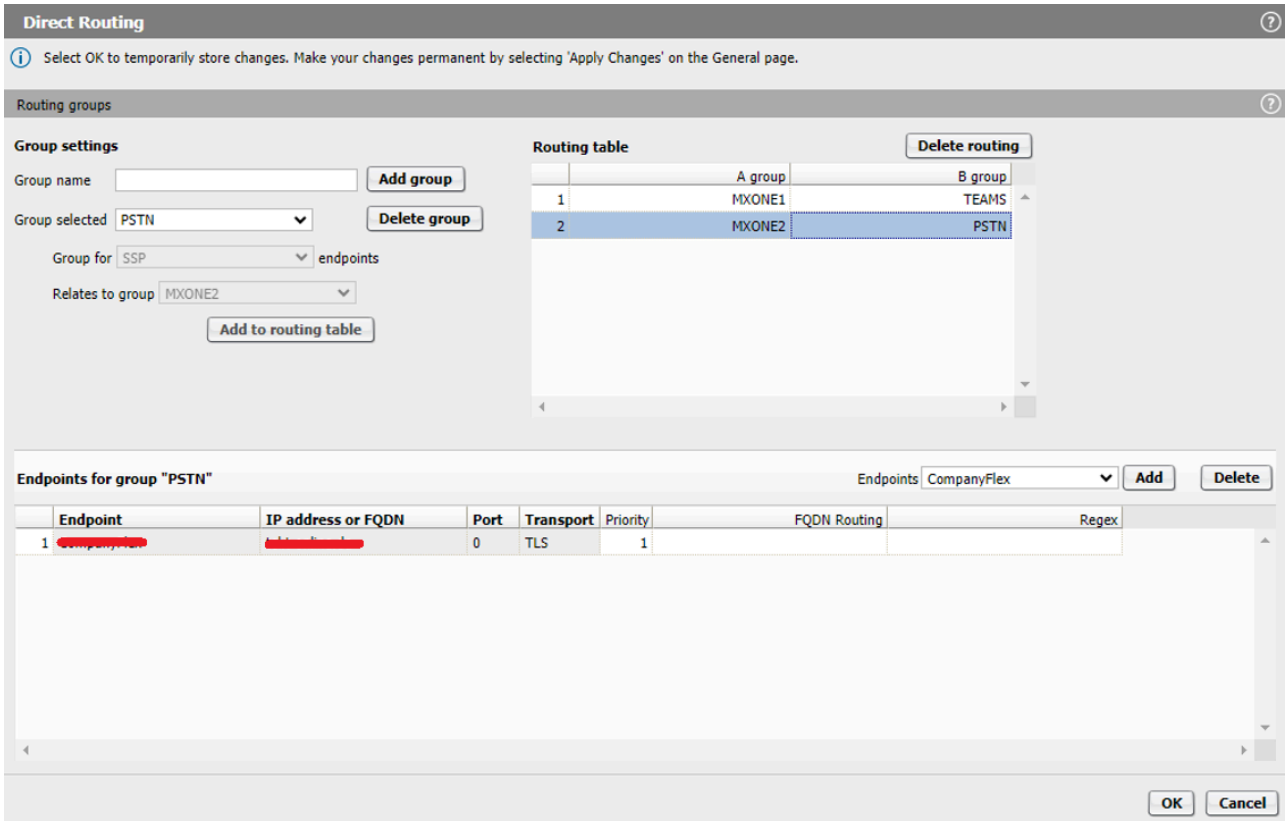


Figure 66: Direct Routing Configuration (PSTN)

d. Create **TEAMS** group and configure the endpoints:

i. On **Group settings**, configure **Group name** as **TEAMS**.
ii. Click on **Add group**. The **Group selected** automatically configured as **TEAMS**.
iii. Select **Group for** as **MS Teams** endpoints.
iv. On **Endpoints for group "TEAMS"** do the following:

a) On **Endpoints** select **Teams_SP1** and click on **Add**.
b) On **Endpoints** select **Teams_SP2** and click on **Add**.
c) On **Endpoints** select **Teams_SP3** and click on **Add**.

The following figure depicts the sample **TEAMS** endpoints configuration.

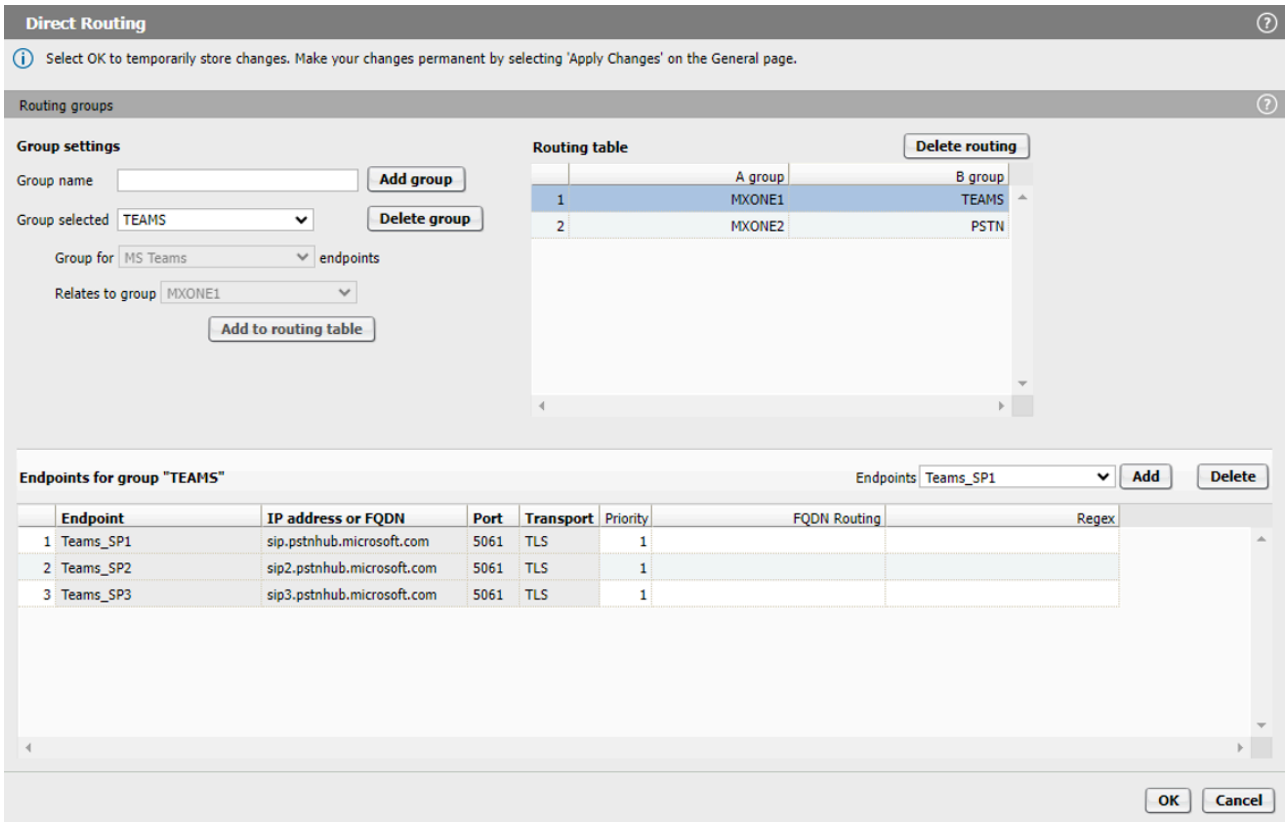


Figure 67: Direct Routing Configuration (TEAMS)

5. Link the groups.

a. Link **MXONE1** to **TEAMS**:

i. On **Group settings**, select **Group selected** as **MXONE1**.

ii. Select **Relates to group** as **TEAMS**.

iii. Click on **Add to routing table**. The entry is displayed on the **Routing table** window as depicted in the following figure.

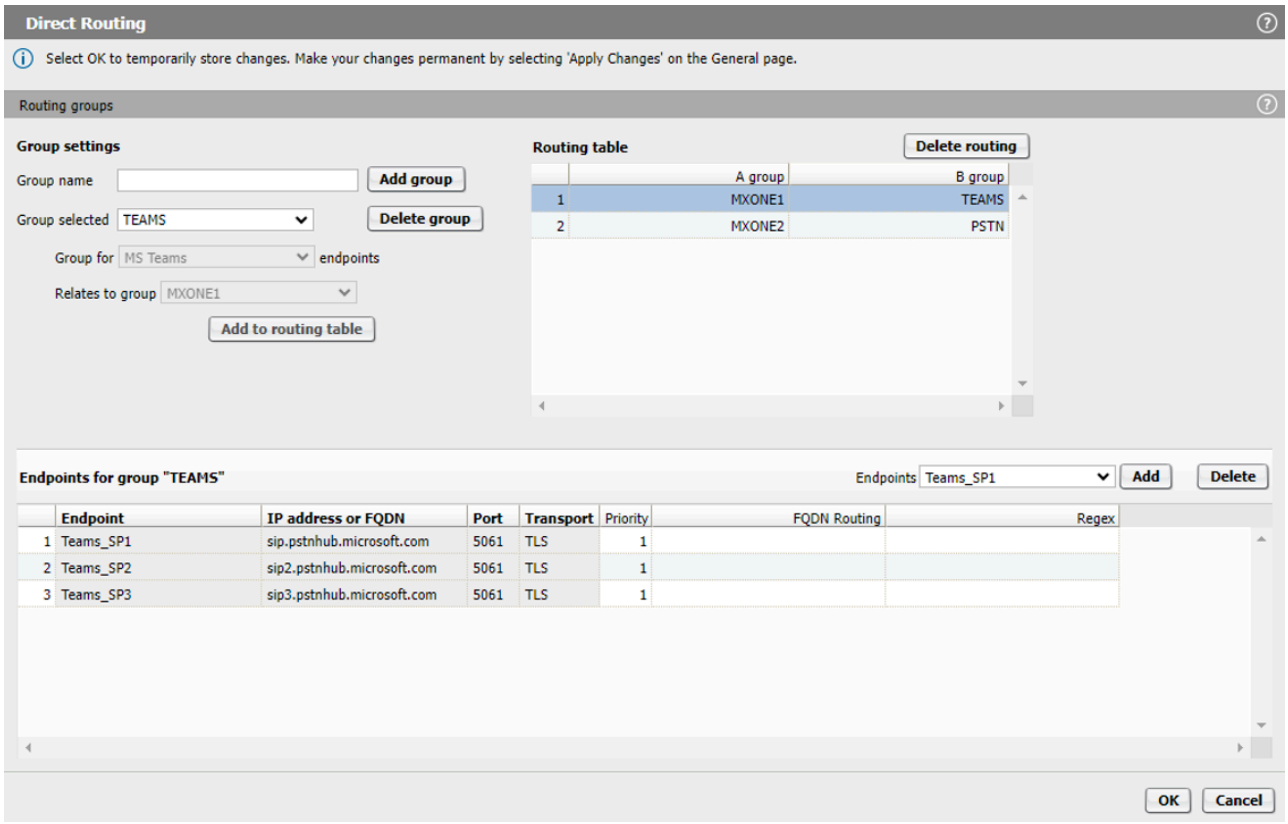


Figure 68: Direct Routing Configuration (MX-ONE to TEAMS)

b. Link **MXONE2** to **PSTN**:

Important:
This step is not required if the MBG is used for the SSP connection.

i. On **Group settings**, select **Group selected** as **MXONE2**.
ii. Select **Relates to group** as **PSTN**.
iii. Click on **Add to routing table**. The entry is displayed on the **Routing table** window as depicted in the following figure.

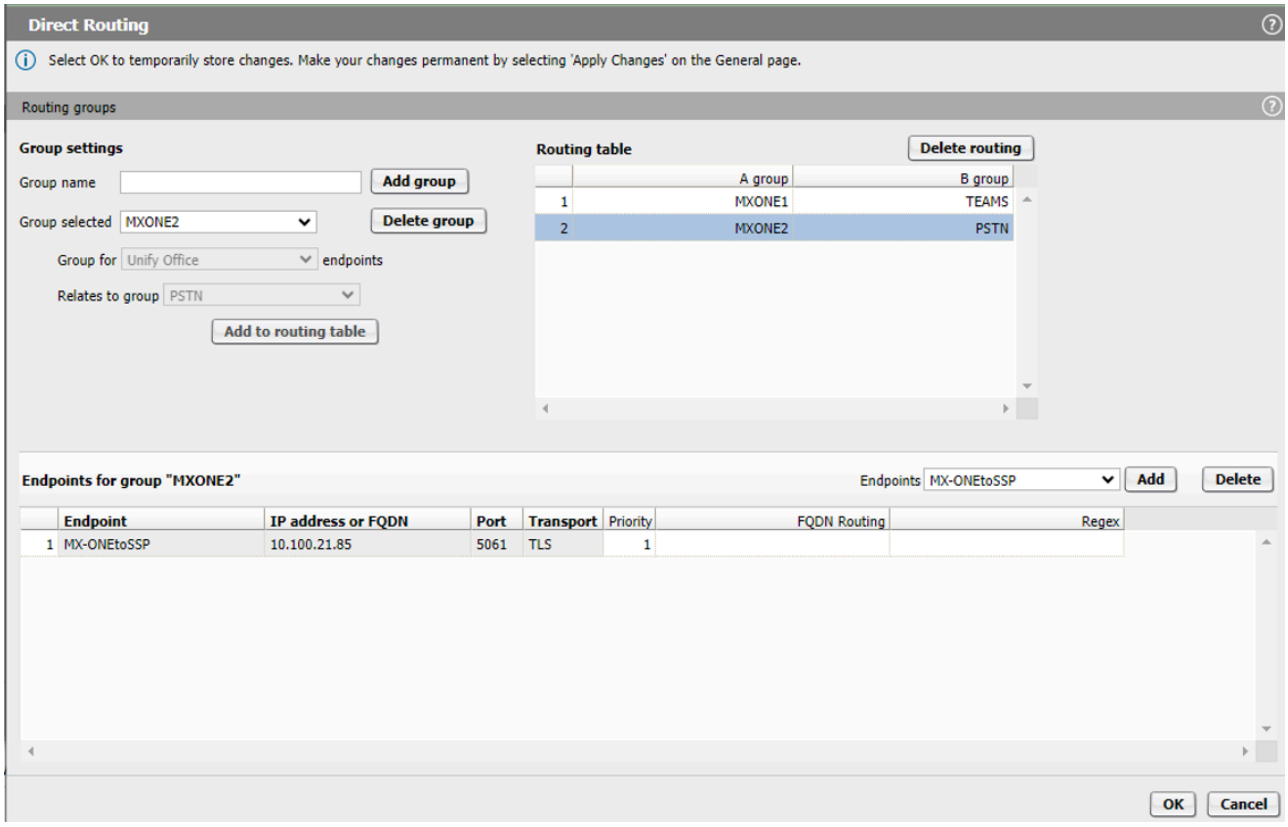


Figure 69: Direct Routing Configuration (MXONE2 to PSTN)

6. Click **OK** and then click **Apply Changes** to save the direct routing configuration.

Configuring Microsoft Teams 7

This chapter contains the following sections:

This section outlines the configuration steps that need to be performed on the Microsoft Teams as part of this solution. Most of the actions detailed in this section must be carried out using the Microsoft Teams admin web center.

Note:

Mitel recommends you to refer to the latest *Microsoft Teams Administration documentation* for the most recent or up-to-date instructions on configuring Microsoft Teams as a part of this solution. The specific procedures outlined in this section must be executed within the Microsoft Teams admin center. The sequence of steps might vary depending on the updates made by Microsoft to the Microsoft Teams application.

Prerequisite

Before you begin, ensure that you have a valid Microsoft Teams admin account. Additionally, ensure that you have created the tenant account, added the users and the domain that will be used for the OpenScape SBC, that is, sbc**@domain.com**. Without a valid Microsoft Teams admin account, the users cannot configure the Microsoft Teams Admin center.

7.1 Connecting OpenScape SBC to Direct Routing

Use the OpenScape SBC FQDN with the domain name that matches the Azure domain name to create an entry for OpenScape SBC:

1. In the Microsoft Teams admin center, navigate to **Voice > Direct Routing > SBCs**.
2. Configure the **SBCs** as follows. The following table lists the sample configuration.

Note:

For other parameters use the default value in the system, for more information, refer to the Connect your Session Border Controller (SBC) to Direct Routing.

Table 5: Destination Configuration

Parameter	Sample Value
Enabled	Turn **On**
SIP signaling port	5061 This value must be same as the Microsoft Teams value (eth) configured in .(see Configuring Network/Net Services on page 42)
Send SIP options	Turn **Off**
Forward call history	Turn **On**
Forward P-Asserted-Identity (PAI) header	Turn **On**
Media bypass	Environment specific value. For information on deployment options, see Deployment Scenarios on page 5.
Bypass mode	Always

3. Click **OK** to save the configuration.

7.2 Verifying SSP Connectivity Status

To verify the SSP connectivity status in OpenScape SBC:

1. In the SBC management portal, navigate to **Administration > System Status**.
2. On **SSP Status**, click **Show**. The **SSP connectivity Status** pop-up window is displayed.

3. Ensure that the **SSP Trunk Names** (MX-ONE, Microsoft Teams, and PSTN) are displayed and the **Status** is shown in green as depicted in the following figure.

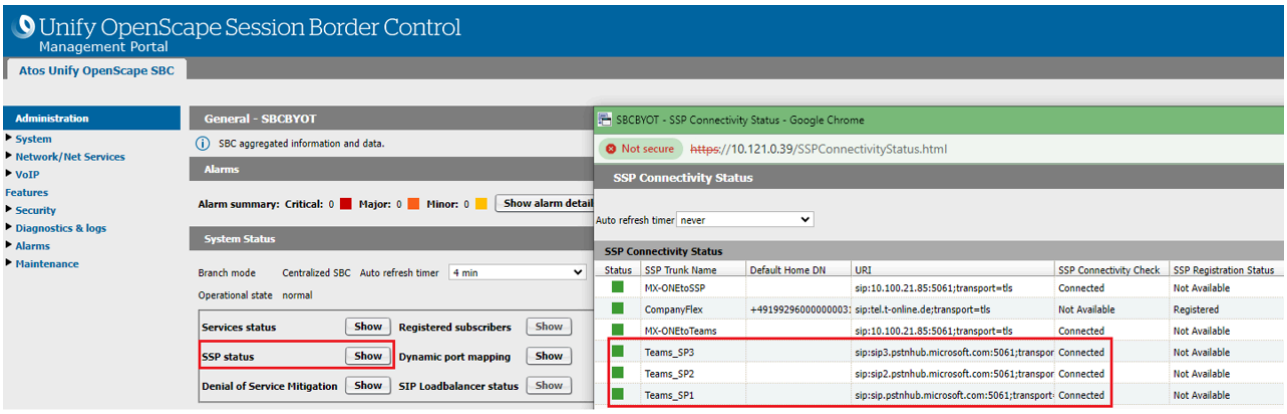


Figure 70: SSP Connectivity Status

7.3 Assigning a PSTN Number to the User

To assign a PSTN number to the user:

1. In the Microsoft Teams admin center, navigate to **Users** > **Manage Users**.
2. In the **Manage Users** page, select the user to update.
3. Navigate to **Account** > **General Information**, and click **Edit**.
4. In the **Phone number** type, select the **Choose the type of phone number** option from the drop-down list.
5. In the **Assigned phone number** field, enter the Direct Routing number you want to assign to the user. For example, 17025551212.

> **Note**:
>
> Do not make any changes in the **Phone Number Extension** field.

6. Click **Apply** to assign a PSTN number.

7.4 Configuring Direct Routing

To configure the direct routing, the entry for OpenScape SBC is created by default based on the certificates generated and imported into OpenScape SBC.For more information, see Configuring Certificates.

Note:
Microsoft Teams uses global proxies and rotates regions for inbound signaling traffic to on-premises systems. For more information, refer to the official Microsoft Teams documentation on Direct Routing.

1. In the **Microsoft Teams admin center**, navigate to **Voice > Direct Routing**.
2. Click on **SBCs**. The SBCs entries are displayed.
3. Click **Add** to create a direct routing configuration. The following table lists the sample configuration.

Table 6: Direct Routing Configuration

Parameter	Sample Value
SBC settings	
Add an FQDN for the SBC	The FQDN must be the FQDN address identifying the network domain for Microsoft Teams that you provided in the **SIP service address** field in Microsoft Teams SIP Service Provider Profile configuration.
Enabled	Turn **On**
SIP signaling port	5061 This value must be same as the Microsoft Teams value (eth) configured in section Configuring Network/Net Services on page 42.
Forward call history	Turn **On**
Forward P-Asserted-Identity (PAI) header	Turn **On**
Concurrent call capacity	The default value is 24
Failover response codes	The default values are 408, 503, 504
Failover time (seconds)	The default value is 10

Parameter	Sample Value
Location based routing and media optimization	
Media bypass	Environment specific value. For information on deployment options, see Deployment Scenarios on page 5.
Bypass mode	Always
Preferred country or region for media traffic	Auto
Location based routing	Off
Gateway site ID	None
Proxy SBC	None

4. Click **Save** to save the direct routing configuration.

Note:
For more information on direct routing configuration, see Configure Direct Routing.

7.5 Configuring Voice Routes

Add and associate a voice route with the OpenScape SBC established in Configuring Direct Routing on page 101. Additionally, create a Dial number pattern for this voice route to facilitate a communication within the Microsoft Teams environment.

To configure voice routes:

1. In the **Microsoft Teams admin center**, navigate to **Voice > Direct Routing**.
2. Select **Voice routes**.

3. Click **Add**. The following table lists a sample configuration:

Table 7: Voice Routes Configuration

Parameter	Sample Value
Add a name for your voice route	Enter a name for your voice route..
Description	Enter the name and description for the voice route.
Priority	Enter the priority of the voice route based on the number of voice routes.
Dialed number pattern	Enter the dialed number pattern of the voice route. For example, ^(\+30[0-9]{10})$.
SBCs enrolled • Click **Add SBCs** to add an SBC. Select the SBC you want to add and click **Apply**. • Click **Edit SBCs** to edit the SBC information, and click **Apply**.	
PSTN usage records a. Click **Add PSTN usage** to add the PSTN records. b. Click **+Add**. c. Enter the PSTN usage record. For example, MitelAth1. d. Select the PSTN usage record that you created. e. Click **Save and apply**.	

4. Click **Save** to save the voice route configuration.

Note:
For more information on voice routes configuration, see Configure call routing for Direct Routing.

7.6 Configuring Voice Routing Policies

Note:

The voice routing policies are associated with the MS Team users, so the calls are routed to OpenScape SBC.

To configure voice routing policy:

1. In the **Microsoft Teams admin center**, navigate to **Voice > Voice routing policies**. The voice routing policies are displayed.
2. In **Manage policies**, click **Add** to create a new voice routing policy.
3. Enter a name in the **Add a name for your voice routing policy** field.
4. In **PSTN usage records**, click **Add or remove** to assign the PSTN usage record previously created in Configuring Voice Routes.
5. Click **Save** to save the routing policy configuration.

Note:

For more information on voice routing policy configuration, see Configure call routing for Direct Routing.

7.7 Configuring User's Voice Routing Policy

To configure Microsoft Teams user voice routing policy:

1. In the **Microsoft Teams admin center**, navigate to **Users > Manage users**.
2. Select the user to configure the voice routing policy.
3. Click the **Policies** tab. The policy entries are displayed.
4. Select the policy and click on **Edit**.
5. From the **Voice routing policy** drop-down list, select the voice policy created in Configuring Voice Routing Policies on page 104.
6. Click **Apply** to assign the voice routing policy to the Microsoft Teams user.

Note:

For more information about configuring users' voice routing policies, see Configure call routing for Direct Routing.

Configuring an E911 Solution 8

This chapter contains the following sections:

This chapter provides information on the necessary configurations to ensure that the E911 solution can successfully determine the physical location of a registered user during an emergency call. Once the exact location is identified, the E911 solution routes the E911 call to the appropriate Public Safety Answering Point (PSAP) and notifies security personnel.

E911 Solutions must comply with E911 legislation. The Federal Communications Commission (FCC) developed Kari's Law and the RAY BAUM's Act, which comprise a set of rules and regulations that specify direct dialing, notification, and dispatchable location minimum requirements for all Multi-line Telephone System (MLTS) platforms. All organizations across the US must comply with both Kari's Law and the RAY BAUM's Act.

MiVoice MX-ONE, as a Multi-line Telephone System (MLTS), implements Section 506 of RAY BAUM Act and Kari´s Law support in conjunction with third-party Next Generation of 911 emergency services providers in the USA.

For MiVoice MX-ONE, we have the following device categories:

- Fixed MLTS Devices. For example, TDM devices (Analog Devices, Digital Devices, and Integrated DECT).
- Non-Fixed MLTS devices. For example, IP Devices, SIP Devices, softphones, all teleworkers, and so on.

To fully support the requirements above, MiVoice MX-ONE is integrated with Intrado in USA and with Redsky in USA and Canada. A valid service agreement with either RedSky or Intrado is necessary for the E911 Solution.

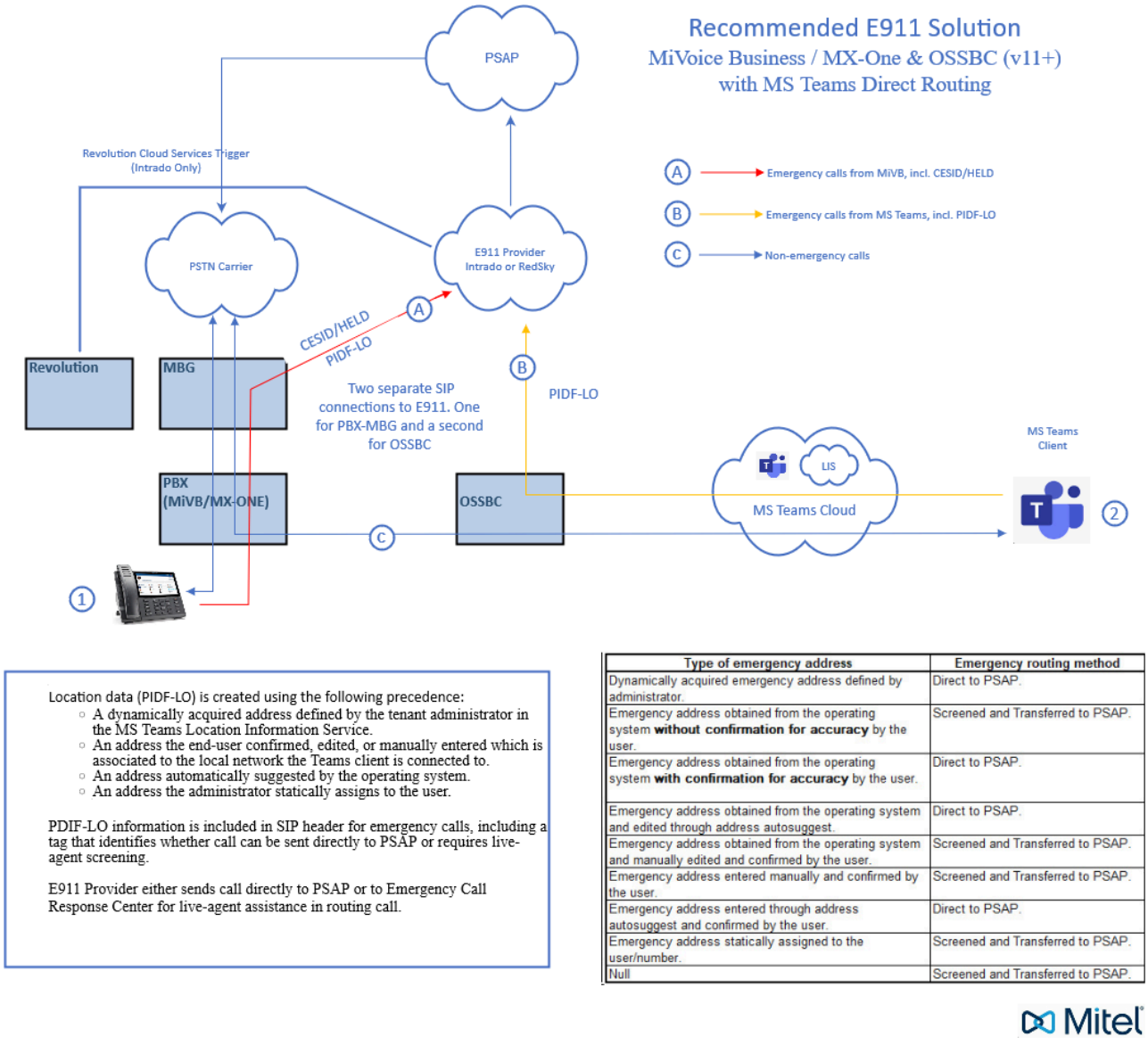
Note:
Mitel does not provide this service agreement directly. To support local notifications compliant with Kari's law compliant, the solution will use the E911 Provider's notification application.

RedSky and Intrado use SIP trunks to route E911 calls to the appropriate Public Safety Answering Points (PSAPs) based on the civic address. Both providers pass callback information from the call-server to enable the PSTN to route the call back from the PSAP to the specified callback number.

Note:
Intrado also offers a function called Extension bind for non-DID numbers. This function, when enabled, assigns a temporary valid Direct Inward Dialing (DID) callback number for the extension number (non 10-digits number) that made the 911 call. In this case, if the call gets disconnected the Emergency Response Team can call back the person that called the Emergency Service.

The diagram below presents the high-level architecture of the E911 Solution with MiVoice MX-ONE and OpenScape SBC with Microsoft Teams.

An emergency call initiated from Microsoft Teams utilizes components such as Presence Information Data Format - Location Object (PIDF-LO) headers.These components encapsulate location data of a device or user in a standardized format, ensuring that emergency services can accurately locate and respond to calls. The specific usage of these components in Microsoft Teams' E911 implementation may vary based on deployment and integration requirements. Subsequently, the OpenScape SBC processes the call and routes it to the E911 provider. This ensures that emergency calls are routed correctly and that the relevant location information is conveyed effectively to emergency responders.



Type of emergency address	Emergency routing method
Dynamically acquired emergency address defined by administrator.	Direct to PSAP.
Emergency address obtained from the operating system **without confirmation for accuracy** by the user.	Screened and Transferred to PSAP.
Emergency address obtained from the operating system **with confirmation for accuracy** by the user.	Direct to PSAP.
Emergency address obtained from the operating system and edited through address autosuggest.	Direct to PSAP.
Emergency address obtained from the operating system and manually edited and confirmed by the user.	Screened and Transferred to PSAP.
Emergency address entered manually and confirmed by the user.	Screened and Transferred to PSAP.
Emergency address entered through address autosuggest and confirmed by the user.	Direct to PSAP.
Emergency address statically assigned to the user/number.	Screened and Transferred to PSAP.
Null	Screened and Transferred to PSAP.

Figure 71: E911 Solution

To complete the OSSBC configurations required for an E911 Solution, follow the instructions provided in the following chapters. For the required Microsoft Teams changes, refer to the official Microsoft Teams documentation for Emergency Calling. For more information on the E911 Solutions and specific deployments with either Intrado or Redsky, please refer to Related Documentation.

8.1 Configuring an E911 Media Profile

Follow the steps below to create a new media profile for your E911 Provider.

Note:
This configuration applies to both single-arm and multi-arm deployments. For more information, refer to Deployment Scenarios on page 5.

To configure the media profile:

1. In the SBC local management portal, navigate to **VoIP** > **Media** in the navigation tree under Administration.
2. Under **Media Profiles**, click **Add**.

   The **Media Profiles** window pops up.
3. Under **General**, configure the following:

Field	Description
Name	Enter an E911 Media Profile name. For example, Intra do.
Media protocol	Select **RTP only** from the drop-down list. **Note**: The **Media Protocol** is specified by your E911 Provider. To ensure compliance with their requirements, please contact your E911 Provider's support.

4. If codec configuration is required by your E911 Provider, do the following:

Important:
In some cases, codec configuration from an E911 provider (such as Redsky) is necessary to align technical specifications and ensure that emergency calls can be handled efficiently within the organization's communication infrastructure.

a. Locate the **Codec Configuration** area.
b. Check the **Enforce codec priority in profile** checkbox.
c. From the **Codec** drop-down menu, select the codec as specified by your E911 Provider, according to the region where they are located. For example, select G711U 8kHz - 64 kbps (for US-NA) or G711A 8kHz - 64 kbps (for Europe).
d. Click **Add**.

5. Click **OK** to save the configuration.
6. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

8.2 Configuring Remote Endpoints for E911

An endpoint refers to a remote computing device engaged in bidirectional communication with a connected network. In both single-arm and multi-arm deployment scenarios, you need to first create SIP Service Provider Profiles (SSPs) and then proceed with setting up the remote endpoints configuration settings.

8.2.1 Prerequisite

Ensure that the **Standalone with internal SIP Stack** option is selected from the **Comm System Type** drop-down menu, under VoIP > SIP Server Settings.

8.2.2 E911 SIP Service Provider Profile Configuration

The following configuration must be applied to the E911 Remote Endpoint Profile to handle Microsoft Teams > E911 calls.

1. In the SBC local management portal, navigate to **Features** in the navigation tree under **Administration**.

   The **Features** window pops up. The features are displayed under the **Features configuration** area.
2. Check the **Enable Remote Endpoints** checkbox.
3. Click **Configure** next to the **Enable Remote Endpoints** checkbox.

   The **Remote endpoints** window pops up.
4. Under the **SIP Service Provider Profile** area, click **Add**.

   The **SIP Service Provider Profiles** window pops up.
5. In the **Name** field, enter the name of your E911 Provider. For example, Intrado.
6. Click **OK** to save the configuration.
7. Click **OK**.

8. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

8.2.3 Microsoft Teams SIP Service Provider Profile Configuration for E911

Follow the steps below to configure the Microsoft Teams SIP Service Provider Profile settings.

1. In the SBC local management portal, navigate to **Features** in the navigation tree under **Administration**.

   The **Features** window pops up. The features are displayed under the **Features configuration** area.
2. Check the **Enable Remote Endpoints** checkbox.
3. Click **Configure** next to the Enable Remote Endpoints checkbox.

   The **Remote endpoints** window pops up.
4. Under the SIP Service Provider Profiles area, click **Add**.

   The SIP Service Provider Profile window pops up.
5. Locate the **General** area.
6. In the **Name** field, enter a name for the Microsoft Teams SIP Service Provider Profile. For example, **Teams911**.
7. From the **Default SSP Profile** drop-down menu, select **MSTeams.**

   Ensure that the following checkboxes are automatically selected under the **SIP Service Address** area:

   - **Use SIP Service Address in From header**
   - **Use SIP Service Address in P-Asserted-Identity header**
   - **Use SIP Service Address in Diversion header**
   - **Use SIP Service Address in Contact header**
   - **Use SIP Service Address in Via header**
8. In the **SIP service address** field, enter the FQDN address identifying the network domain for Microsoft Teams.

> **Note**:
> The FQDN address you add here must be the same that you add in Microsoft teams. For more information, see Configuring Direct Routing on page 91.

9. Locate the **Incoming SIP manipulation** area.

   a. From the **SIP User info header** drop-down menu, select **From and P-Asserted-identity headers**.
   b. In the **Regex** field, add a regex to remove the country code received from Microsoft Teams:

   /^\+1(.*)$/\1/

Important:
This regex is removing the country code +1. For example, if you get the +1987654321 number, that rule removes the +1 and sends to the E911 Provider the number 987654321. Replace the country code to match the country code of your area.

10. Locate the **Flags** area and disable the **Preserve To and From headers per RFC2543** flag.
11. Click **OK** to save the configuration.
12. Click **OK**.
13. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

8.2.4 E911 Remote Endpoint Configuration

Follow the steps below to configure an E911 Provider remote endpoint.

Prerequisite: You have created an E911 SIP Service Provider Profile.

1. In the SBC local management portal, navigate to **Features** in the navigation tree under **Administration**.

   The **Features** window pops up.
2. Check the **Enable Remote Endpoints** checkbox.
3. Click **Configure** next to the Enable Remote Endpoints **checkbox**.

   The **Remote Endpoints** window pops up.
4. Scroll down to locate the **Remote endpoint configuration** area.
5. Click **Add**.

   The **Remote Endpoint configuration** window pops up.
6. Under the **Remote Endpoint Settings** area, configure the following:

Important:
For this configuration, it is assumed that a public IP address is already in place for the connection between MBG and the E911 Provider (see **point A** in the E911 Solution diagram on Configuring an E911 Solution on page 106). Therefore, the configuration described below requires providing a separate public Firewall IP to connect OSSBC to your E911 provider (please refer to **point B** in the E911 Solution diagram on Configuring an E911 Solution on page 106), which must be whitelisted (see note below).

Menu item	Action
Name	Enter a unique name for the E911 Provider remote endpoint. For example, Intrado.

Menu item	Action
Profile	From the drop-down list, select the E911 SIP Service Provider Profile you created in E911 SIP Service Provider Profile Configuration on page 109
Access realm profile	From the drop-down list, select the network ID that has access to Internet. For example, **Main-access-Realm**. **Important**: For security purposes, IP whitelisting is used by E911 Providers to block network access to all IPs except those in the whitelist. To ensure the public Firewall IP you are using will be whitelisted, share it with your E911 Provider.
Core realm profile	From the drop-down list, select the core realm profile. For example, **Main-core-realm-ipv4.**

7. Under the **Remote Location domain list** area, click **Add.**

The **Remote Location Domain** window pops up.

a. Under **General**, configure the following:

Note:
The settings presented below are provided by your E911 Provider.

Menu item	Action	Notes
Remote URL	Enter the URL of the remote endpoint for E911.	The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name).

Menu item	Action	Notes
Remote port	Enter the remote port for communication between E911 and OSSBC.	
Remote transport	From the **Remote transport** drop-down menu, select the remote transport protocol provided by your E911 Provider (TCP, UDP, or TLS).	

b. Locate the **Media Configuration** area.
c. From the **Media Profile** drop-down menu, select the Media profile of your E911 Provider created in Configuring an E911 Media Profile on page 108.
d. Click **OK**.

You are directed back to the **Remote Endpoint Configuration** window.

8. Locate the **Remote Location Identification Routing** area.

   a. In the **Core realm** port, enter a unique value.
9. Click **OK**.

   You are directed back to the **Remote Endpoints** window. The E911 Provider Remote endpoint is shown under the **Remote endpoint configuration** table.
10. Click **OK**.
11. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

8.2.5 Microsoft Teams Remote Endpoint Configuration for E911

Follow the steps below to configure three Microsoft Teams remote endpoints.

Prerequisite: You have created a Microsoft Teams SIP Service Provider Profile.

1. In the SBC local management portal, navigate to **Features** in the navigation tree under **Administration**.

   The **Features** window appears with the list of features under the **Features configuration** tab.
2. Check the **Enable Remote Endpoints** checkbox.
3. Click **Configure**.

   The **Remote Endpoints** window pops up.
4. Scroll down to locate the **Remote endpoint configuration** area.

5. Click **Add**.

   The **Remote Endpoint configuration** window pops up.
6. Under the **Remote Endpoint Settings** area, configure the following:

Menu item	Action
Name	Enter a unique name for the remote endpoint. For example, Teams_Emergency.
Profile	From the drop-down list, select the Microsoft Teams profile. For example, Teams911.
Access realm profile	From the drop-down list, select the Network ID that has access to the internet. For example, **Main-access-Realm.**
Core realm profile	From the drop-down list, select **Main-Core-Realm-ipv4**.

7. Under the **Remote Location domain list** area, click **Add.**

   The **Remote Location Domain** window pops up.
8. Under **General**, do the following:

Note:
The settings presented below are provided by Microsoft Teams.

Menu item	Action	Notes
Remote URL	Enter the URL of the remote endpoint or domain: **sip.pstnhub.microsoft.com**	The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name).
Remote port	Enter the remote endpoint SIP port. For example, 5061.	
Remote transport	From the drop-down list, select **TLS**.	

9. Locate the **TLS** area and configure the following:

   a. From the **TLS mode** drop-down menu, select **Mutual authentication**.
   b. From the **Certificate profile** field, select the TLS certificate profile for teams, created in Configuring Certificates on page 64. For example,Teams.
10. Locate the **Media Configuration** area.
11. From the **Media profile** drop-down menu, select the media profile for Microsoft Teams, created in Configuring Media Profiles on page 54. For example, Teams.
12. Click **OK**.

    You are directed back to **Remote Endpoint configuration** window.
13. Locate the **Remote Location Identification/Routing** area.

    a. In the **Core realm port** field, enter a port value within the system-wide static port range. Ensure that both the Core Realm IP address and Core Realm Port are unique for each remote endpoint. For example, 51104.
    b. In the **Incoming Routing prefix** field, enter the 3-digit emergency call number that the user will dial from the Microsoft Teams. For example, 911.
    c. Click **Add**.
14. Click **OK**.
15. Repeat **steps 6-14** to add two more Microsoft Teams remote endpoints:

    - sip2.pstnhub.microsoft.com
    - sip3.pstnhub.microsoft.com
16. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

8.3 Configuring SIP Server Settings for E911

When in **Standalone with Internal SIP Stack** mode, you must create a routing table to interconnect the remote endpoints configured in OpenScape SBC. It is required to configure a direct routing group for communication between your E911 Provider and Microsoft Teams.

To accomplish this, you must create one group for your E911 Provider and another for Microsoft Teams, and then relate them together.

Note:
This configuration applies to both single-arm and multi-arm deployment scenarios. For more information, refer to Deployment Scenarios on page 5.

1. In the SBC local management portal, navigate to **VoIP** > **SIP Server Settings** in the navigation tree under Administration.
2. Ensure that **Standalone with internal SIP Stack** is selected in the **Comm System Type** drop-down menu.

Important:
For the OpenScape SBC V11R0.6.0, when you select **Standalone with internal SIP stack**, you must set the SIP-TCP and SIP-TLS ports in the core realm configuration to **0**. For more information, refer to Configuring Network/Net Services on page 42.

3. Under **Direct Routing Configuration**, click **Configure**.

   The **Direct Routing** window pops up.
4. Create the Microsoft Teams Group:

   a. In the **Group name** field, enter the group name for Microsoft Teams. For example, Teams_911.
   b. Click **Add group**.

      The group name you created is displayed in the **Group selected** field.
   c. From the **Group for** drop-down menu, select **MS Teams**.
   d. Locate the **Endpoints for Group '[Group name]'** area.
   e. From the **Endpoints** drop-down menu on the right side, select the Microsoft Teams endpoint(s) created in Microsoft Teams Remote Endpoint Configuration for E911 on page 113 and click **Add** for all the remote Endpoints configured for MS Teams Emergency (3 in total).
   f. Create the E911 Group:

      i. In the **Group name** field, enter the group name for your E911 Provider. For example, Intrado.
      ii. Click **Add group**.

         The group name you created is displayed in the **Group selected** field.
      iii. From the **Group for** drop-down menu, select **SSP**.
      iv. Locate the **Endpoints for Group '[Group name]'** area, as depicted in the following figure.
      v. From the **Endpoints** drop-down on the right, select the E911 Provider group and click **Add**. For our example, select **Intrado.**
5. Relate the E911 group to the Microsoft Teams group:

   a. From the **Relates to Group** drop-down menu, select the Microsoft Teams group, such as **Teams_911**.
   b. Click **Add to routing table**.

      The endpoint is added to the Routing table.
   c. Double-click on the E911 group (for example, Intrado) and add **911** as regex.
   d. Optional: To modify the details of a routing group, such as changing the priority or adding a regex, simply double-click on the entry under the **Routing table** you wish to modify.
6. Click **OK**.
7. Click **OK** to save the configuration.

8. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

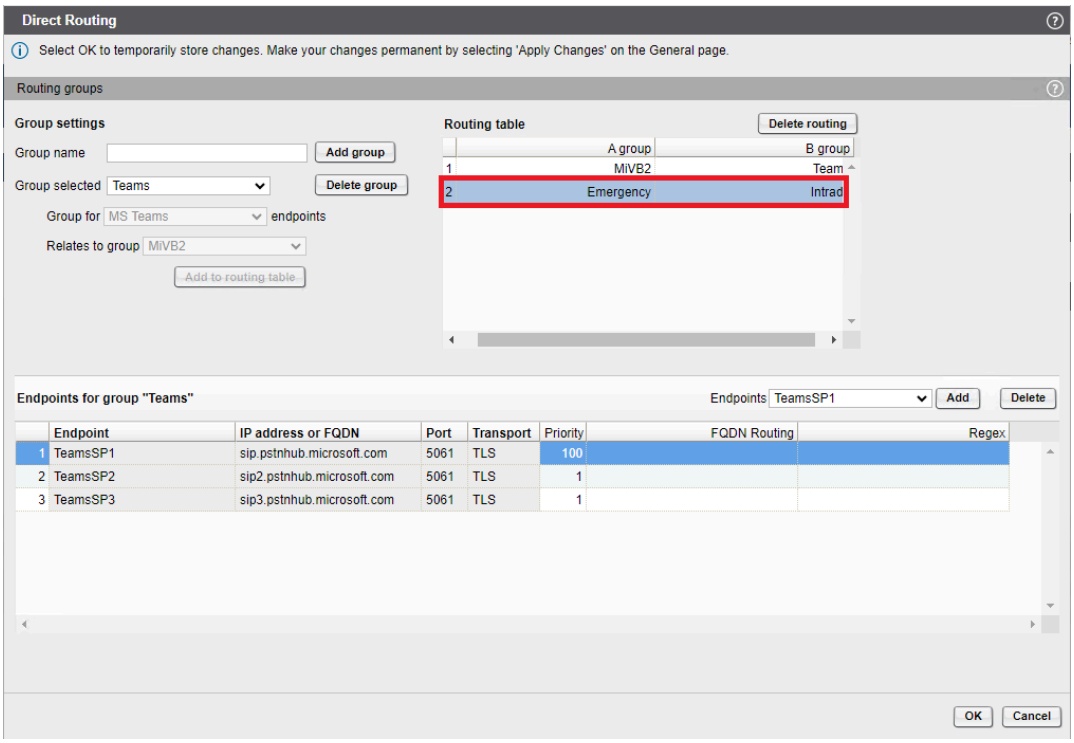


Figure 72: E911 Direct Routing

Appendix A: Restrictions and Known Issues 9

The following table lists the tested features when Microsoft Teams is integrated with MiVoice MX-ONE through OpenScape SBC.

Feature	Description	Test Result
Basic Call	Making and receiving calls through OS SBC between MiVB, MS Teams and the PSTN. Features tested were, busy calls, reject calls, not answered, call cancellation and call to unavailable.	Minor issues found
Basic Call Extended	This feature covers basic telephony features such as call history, long duration, do not disturb, number presentation, private calling, and call mute.	No issues found
Telephony Extended	This feature covers comprehensive telephony capabilities such as hold, consultation calls, call transfers, call waiting, simultaneous ringing, call parking, hunt groups, various transfer and forwarding options, voicemail, and conference.	No issues found
Audio	This feature covers Audio Codecs and DTMF.	No issues found

The following table lists the restrictions and known issues when Microsoft Teams is integrated with MiVoice MX-ONE through OpenScape SBC.

Feature	Issue Description
Hold	As recommended by Microsoft, "a=inactive" should be used in SDP when PBX sends a re-INVITE to put the call on hold. Therefore, it is not recommended to use Music on Hold in MX-ONE. "RTP Only" is recommended in the SBC default media profile since it is used in the core. It is not recommended to use "SRTP Best Effort" in the SBC default media profile because this may lead to payload issues after hold and retrieval. It is recommended to use the SBC configuration as described in Configuring OpenScape SBC on page 37.

Feature	Issue Description
INVITE without SDP	INVITE without SDP is rejected by Microsoft Teams. It is recommended to use the MX-ONE routing configuration as described in Configuring MX-ONE on page 9.
Call Display	After answering an incoming call from Microsoft Teams on the MX-ONE device, the name of the Microsoft Teams user is not displayed. SBC drops the display name in the P-Asserted-Identity header. As a solution, save the Microsoft Teams number as a contact on the Mitel device. Microsoft Teams will only display the number for external call partners. Microsoft Teams does not use the P-Asserted-Identity header sent by MX-ONE.
Park	Park fails if Microsoft Teams uses REFER. Currently, REFER is not supported by the SBC in Standalone (BYOT) mode. **Note**: Microsoft Teams uses REFER to park a call when Media Bypass is enabled.
Forward	In forward scenarios, the information on calling party display may not be correctly updated or may not contain the redirection information: • Calling party MX-ONE does not receive any information when Microsoft Teams forward or transfer the call to another Microsoft Teams user. • Microsoft Teams ignores the information received in headers and uses only the information received in FROM header.
	Single-arm configuration with multiple network access realm: There is no payload when MX-ONE user calls Microsoft Teams user and the call is forwarded to another MX-ONE user (valid for all types of call forwarding and parallel ringing).

Feature	Issue Description
Transfer	In Transfer scenarios, the information on display may not be correctly updated: • SBC does not forward Referred-By or Replaces headers. • Calling party MX-ONE does not receive any information when Microsoft Teams forward or transfer the call to another Microsoft Teams user. • Microsoft Teams ignores the information received in headers and uses only the information received in FROM header. • Microsoft Teams does not use P-Asserted-Identity header sent by the MX-ONE.
Parallel Ringing	The calling party's display is not updated if the parallel device answers the call.
Delays Microsoft Teams	Occasionally, Microsoft Teams delays from 1 to 2 seconds to connect the audio with MX-ONE or PSTN.
Emergency Calls	In the emergency calls from Microsoft Teams users, the user location information provided by Microsoft is bypassed to the IP PBX in the SIP message inside SDP body for PIDF-LO. The ELIN code inside this message is not copied to the SIP PAI header which may be required by some emergency providers to retrieve the correct user location.
	The emergency calling is not supported when using Microsoft Teams web client. Microsoft Teams desktop application or mobile application could be used instead, based on the following URL for supported clients. For more information, see the official Microsoft Teams page for Emergency calling.
	MiVB and MX-ONE will not receive logs, records, alerts, or notifications from the OS SBC about emergency calls that have been made. This means that the systems will not be informed of the occurrence of an emergency call and will not have any indication that such a call was made.
MiCollab Integration	For Microsoft Teams integration with MX-ONE, the MiCollab features are not validated.

Appendix B: Default User Name and Password

10

The following table lists the default user name and password for the OpenScape SBC system.

User Name	Password
administrator	Asd123!.
root	T@R63dis
service	BF0bpt@x
guest	1clENtk=

For information on OpenScape SBC Security Checklist, refer to OpenScape SBC V11 Security Checklist.

Appendix C: MX-ONE Number Conversion

11

This section describes the sample number conversion used for the SIP trunk calls.

All calls between Microsoft Teams and PSTN are routed through MX-ONE. When calls are made from PSTN to Microsoft Teams (or Microsoft Teams to PSTN), the calls are verified by using the conversion rules. If the match is found, then the call is notified to the respective destination. Appropriate number conversion data needs to be configured to covert numbers sent and received on the SIP route from Microsoft Teams and PSTN to correct format.

Sample Number Conversion

The following figure depicts the sample number conversion made on the MX-ONE system.

```
mxone_admin@MXOne:~> number_conversion_print
Number conversion data:
Entry                   Cnvtyp Numtyp Rou Tardest    Pre                 Trc Newtyp Cont Bcap Hlc
49228422                0      1      1                                  8
49228536                0      1      1                                  8
49615135                0      1      1             000
49897007                0      1      1             000
68                      1      10     1             49228536               1
68                      1      11     1             49228536               1
70                      1      10     1             49228422               1
70                      1      11     1             49228422               1
1                       4      1                    000
2                       4      1                    000
3                       4      1                    000
4                       4      1                    000
5                       4      1                    000
6                       4      1                    000
7                       4      1                    000
8                       4      1                    000
9                       4      1                    000
```

Appendix D: Generating Certificates for MX-ONE in .pem Format

12

Generate certificates in *.pem* format for either of the following scenarios when communication with MX-ONE is configured through TLS protocol:

Note:
The Certificate Signing Request (CSR) in OpenScape SBC must be created according to the Configuring SIP Routing on page 13:

- If sip_route in MX-ONE is configured using the IP address in parameters **-ipproxy** or **-uristring0**, it is expected that the CSR provided by the SBC includes the IP address in common or alternative name. If an IP address is not in the CSR, it will not match what is configured in the SIP trunk, and the error "Certificate name mismatch" is displayed.
- The other configuration option in the MX-ONE SIP trunk is to use the SBC FQDN in **-proxyip** or **-uristring0** parameter instead of the IP address. This FQDN name must be resolvable and configured in a DNS server. In this case, the CSR provided by the SBC should include this FQDN as a Common or Alternative Name.

- Generate .pem file if MX-ONE is CA:

1. Create a Certificate Sign Request (CSR) in OpenScape SBC. For more information, refer to the *Chapter 9* of *OpenScape SBC V11 Configuration Guide, Administration Documentation*.
2. Import the CSR to MX-ONE to generate a *.pem* certificate signed by MX-ONE.
3. Export the *.pem* certificate from MX-ONE.
4. The exported *.pem* file must be imported to OpenScape SBC along with MX-ONE *root.CA* and *key.pem* (generated when CSR is created for OpenScape SBC) files. To import the certificates, see Importing OpenScape SBC Certificates on page 64.

(Or)

- Generate .pem file if third-party is CA:

1. Generate CSR from both MX-ONE and OpenScape SBC.
2. After generating the CSRs, get the approval sign from third party authority.
3. Import the certificates to both MX-ONE and OpenScape SBC. To import the certificates, see Importing OpenScape SBC Certificates on page 64.