A MITEL
PRODUCT
GUIDE

MiVoice Business

Integration with Microsoft Teams Through Unify OpenScape Session Border Controller

Release 10.1
Document Version 1.0

July 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.

®,™ Trademark of Mitel Networks Corporation

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 What's New in this Document..... 1

2 Preface.....2
2.1 About This Document..... 2
2.2 Related Documentation.....2
2.3 Intended Audience..... 3
2.4 Disclaimer.....3

3 About the MiVoice Business - OpenScape SBC - Microsoft Teams Solution.....4
3.1 Overview.....4
3.2 Deployment Scenarios..... 4
3.3 Software Versions..... 7

4 Configuring MiVoice Business..... 8
4.1 Prerequisites.....8
4.2 Configuring Licenses.....9
4.3 Configuring Class of Restriction..... 10
4.4 Configuring Class of Service..... 11
4.5 Configuring the Network Elements..... 12
4.6 Configuring Trunk Attributes..... 14
4.7 Configuring SIP Peer Profile.....15
4.7.1 OpenScape SBC SIP Peer Profile Configuration..... 16
4.7.2 PSTN SIP Peer Profile Configuration..... 17
4.8 Configuring Automatic Route Selection (ARS)..... 18
4.9 Configuring Direct Inward Dialing Service..... 21

5 Installing OpenScape SBC.....23
5.1 Using OVA File.....23
5.1.1 Prerequisite..... 23
5.1.2 Installing OpenScape SBC Using OVA File..... 23
5.1.3 Configuring IP Address.....24
5.1.4 Verifying SBC Software Status..... 26
5.2 Using OVF Files.....27
5.2.1 Prerequisite..... 27
5.2.2 Generating ISO image with USB stick..... 27
5.2.3 Installing SBC Using OVF File..... 29
5.2.4 Verifying SBC Software Status..... 30

6 Configuring OpenScape Session Border Controller..... 31

6.1 Verifying License..... 32
6.2 Configuring Network/Net Services..... 36
6.3 Configuring the Network/Net Services DNS Server..... 40
6.4 Configuring Certificates..... 41
6.5 Configuring the External Firewall..... 43
6.5.1 External Firewall Settings configuration..... 44
6.6 Enabling Codec Support for Transcoding..... 46
6.7 Configuring Media Profiles..... 47
6.8 Configuring Remote Endpoints..... 51
6.8.1 MiVoice Business SIP Service Provider Profile configuration..... 52
6.8.2 Microsoft Teams SIP Service Provider Profile configuration..... 53
6.8.3 MiVoice Business Remote Endpoint configuration..... 54
6.8.4 Microsoft Teams Remote Endpoints configuration..... 56
6.9 Configuring SIP Server settings..... 58
6.10 Configuring Port and Signaling Settings..... 60
6.11 Configuring Error Codes..... 62

7 Configuring Microsoft Teams..... 64

7.1 Configuring Direct Routing..... 64
7.2 Configuring Voice Routes..... 66
7.3 Configuring Voice Routing Policies..... 67
7.4 Assigning a PSTN Number to the User..... 68
7.5 Configuring User's Voice Routing Policy..... 68

8 Appendix A: Restrictions and Known Issues..... 70

9 Appendix B: Default User Name and Password..... 73

What's New in this Document 1

This section summarizes changes in the Microsoft Teams integration with MiVoice Business through OpenScape Session Border Controller (SBC).

Table 1: Document Version 1.0

Feature/Enhancement	Updates	Location	Publish Date
Integration of Microsoft Teams with MiVoice Business through OpenScape SBC.	This is the initial release of the integration of Microsoft Teams with MiVoice Business through OpenScape SBC.	Entire Document	July 2024

Preface 2

This chapter contains the following sections:

- About This Document
- Related Documentation
- Intended Audience
- Disclaimer

This guide outlines the steps required to connect Microsoft Teams with MiVoice Business through OpenScape SBC.

Note:

This document focuses only on the MiVoice Business, 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 Business initial configuration, refer to the MiVoice Business documentation on the Document Center.

2.1 About This Document

This document provides a reference to Mitel Authorized Solutions providers for configuring the MiVoice Business 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 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 MiVoice Business, refer to the following documents:

- MiVoice Business System Administration Tool Help
- MiVoice Business Engineering Guidelines document

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 Business, 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 MiVoice Business - OpenScape SBC - Microsoft Teams Solution 3

This chapter contains the following sections:

- Overview
- Deployment Scenarios
- Software Versions

3.1 Overview

Mitel MiVoice Business 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 130,000 users, MiVoice Business accommodates both single-site deployments and multi-site networks across onsite, private cloud, public cloud, or hybrid environments. Additionally, customers can opt for either capital expenditure or subscription licensing models when acquiring MiVoice Business.

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 MiVoice Business and OpenScape Session Border Controller (SBC) with Microsoft Teams. For information on restrictions and known issues, refer to the Appendix A: Restrictions and Known Issues on page 70.

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

- MiVoice Business Integration with Microsoft Teams Through Unify OpenScape Session Border Controller
- Configuring OpenScape Session Border Controller
- Configuring Microsoft Teams

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.

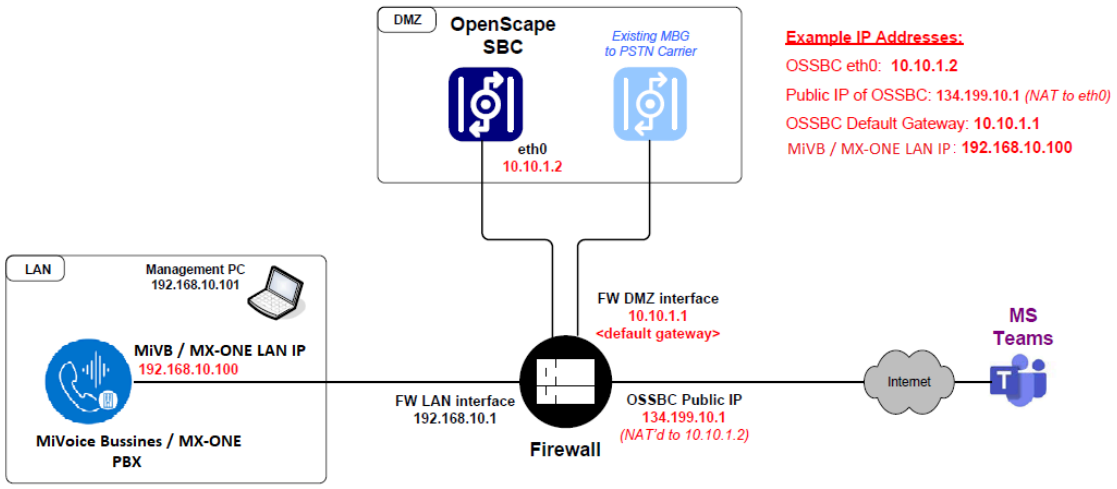


Figure 1: Single-arm Configuration

- **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 6) and **ICE-FULL** for

Firewall NAT mode (see Figure 3: Multiple-arm Configuration - Firewall NAT Mode on page 6) because Microsoft Teams receives the external address of the firewall in the SDP.

The following figures depict the multiple-arm deployment scenarios.

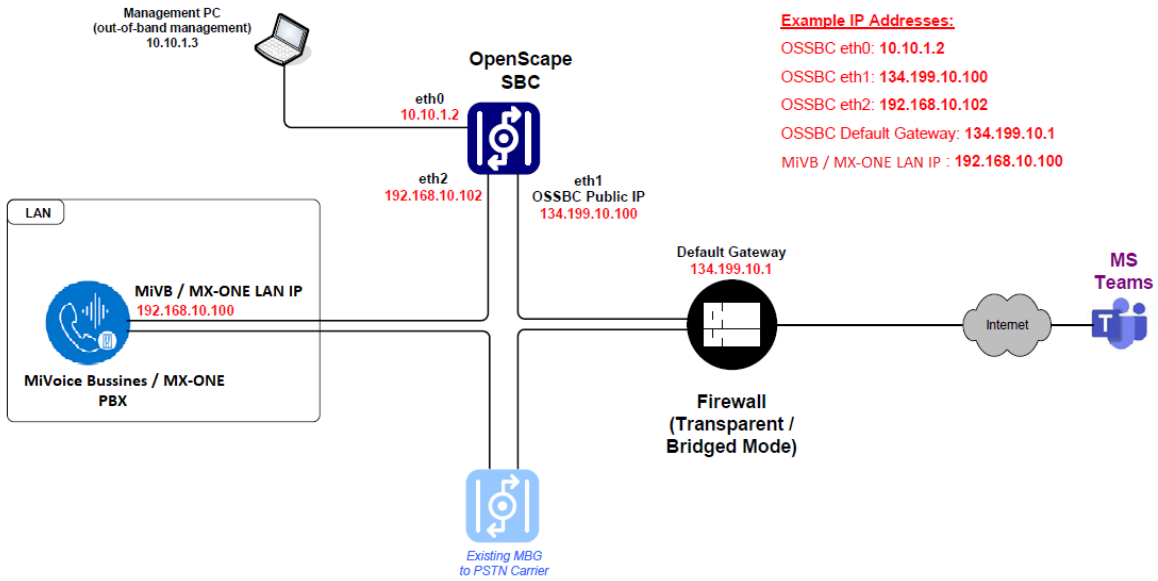


Figure 2: Multiple-arm Configuration - Firewall Bridged Mode

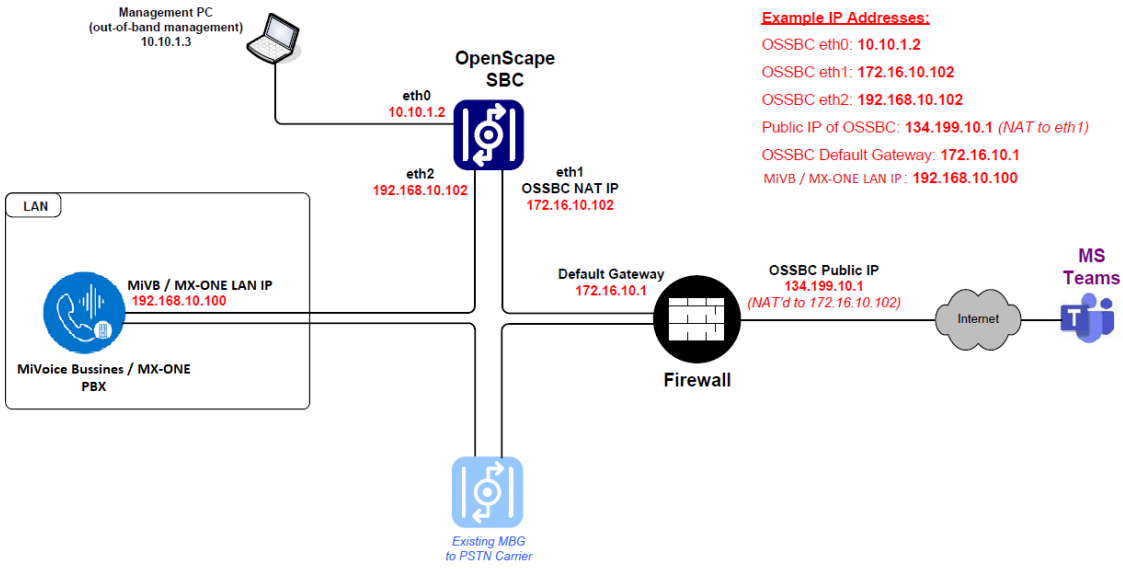


Figure 3: Multiple-arm Configuration - Firewall NAT Mode

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.

Product	Minimum Software Version
MiVoice Business	10.0 SP1 (10.0.1.18) 10.1 (10.1.0.29)
6900/6900W/5300-Series MiNET	02.01.00.037
OpenScape SBC	11.0 (11 R0.05.00)
Microsoft Teams Web Client	V2

Note:

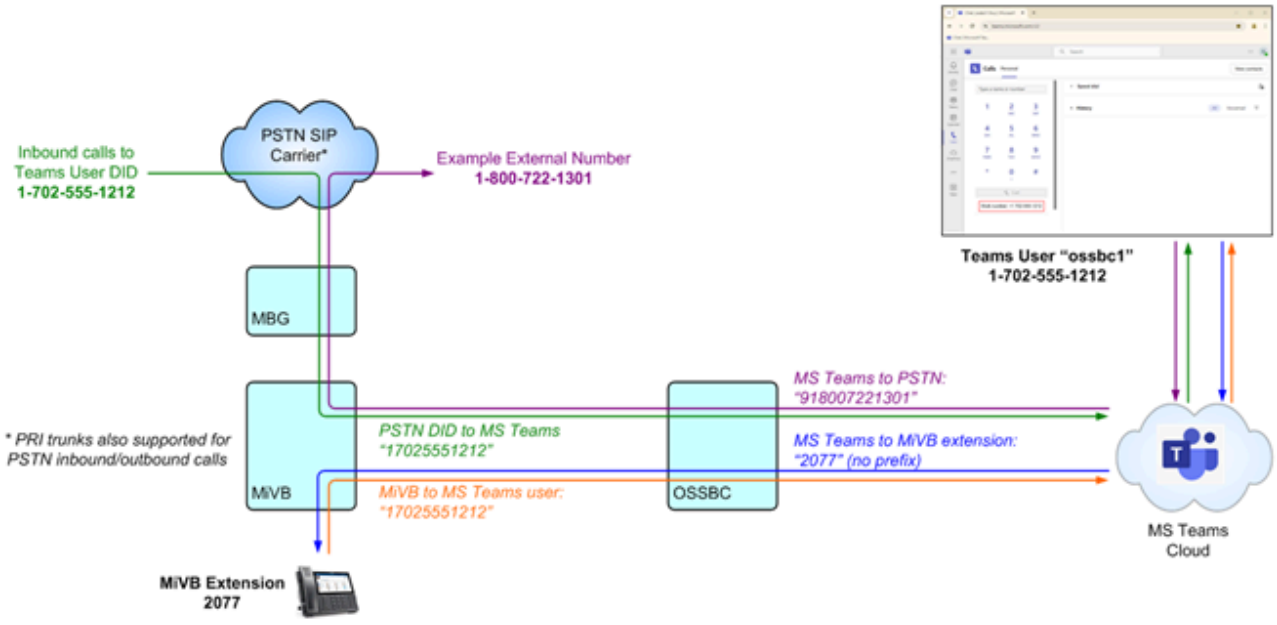
The Software Versions section provides the **minimum** software requirements and can be extended to future software variants compatible with similar firmware.

Configuring MiVoice Business 4

This chapter contains the following sections:

- Prerequisites
- Configuring Licenses
- Configuring Class of Restriction
- Configuring Class of Service
- Configuring the Network Elements
- Configuring Trunk Attributes
- Configuring SIP Peer Profile
- Configuring Automatic Route Selection (ARS)
- Configuring Direct Inward Dialing Service

This section describes the configuration steps necessary to integrate MiVoice Business with Microsoft Teams through Unify OpenScape SBC. Most actions detailed in this section should be executed using the MiVoice Business System Administration Tool.



This document does not cover the initial setup for each component, including installation, user creation, telephony feature activation, calling policy modifications, and other related tasks. For more information about the initial setup for each component, see the MiVoice Business documentation located at Mitel Document Center.

4.1 Prerequisites

This document assumes that there is already a PSTN carrier configured on the MiVoice Business and that Automatic Route Selection (ARS) is configured to send calls to the PSTN using the prefix "9" plus the phone number.

Microsoft Teams users are always assigned an actual Direct Inward Dialing (DID) number, which in North America is +1 (NNN) NNN-NNNN.

Example: Microsoft Teams user **OSSBC1** is assigned +1 (702) 555-1212. A MiVB user who wants to call that Microsoft Teams user will dial "17025551212". For suggestions on ways to shorten this under certain conditions, see Note in Configuring Automatic Route Selection (ARS) on page 18.

Microsoft Teams users can dial external PSTN numbers using the prefix "9" and directly dial MiVB extensions (4 digits in this example) without using any prefixes.

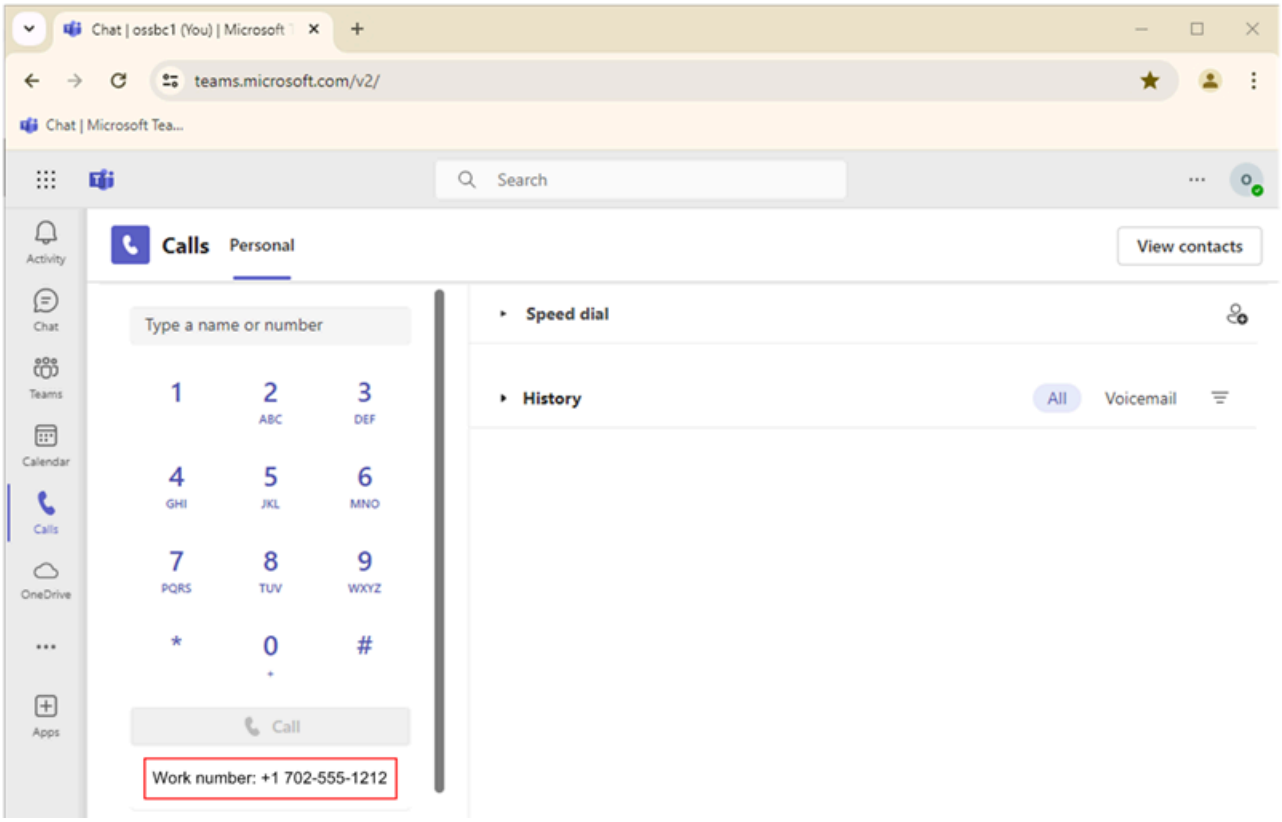


Figure 4: Microsoft Teams call view

4.2 Configuring Licenses

Ensure sufficient MiVoice Business trunk licenses are available and assigned to the MiVoice Business. Trunk Licensing can be verified on the **Licenses > License and Option Selection**.

The number of licenses in the **SIP Trunks** field denotes the maximum number of SIP trunk sessions that can be configured in MiVoice Business for use with all service providers, applications, and SIP trunking devices.

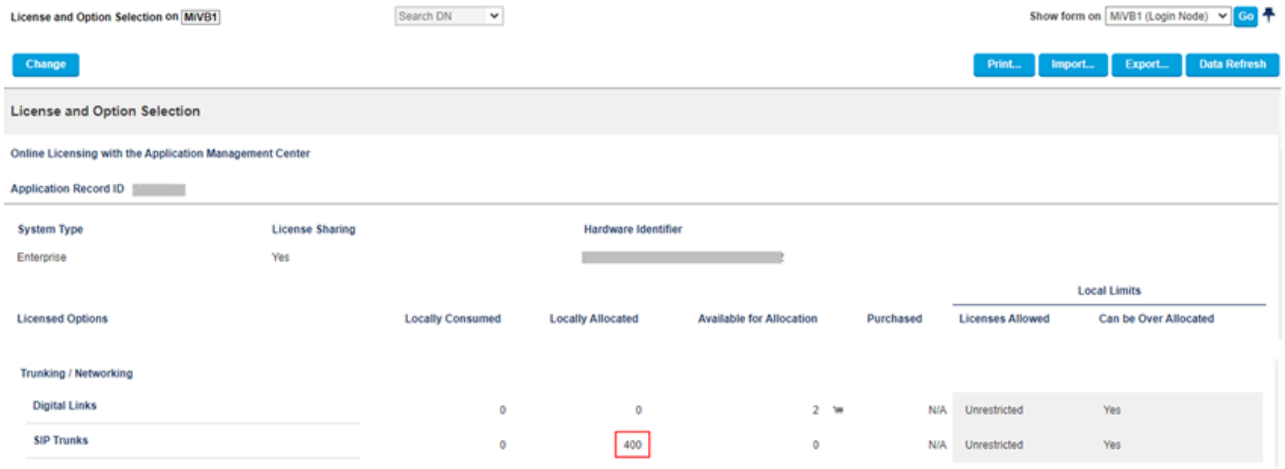


Figure 5: License configuration

4.3 Configuring Class of Restriction

If not already created, create a new Class of Restriction (COR).

1. In the MiVoice Business System Administrator Tool, navigate to **System Properties** > **System Feature Settings** and select **Class of Restriction Groups**.
2. Click on COR number **2**.
3. Click **Change.**
4. In the **Classes of Restriction for Group** field, enter **1,4,5,6,7,10-99,101-110**
5. Click **Save**.

> **Note**:
> If the Mitel Configuration Wizard (MICW) has previously been used to configure this system, COR 2 may already exist and can be used as is.

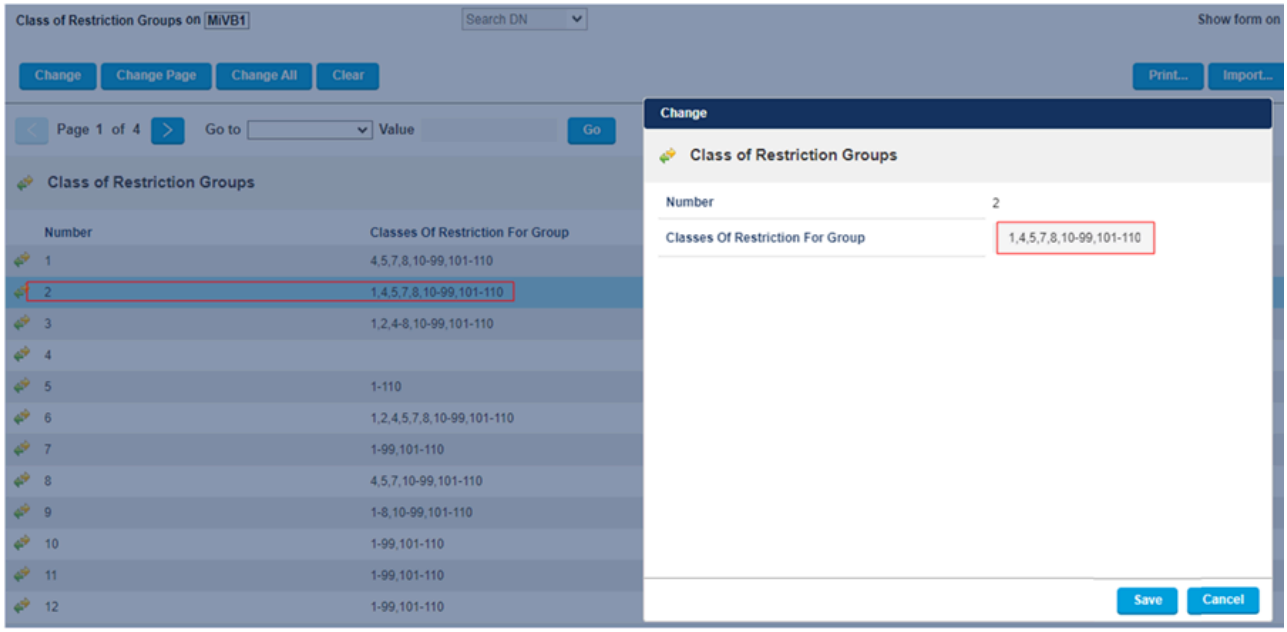


Figure 6: Class of Restriction

4.4 Configuring Class of Service

Classes of Service, identified by Class of Service numbers, are referenced in the Trunk Attributes form for SIP trunks. If not already created, create a new Class of Service (COS).

1. In the MiVoice Business System Administrator Tool, navigate to **System Properties** > **System Feature Settings** and select **Class of Service**.
2. Select **Class of Service** number **56**.
3. Click **Change**.
4. Configure the following under the **General** Tab:

    a. In the **Comment** field, enter a COS name corresponding to the configuration, such as **Trunk-SIP/OSSBC**.
    b. Under the Trunk area, set **Public Network Access via DPNSS** to **Yes**.
    c. Set **Public Network To Public Network Connection Allowed** to **Yes**.
    d. Set **Public Trunk** to **Yes**.
5. Click **Save**.

Note:

Throughout this guide, slot 56 is used for various system options such as Trunk Attributes, Class of Services, ARS Route, etc. You may choose different values for these if they conflict with values in the existing MiVB deployment.

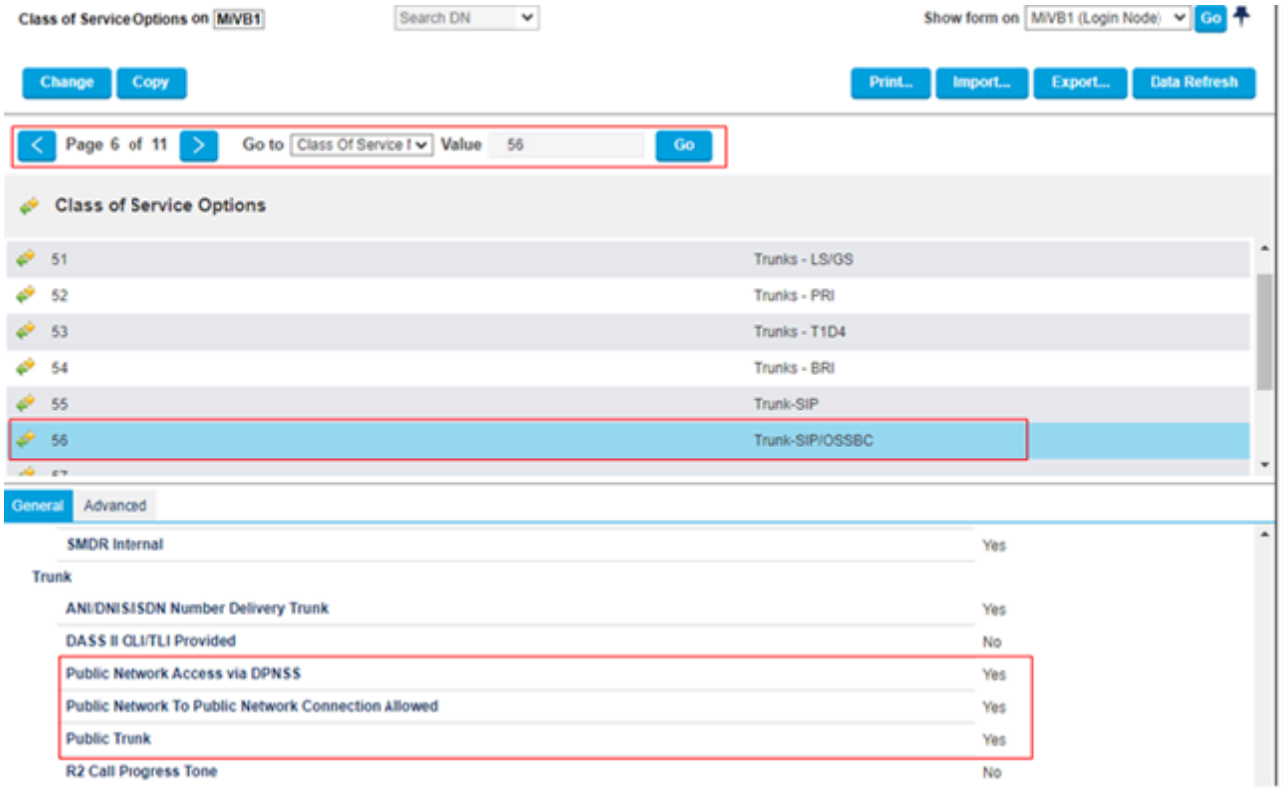


Figure 7: Class of Service

4.5 Configuring the Network Elements

A network element is a physical device or a service component within the network's infrastructure. The configuration settings depend on your system deployment.

To create a network element:

1. In the MiVoice Business System Administrator Tool, navigate to **Voice Network** and select **Network Elements**.
2. Click **Add**.
3. In the **Add** pop-up window, configure the following:

    a. In the **Name** field, enter a unique name that corresponds to the network element you are creating.

> **Note**:
>
> For example, if you are creating a network element for OpenScape SBC, enter **OSSBC**.

b. From the **Type** drop-down menu, select **Other**.
c. In the **FQDN or IP Address** field, enter the IP address of OSSBC.

> **Note**:
> For a multiple-arm deployment, enter the IP address of the LAN interface of the firewall.

d. Check the **SIP Peer** checkbox.
e. From the **SIP Peer Transport** drop-down menu, select **TCP**.
f. In the **SIP Peer Port** field, enter the SIP peer port of the network element, such as 5060.

> **Note**:
> The SIP Peer Port configured in MiVB must match the SIP port configured in the SBC. For example, enter 5060 for both the TCP port configuration in MiVB and the corresponding SBC setting.

g. Click **Save**.

The network element you created is displayed under the **Network Elements** list.

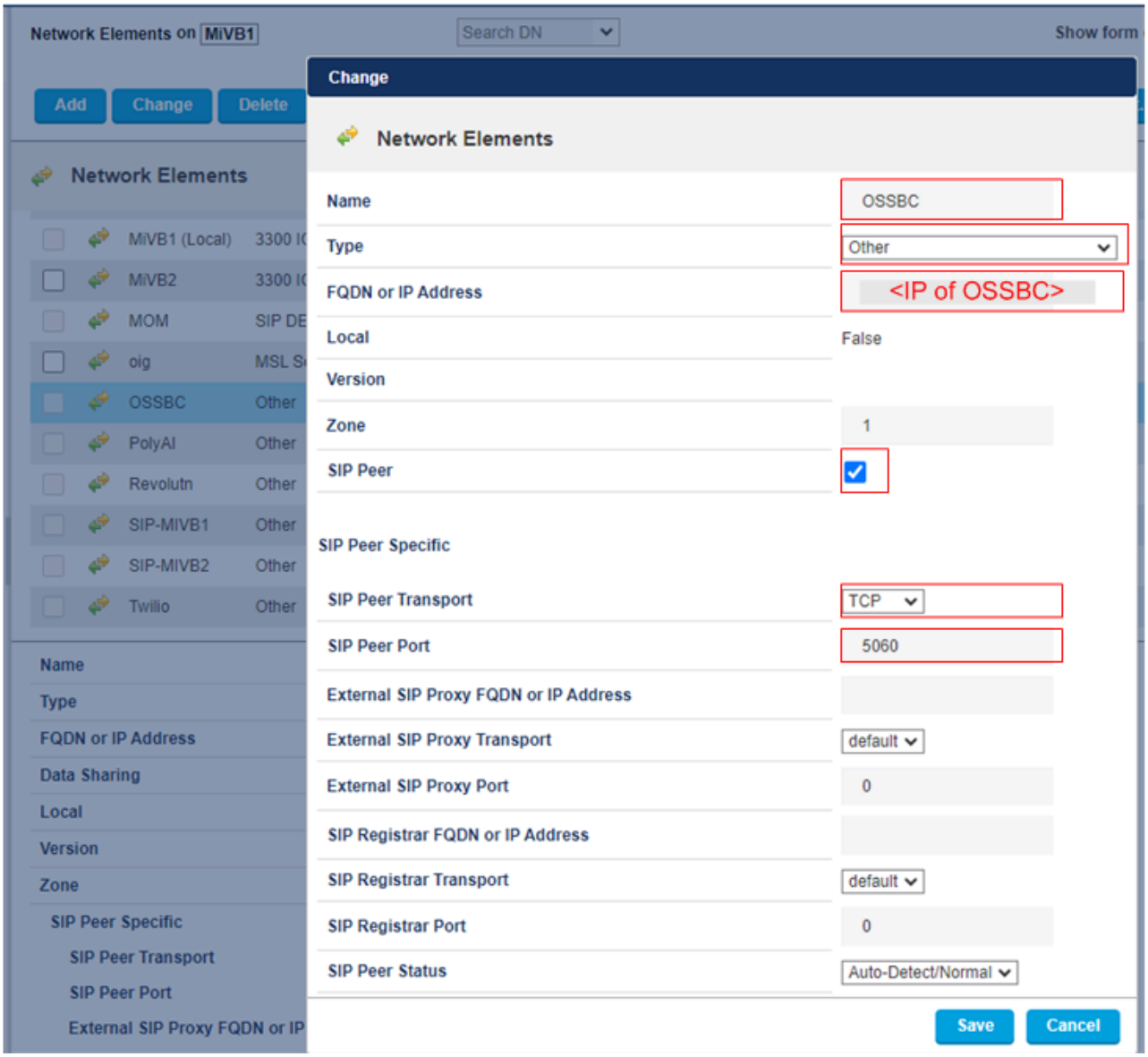


Figure 8: Example: Adding a Network Element for OpenScape SBC

4.6 Configuring Trunk Attributes

This section describes how to configure the **Trunk Attributes** to direct incoming calls to an answer point in the MiVoice Business system.

1. In the MiVoice Business System Administrator Tool, navigate to **Trunks** and click **Trunk Attributes**.
2. Double-click on Trunk Service Number **56**, or select it and click **Change**.

3. In the **Change** pop-up window, do the following:

   a. In the **Class of Service** field, enter: **56**, as configured in step 2 in Configuring Class of Service on page 11.
   b. In the **Class of Restriction** field, enter: **2**, as configured in step 2 in Configuring Class of Restriction on page 10.
   c. In the **Dial In Trunks Incoming Digit Modification - Absorb** field, enter **0**.
   d. In the **Trunk Label** field, enter a unique label corresponding to the trunk attribute, such as **OSSBC**.
4. Click **Save** to save the changes.

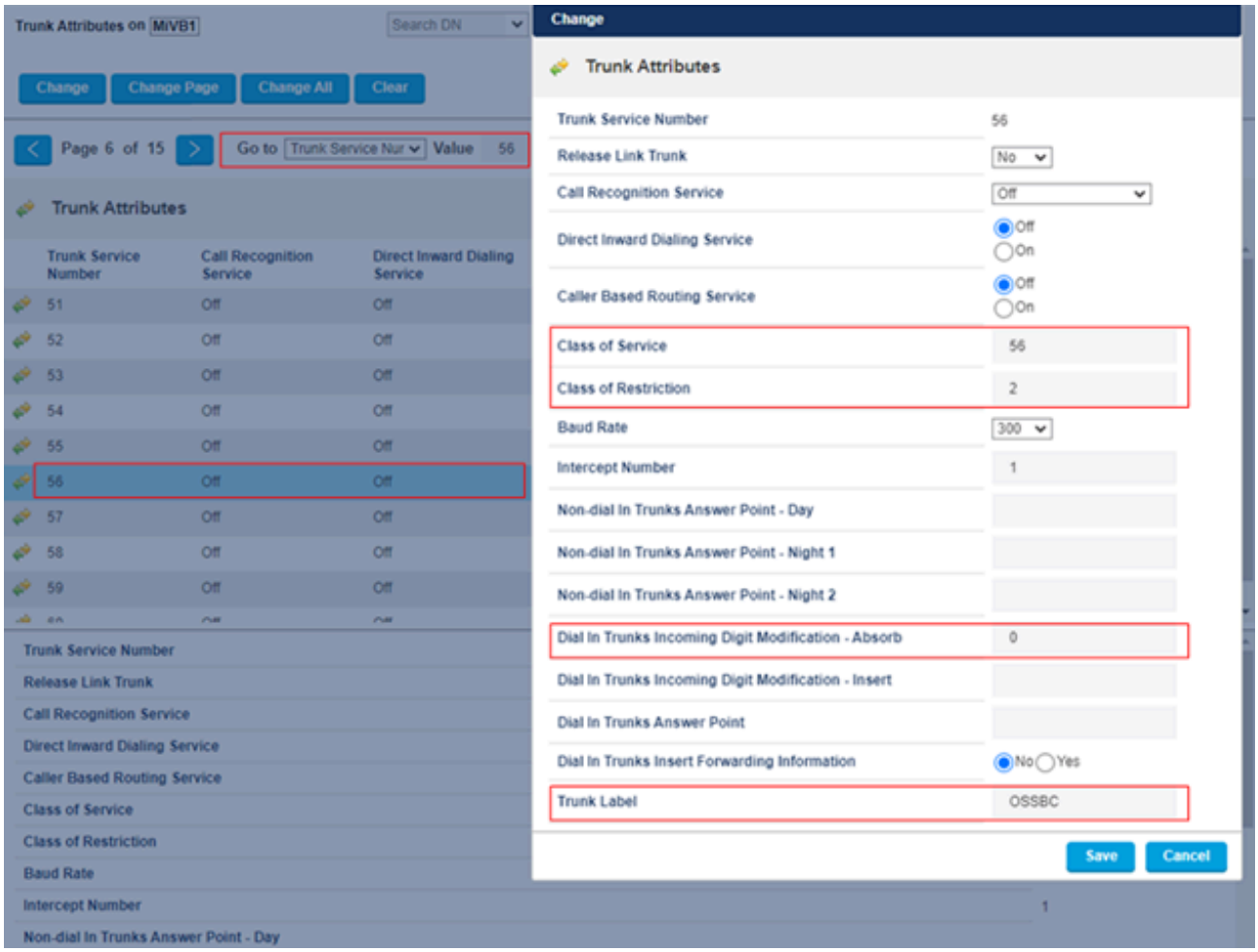


Figure 9: Trunk Attributes form

4.7 Configuring SIP Peer Profile

You can configure SIP peer profiles to manage various aspects of SIP communication, such as authentication, encryption, and Codec negotiation, to facilitate seamless connections between SIP endpoints.

4.7.1 OpenScape SBC SIP Peer Profile Configuration

Follow the steps below to create a SIP Peer Profile for OpenScape Session Border Controller.

1. In the MiVoice Business System Administrator Tool, navigate to **Trunks** > **SIP** and click **SIP Peer Profile**.
2. Click **Add**.
3. Configure the following under the **Basic** tab:

    a. In the **SIP Peer Profile Label**, enter a unique label name that corresponds to the SIP Peer Profile you create, such as **OSSBC**.
    b. From the **Network Element** drop-down menu, select **OSSBC**, as configured in Configuring the Network Elements on page 12.
    c. Under the Local account Information area, in the **Address Type** field, click the radio button for the MiVB IP address.
    d. Under the Administration Options area:

        i. In the **Maximum Simultaneous Calls** field, enter a value equal to or less than the available SIP Trunk licenses.
        ii. In the **Trunk Service** field, enter **56**, as configured in Configuring Trunk Attributes on page 14.
4. Go to the **SDP options** tab:

    a. Set the **Force sending SDP in initial invite message** to **Yes**.

> **Note**:
> The SDP Options tab in the SIP Peer Profile form enables you to configure the connection between MiVoice Business and OS SBC with SRTP. To do so, you must set the AVP Only Peer field to **No**.

5. Configure the following under the **Signaling and Header Manipulation** tab:

    a. Set the **Allow Display Update** to **Yes**.
    b. Set the **Disable Reliable Provisional Responses** to **Yes**.
    c. Set the **E.164: Enable sending '+'** to **Yes**.
    d. In the **E.164 Add '+' if digit length > N digits** field, enter **11**.

The SIP Peer Profile you created is displayed under the **SIP Peer Profile** area.

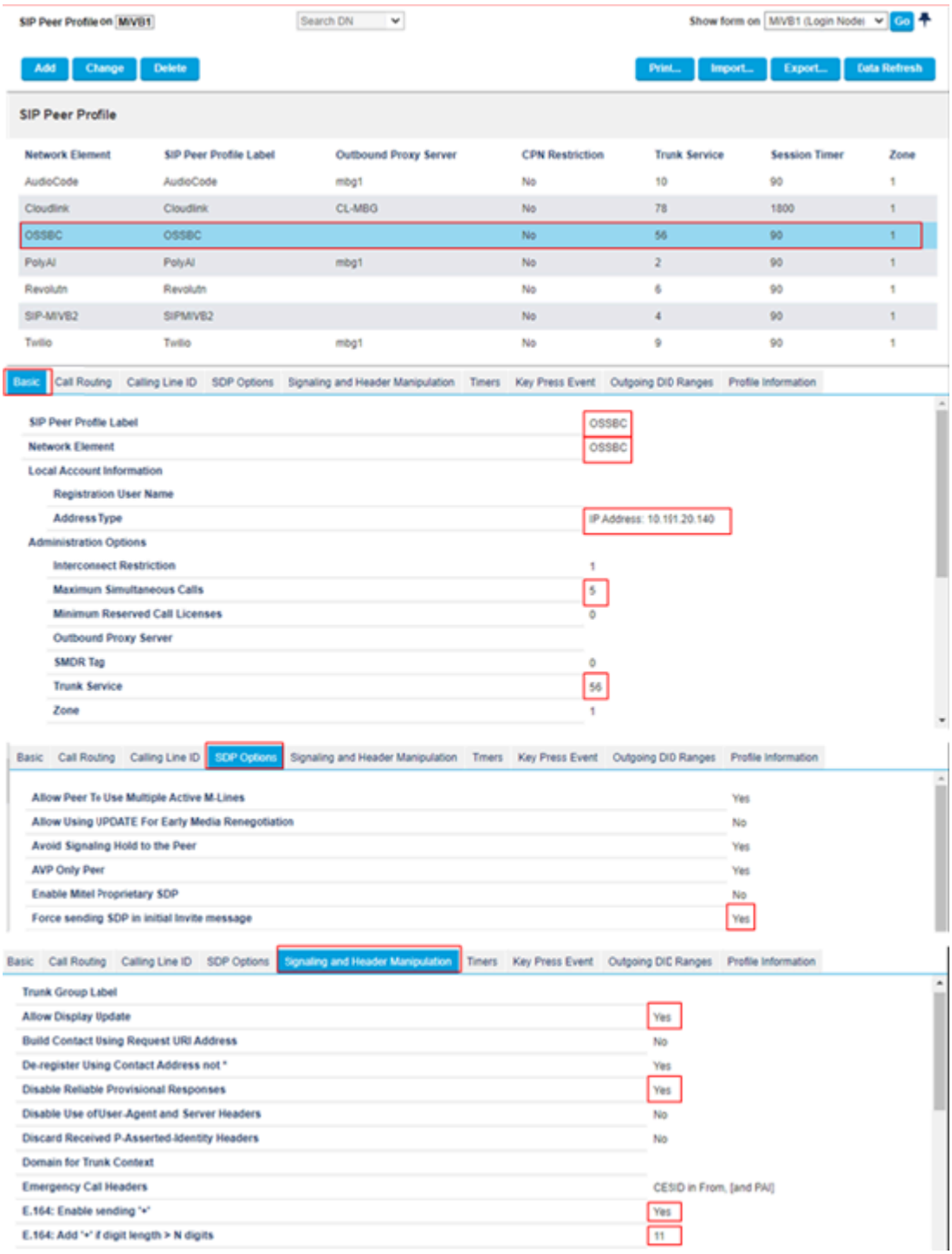


Figure 10: SBC SIP Peer Profile

4.7.2 PSTN SIP Peer Profile Configuration

If you want the Microsoft Teams users' configured phone numbers to be presented as the Calling Party Number/CallerID on outbound PSTN calls, follow the steps below to create a SIP Peer Profile for PSTN.

1. In the MiVoice Business System Administrator Tool, navigate to **Trunks** > **SIP** and click **SIP Peer Profile**.
2. Click on the SIP Peer Profile of your PSTN trunk provider and ensure that the **Public Calling Party Number Passthrough** flag is set to **Yes**.

> **Note**:
> If you choose not to do this, the same **Default CPN** will be presented as the **CallerID/ANI** on all outbound calls.

3. Under the **Calling Line ID** tab, set the **Public Calling Party Number Passthrough** to **Yes**.
4. Click **Save**.

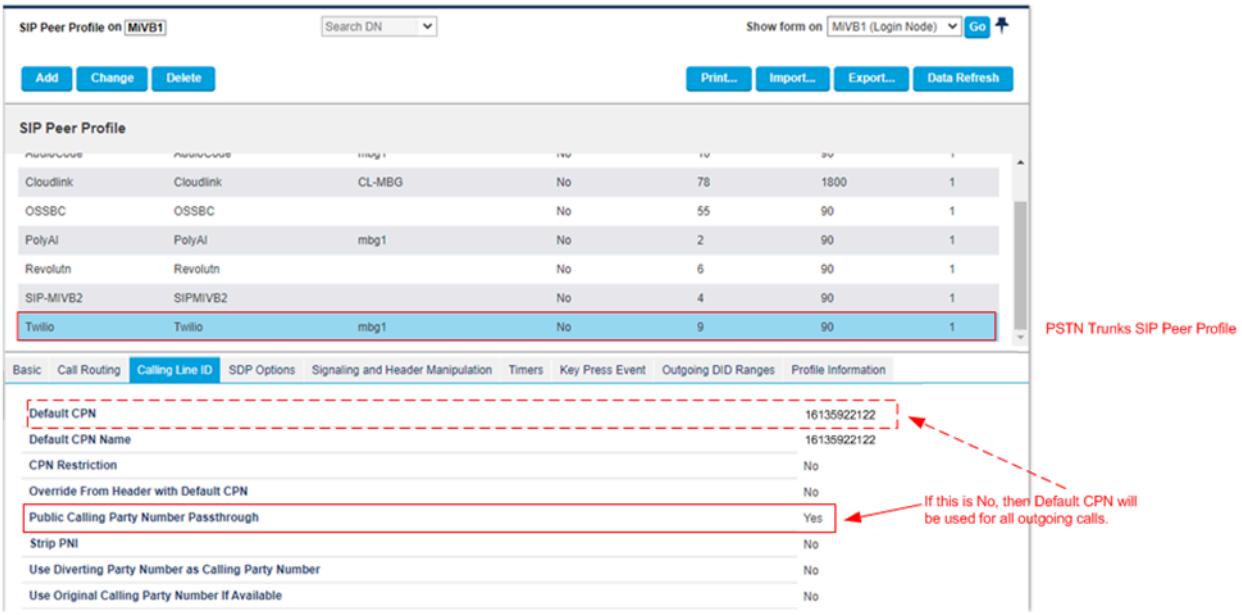


Figure 11: PSTN SIP Peer Profile

4.8 Configuring Automatic Route Selection (ARS)

As stated before, this document assumes that PSTN trunk access is already in place and that MiVoice Business and Microsoft Teams users can place an external call by dialing "9" plus the external phone number. For MiVB users, dialing the Microsoft Teams user's full phone number (including the 1) will route the call to the Microsoft Teams user via Direct Routing. Note that since Microsoft Teams users have dialable phone numbers, each Microsoft Teams user number will need to be entered into ARS, to ensure that returned calls (e.g. from the Missed Calls feature of the MiVB phone) are routed via Direct Routing instead of via the PSTN.

Procedure

- **ARS Digit Modification**: Step 1 creates a digit modification plan that does not absorb or insert any digits.

- **ARS Routes**: Step 2 defines a route to the OSSBC and will be used when there is a matching pattern of digits dialed (as defined in step 3). It will apply Digit Modification Number 56 (as defined in step 1) to dial the Teams user's number without any additional modification.
- **ARS Digits Dialed**: Step 3 tells the MiVB to send any call that matches an MS Teams user's number or pattern to use the route to the OSSBC.

  - If all of the Microsoft Teams users are assigned phone numbers that match a pattern such as 1-702-555-12**00** through 1-702-555-12**99**, then a pattern such as 9 digits with 2 digits to follow would allow any of these numbers to be routed with a single entry.
  - Any Microsoft Teams numbers that do not fit a pattern will need to be explicitly defined in ARS.

Follow the detailed instructions below to configure Automatic Route Selection:

1. In the MiVoice Business System Administrator Tool, navigate to **Call Routing** > **Automatic Route Selection (ARS)** and click **ARS Digit Modification Plans**.

   The **ARS Digit Modification Plans** window is displayed.

   a. Go to the **Digit Modification Number 56** and click **Change** to modify it.

      The **Change** window pops up.

   b. In the **Number of Digits to Absorb** field, enter the number of dialed digits to remove from the start of the dialed number. In this scenario, enter **0**.

   c. Click **Save**.

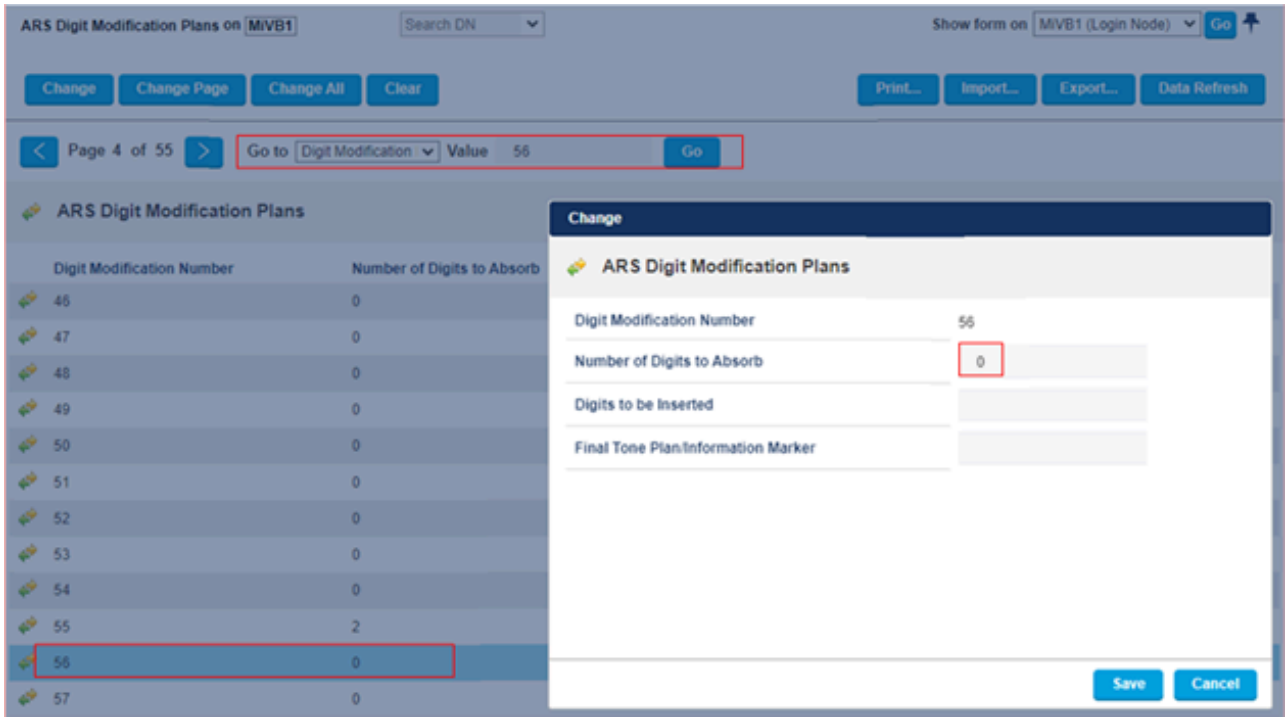


Figure 12: **ARS Digit Modification**

2. Navigate to **Call Routing** > **Automatic Route Selection (ARS)** and click **ARS Routes**.

   a. Go to the **Route Number 56** and click **Change** to modify it.
   b. From the **Routing Medium** drop-down menu, select **SIP Trunk**.
   c. From the **SIP Peer Profile** drop-down menu, select **OSSBC**, as configured in OpenScape SBC SIP Peer Profile Configuration on page 16.
   d. In the **COR Group Member** field, enter **2,** as configured in Configuring Class of Restriction on page 10.
   e. In the **Digit Modification Number** field, enter **56**, as configured in step 1.
   f. Click **Save**.

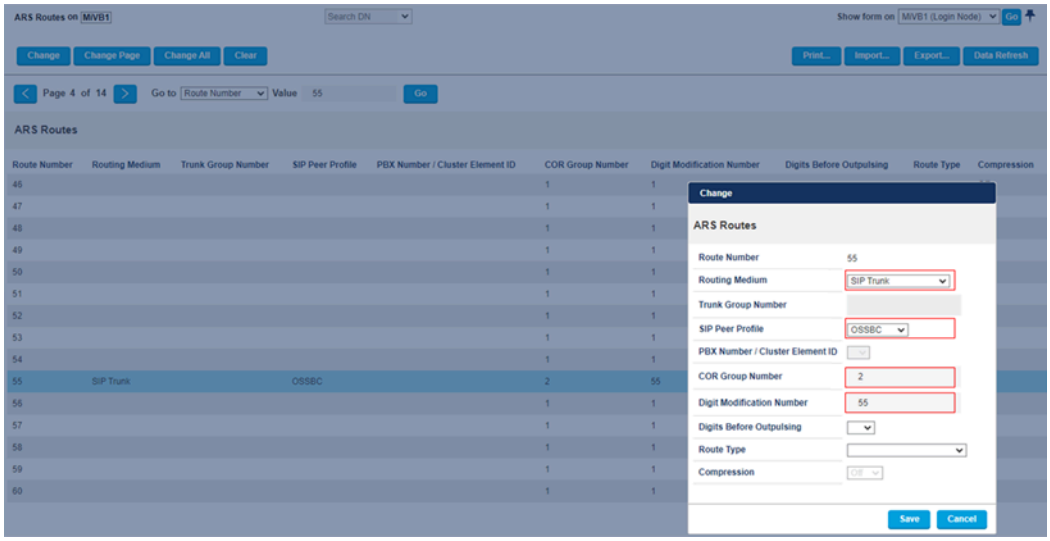


Figure 13: **ARS Routes**

3. Navigate to **Call Routing > Automatic Route Selection (ARS)** and click **ARS Digits Dialed**.

   a. To enter the first pattern or individual number for Microsoft Teams users, click **Add**.
   b. Locate the **Value to change** area and configure the following:

      i. In the **Digits Dialed** field, enter the least specific pattern for only Microsoft Teams users' phone numbers. In the example below, if all of the Microsoft Teams phone numbers range from 1-702-555-1200 through 1-702-555-1299, then enter the portion that is common to all MS Teams users, i.e. "170255512", with 2 digits to follow.
      ii. From the **Number of Digits to Follow** drop-down menu, select the number of digits expected to follow the partial number specified under **Digits Dialed**. In this scenario, select **2**.
      iii. From the **Termination Type** drop-down menu, select **Route**.
      iv. In the **Termination Number** field, enter a **Route Number** corresponding to the **OSSBC.** In this scenario, enter **56.**
      v. If there are Microsoft Teams users with numbers that cannot be defined using a wildcard pattern for one or more digit places, then they will need to be added in their entirety as discrete entries

in the ARS table, with 0 digits to follow. In the screenshot below, the number 17025551399 is explicitly defined as using route **56** to reach the OSSBC.

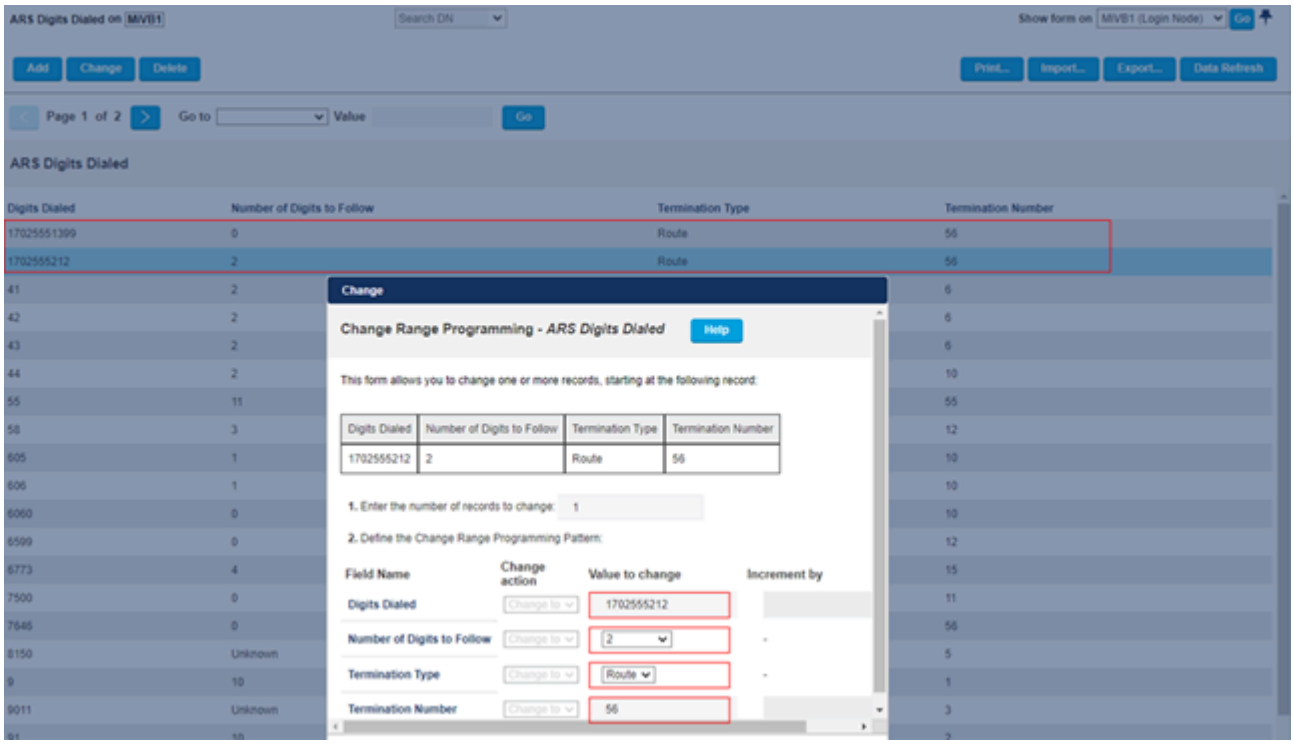


Figure 14: **ARS Digits Dialed**

4. Click **Save.**
5. Repeat as needed to add all MS Teams numbers and/or patterns.

Note:

If desired, **System Speed Calls** can be used to reduce the number of digits that MiVB users need to dial to reach Microsoft Teams users. For example, a System Speed Call could be configured such that dialing 1212 equates to 5517025551212. In this case, each Microsoft Teams user would need have their number associated with a System Speed Call entry.

4.9 Configuring Direct Inward Dialing Service

Microsoft Teams users can be reached from the outside by dialing their DID which is the same as their MS Teams Phone Number.

1. In the MiVoice Business System Administrator Tool, navigate to **Call Routing** > **Call Handling** and click **Direct Inward Dialing Service**.
2. In the page that opens, click **Add**.

3. In the **Add Range Programming - Direct Inward Dialing Service** page that opens, do the following:

   a. In the **DID Number** field, enter **17025551212**.

> **Note**:
> Valid digits are: 0-9, *, and #. Complete DID numbers are preferred, but partial numbers are accepted; the format is determined by the Dial-In Trunks Incoming Digit Modification process, as configured in the Trunk Attributes form.

   b. In the **Destination Number** field, enter a unique 1- to 26-digit Destination Number (internal Directory Number or any other termination point) to which the DID Number will be redirected. In this scenario, enter **17025551212**.
   c. Ensure that **Standard DID** is selected from the **DID Type** drop-down menu.
   d. Click **Save**.

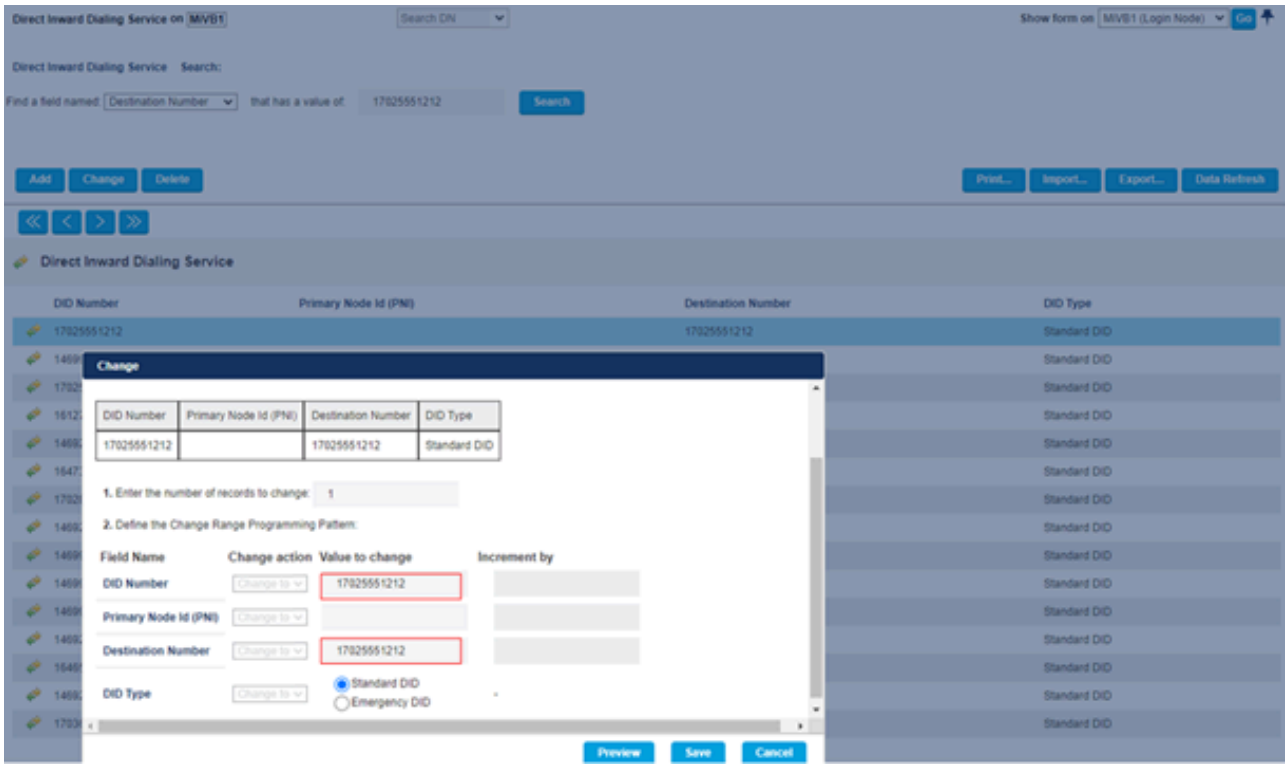


Figure 15: Direct Inward Dialing

Installing OpenScape SBC 5

This chapter contains the following sections:

- Using OVA File
- Using OVF Files

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 23 **(recommended)**
- Using OVF Files on page 27

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 11.5 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 *image_oss-11.00.XX.YY.ova* package from the Mitel 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 23.
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 73.

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 4 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

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.

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 Prerequisite

Important:
You must use SBC version 11.5 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 *image_oss-11.00.XX.YY.ova* package from the Mitel 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**.

5.2.2 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 4.

To generate the ISO image:

1. Extract the *oss-11.00.XX.YY.zip* SBC package. The *oss-11.00.XX.YY.zip* folder is generated.
2. Open the *oss-11.00.XX.YY* folder and extract the *usbsticksetup_oss-11.00.XX.YY.zip* file. The *usbsticksetup_oss-oss-11.00.XX.YY* folder is generated.
3. Move the *image_oss-11.00.XX.YY.tar* file from the *oss-11.00.XX.YY* folder to the *usbsticksetup_oss-11.00.XX.YY/ob* folder.
4. Navigate to the *usbsticksetup_oss-11.00.XX.YY.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-11.00.XX.YY.zip* file. The *vApps_oss-11.00.XX.YY* 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-11.00.XX.YY/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 Verifying SBC Software Status

To verify the SBC software status, see Verifying SBC Software Status on page 26.

Configuring OpenScape Session Border Controller

6

This chapter contains the following sections:

- Verifying License
- Configuring Network/Net Services
- Configuring the Network/Net Services DNS Server
- Configuring Certificates
- Configuring the External Firewall
- Enabling Codec Support for Transcoding
- Configuring Media Profiles
- Configuring Remote Endpoints
- Configuring SIP Server settings
- Configuring Port and Signaling Settings
- Configuring Error Codes

This section describes the configuration required for connecting the OpenScape Session Border Controller (SBC) with MiVoice Business and Microsoft Teams. The instructions provided apply to both single-arm and multi-arm deployment scenarios, unless clearly stated otherwise. For more information, refer to Deployment Scenarios on page 4. In the presented configuration, OpenScape SBC clustered configuration is used, and an external firewall is utilized to route calls to the OpenScape SBC.

The OpenScape SBC can be efficiently administered through a web-based Graphical User Interface (GUI) at the local level, serving as a unified network element within the internal LAN network. This simplifies its management alongside other OpenScape solution components forming the enterprise network. In this solution, we utilize the local management portal to execute the required configurations.

The following figure depicts the OpenScape SBC login page. For the default login credentials, refer to Appendix B: Default User Name and Password on page 73. For restrictions and know issues, refer to Appendix A: Restrictions and Known Issues on page 70.

Figure 16: 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.

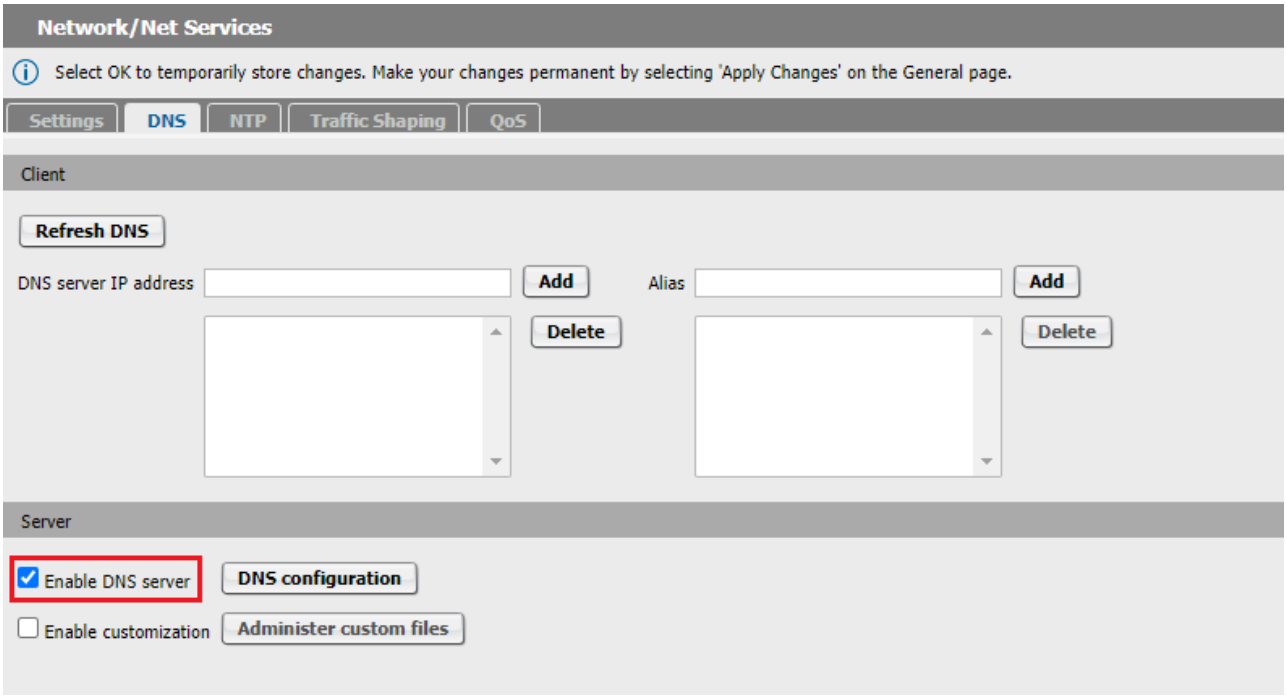


Figure 17: Enabling the DNS Server

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.

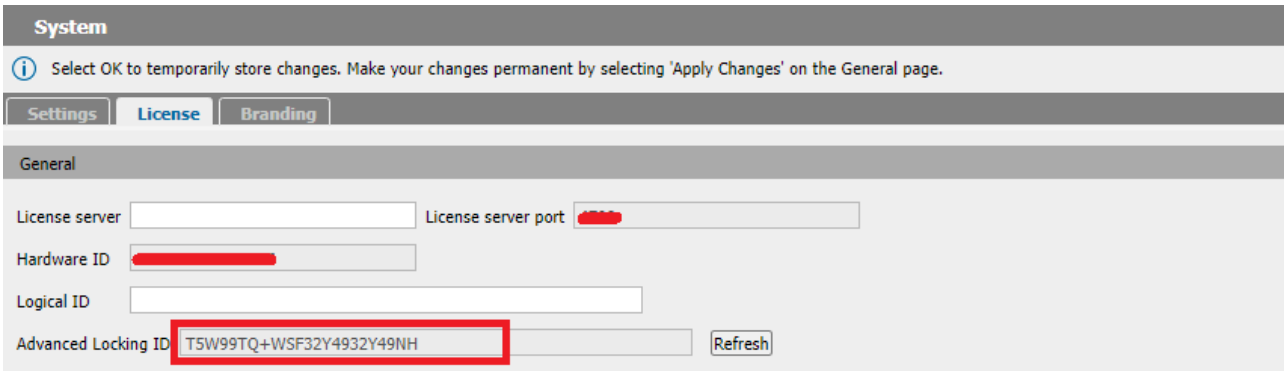


Figure 18: Generating ALI

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 32.

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 19: 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 64.

6.2 Configuring Network/Net Services

This section describes the network and net services configuration for single-arm and multiple-arm deployment. You need to create two access connections:

- One is for communication with the MiVB subnet (access to MiVB).
- A second one for communication with Internet (access Microsoft Teams).

For more information, refer to Deployment Scenarios on page 4.

1. Log in to the SBC local management portal using the local administrative username and password (see Appendix B: Default User Name and Password on page 73).
2. Navigate to the **Network/Net Services** > **Settings** tab in the navigation tree under **Administration**.

   The **Network/Net Services** window pops up.
3. Under the **Physical Network Interface** area, configure the following depending on the deployment:

   a. **Single-arm deployment**

      i. Check the **Single armed** checkbox.

      Note:
      When Single armed is enabled, only the **eth0** interface is enabled. Ensure that both **Single armed** and **eth0** options are enabled.

   b. **Multi-arm deployment**

      i. Ensure that the following options are **Enabled**:

      a) **eth0**
      b) **eth1**
      c) **eth2**

      Note:

      - eth0: This is the network card used for cluster and web interface.
      - eth1: This is the network card used for communication with external firewall (and MS Teams).
      - eth2: This is the network card used for communication with MiVoice Business.

4. Optionally, under **Interface Configuration** > **Core realm configuration**:

   a. **Single-arm deployment:**

      i. The Core realm configuration for eth0 is completed during the installation. Ensure that for the Main-Core-Ipv4:

         a) The interface is set to **eth0**.
         b) Both the **IP address** and **Subnet mask** match the values configured during installation.
         c) Ensure that **SIP-UDP, SIP-TCP** and **SIP-TLS** values are set to **0.**

   b. **Multi-arm deployment:**

      i. The Core realm configuration for the interface (i.e. eth1) is completed during the installation. Ensure that:

         a) The interface matches the value configured during installation.
         b) Both the **IP address** and **Subnet mask** match the values configured during installation.
         c) Ensure that **SIP-UDP, SIP-TCP** and **SIP-TLS** values are set to **0.**

5. Under **Access and Admin realm configuration,** click **Add** to create an entry for communication to Internet (accessing Microsoft Teams).
6. Configure the following:

Settings	Action
Type	From the drop-down menu, select from the following options: **Single-arm deployment:** • For Internet access, select **SA Main IPv4** • For MiVB access, select **Non-VLAN IP** **Multi-arm deployment:** • **Main IPv4** (for eth1) • **Non-VLAN IP** (for eth2 and so on)
Network ID	Enter a unique name for the network ID. For example, Main-Access-IPv4.

Settings	Action
Interface	**Single-arm deployment**: Leave the default setting (eth0). **Multi-arm deployment**: Select the network interface. For example, eth1.
IP address	For accessing Microsoft Teams, enter the Access IP of the SBC located in the same subnet with the firewall. **Note**: See note in step 6 for configuring this setting for MiVoice Business.
Subnet mask	Enter the Subnet mask ID.
Signaling	Ensure that this checkbox is selected.
Media	Ensure that this checkbox is selected.
SIP-UDP	Enter the SIP UDP Port information.
SIP TCP	Enter the SIP TCP port information.
SIP TLS	Enter the SIP TLS port information. **Note**: When configuring the SIP TLS for MiVB, ensure that it matches the corresponding value configured in the MiVB network elements. For example, enter 5061 for both the TLS port configuration in MiVB and the corresponding SBC setting.

Settings	Action
SIP MTLS	Enter 5061. The SIP-MTLS port is used for communication with MS Teams (Mutual authentication).

7. Repeat step 5 to add the **MiVoice Business** network interfaces.

> **Important**:
>
> For MiVB, the **IP address** setting needs to be configured as follows:
>
> Enter the IP for accessing MiVB. For more information, refer to Deployment Scenarios on page 4

8. Under **Realm Profile**, click **Add**.Configure the following:

Settings	Action
Realm Profile	Enter the realm profile for the configuration. For example, Main IPv4. **Note**: Ensure that the Realm profile ID matches the network ID you provided in the **Type** field under **Access and Admin realm configuration** in step 5.
Realm	Select **access**
Signaling network ID	Select the appropriate signaling network ID that you created previously under **Access and Admin realm configuration** in step 5. For example, Main-Access-IPv4.
Media network ID	Select the appropriate media network ID that you created previously under **Access and Admin realm configuration** in step 5. For example, MivVB.

9. Repeat step 7 to add the realm profile for MiVoice Business.
10. Under **Routing**, enter the default gateway IP address in the **Default gateway address** field.

11. Optionally, to create a route to a destination other than the default gateway, then you must create a new routing rule. To do so, under **Routing configuration**, click **Add**. Configure the following:

Settings	Action
Destination	Enter the Destination IP address.
Gateway	Enter the Gateway IP address.
Netmask	Enter the network mask ID.
Interface	Select the interface that will be used to route the IP packets.

12. Optionally, to enable redundancy, select the **Enable redundancy** checkbox.

> **Note**:
>
> For more information, refer to the OpenScape SBC V11 Configuration Guide.

13. If you have selected the **Enable redundancy** checkbox:

    a. Enter the default gateway IP address in the **Core link connectivity check IP address** field.
    b. Check the **Enforce call context mirroring based on LAN MTU size** checkbox.
14. Click **OK**.
15. Click **Apply Changes** to apply this configuration.

6.3 Configuring the Network/Net Services DNS Server

The DNS server should include the IP addresses of the DNS servers for Access subnet (if needed). To do so:

1. In the SBC local management portal, navigate to **Network/Net Services** > **DNS** tab in the navigation tree under **Administration**.
2. In the **DNS server IP address** under the Client area, enter the DNS server of the firewall network and click **Add**.

Note:
You can add up to 3 DNS servers.

3. Click **OK** to save the configuration.
4. Click **Apply Changes**.

6.4 Configuring Certificates

Certificate configuration is mandatory for ensuring successful communication between the OpenScape Session Border Controller and Microsoft Teams.

Note:
Ensure that all the OpenScape SBC certificates are in .pem format before uploading them 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.

Create certificate profiles in OpenScape SBC for the following scenarios:

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

Prerequisites

Perform the following procedure if the third party is CA:

1. Generate the Certificate Signing Requests (CSR).
2. Get the certificates from third party authority.
3. Import the certificates to OpenScape SBC. To import the certificates, see Importing OpenScape SBC Certificates on page 42.

Note:
The SBC FQDN name must be resolvable and configured in a DNS server. In this case, the Certificate Signing Request (CSR) provided by the SBC should include this FQDN as a Common or Alternative Name.

Importing OpenScape SBC Certificates

To import the OpenScape SBC certificates:

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

   The **Security** window pops up.
2. Click **Certificate management**.

   The **Certificate Management** window pops up.
3. Scroll down to locate the **Certificates Upload** area and configure the following:

   a. Under **CA certificates**, click **Choose File**, select the CA certificate file, click **Open**, and then click **Upload** to upload the CA certificate file.
   b. Under **X.509 certificates**, click **Choose File**, select the X.509 server certificate file, click **Open**, and then click **Upload** to upload the certificate file.
   c. Under **Key files**, click **Choose File**, select the private key file, click **Open**, and then click **Upload** to upload the private key certificate file.
4. Scroll up to locate the **Certificate Profiles** area and click **Add** to configure the certificate profile.
5. In the **Certificate Profile** window that opens, configure certificate profile for **Microsoft Teams**.

   a. Under **Certificate Profile configuration** do the following:

Field	Action
Certificate profile name	Enter a certificate profile name, such as **Teams_Cert_Profile**.
Certificate service	Select **SIP-TLS** from the drop-down list.
Local server certificate file	Select the **X.509 Certificate** that you uploaded in step 3.
Local CA file	Add the CA file with the root CA certificate that signed the local certificates.
Local key file	From the drop-down menu, select the local key file containing the private key.

Field	Action
EC param	Enter the appropriate value. This parameter is used to allow the configuration of the Elliptical Curve, which is utilized with ECDH and ECDHE cipher suites.
Attach to Config file	Ensure that this option is NOT checked.

b. Under **Renegotiation**, if checked, uncheck the **Enforce TLS session renegotiation** option.
c. Under **TLS version**, from the **Minimum TLS version** drop-down menu, select **TLS V1.2**.
d. Under **Cipher Suites**, configure the following:

   i. From the **Perfect Forward Secrecy** drop-down menu, select **Preferred PFS**.
   ii. From the **Encryption** drop-down menu, select **Preferred AES-128.**
   iii. From the **Mode of Operation** drop-down menu, select **Preferred GCM.**

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

6.5 Configuring the External 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 4.

To configure the external firewall settings, follow the External Firewall Settings configuration on page 44 instructions.

Prerequisite (Single-arm deployment)

Proper configuration is required in the Firewall prior configuring the external 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 MiVB is located.
3. Configure network equipment to route the traffic between new DMZ LAN interface and the local network (MiVB).
4. Allow traffic between the DMZ LAN interface and the local network, and vice versa.
5. Create firewall rules to allow traffic between MiVB – 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 MiVoice Business (see MiVoice Business Remote Endpoint configuration on page 54). RTP ports depends on configuration of RTP ranges (see Configuring Port and Signaling Settings on page 60). 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 Microsoft Teams Remote Endpoints configuration on page 56) and by access realm SIP ports of SBC (see Configuring Network/Net Services on page 36). The RTP ports depend on the configuration of RTP ranges; (see Configuring Port and Signaling Settings on page 60). 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.

Prerequisite (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 Microsoft Teams Remote Endpoints configuration on page 56) and by access realm SIP ports of Session Border Controller (see Configuring Network/Net Services on page 36).
2. The RTP ports depend on the configuration of RTP ranges (see Configuring Port and Signaling Settings on page 60). 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.

6.5.1 External Firewall Settings configuration

This section describes how to configure the external firewall settings based on your system deployment. For more information, refer to Deployment Scenarios.

In a **single-arm** deployment, you need to configure external firewall settings for each of the following:

- MiVoice Business
- Main, that is, Internet access (Microsoft Teams)

This means you will need to create two entries in the Firewall Settings list.

In a **multi-arm** deployment, you need to configure external firewall settings only for Main, that is, Internet access (Microsoft Teams).

To configure the external firewall settings:

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

   The **Security** window pops up.
2. Click **Add**.

   The **Firewall Configuration** window pops up.
3. From the **Network ID** drop-down menu, select **the Network ID** for which you are configuring the Firewall configuration entry.

   For example, if you are configuring the Main network, select Main. Otherwise, select MiVB.
4. Check the **Enable IP masquerading** checkbox.

   This checkbox allows you to enable IP masquerading. With IP masquerading, LAN addresses are masked when they interact with the WAN, effectively hiding the entire internal address space so that it appears as a single IP address within another, often public, address space.
5. Check the **Enable port forwarding** checkbox.
6. Under Incoming networks connections:

   a. For **single-arm configuration**, select **Allow** for the following services:

   - **SNMP**

   > **Note**:
   > Allow the SNMP incoming network connection only if are configuring the Main Network ID. For the MiVoice Business configuration, block it.

   - **HTTPS**
   - **SSH**
   - **ICMP**
   - **SIP**
   - **TLS**
   - **RTP/sRTP**

> **Note**:
> These settings affect new incoming connections (Devices under SBC trying to access WAN service).

b. For **multiple-arm configuration**, select **Allow** for the following services:

- **ICMP**
- **SIP**
- **TLS**
- **RTP/sRTP**

7. Under the **External Firewall** area, check the **External Firewall** checkbox.
8. In the **Firewall external IP** field, enter the external firewall IP address.

> **Important**:
> For the MiVoice Business configuration, the firewall's external IP must match the corresponding IP configured in MiVoice Business (IP of firewall's LAN interface). In the main configuration, the firewall's external IP is the public IP address of the firewall.

9. Click **OK.**

6.6 Enabling Codec Support for Transcoding

You might need to enable Codec support for transcoding if there is a different Codec selection between MiVoice Business and Microsoft Teams.

To enable Codec support for transcoding:

1. In the SBC local management portal, navigate to **Features** in the navigation tree under Administration.
2. Select the **Enable Codec Support for Transcoding** check box on the page that opens.
3. Click **Configure**.

   Clicking on the **Configure** option launches the Codecs window where various checkboxes for codecs, such as OPUS, can be enabled or disabled.
4. Under the **Enable** column, select the checkboxes for the Codecs required in your system for transcoding. For example:

- **G711A 8 kHz - 64 kbps**
- **G711U 8 kHz - 64 kbps**
- **G722 8 kHz - 64 kbps**
- **G729 8 kHz - 8 kbps**
- **OPUS 48 kHz - Variable**

> **Note**:
> The above codes are for illustration purposes only.

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

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 Business

> **Note**:
> This configuration applies to both single-arm and multi-arm deployments. For more information, refer to Deployment Considerations.

To configure the media profiles:

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. To enable the **Default Media Profile,** configure the following:

Field	Action
Name	Enter a Media Profile name. For example, default.
Media protocol	Select **RTP only** from the drop-down list.
Support ICE	Check the **Support ICE** checkbox. Select **Full** from the drop-down list.

Field	Action
RTP/RCP Multiple in offer	Select the **RTP/RCP Multiplex in offer** checkbox.
SRTP configuration	Select **SDES Both**.
RTCP configuration	Do the following: a. In the **RTCP Mode** field, ensure that the default option **Bypass** is selected from the drop-down list. b. In the **RTCP generation timeout** field, enter the time (in seconds) that the media application must wait for an RTCP on the same direction before it starts generating them.
Codec configuration	Select the **Allow unconfigured codecs** option.
Codec	Select **G711A 8kHz - 64 kbps** (for Europe) or **G711U 8kHz - 64 kbps** (for US-NA)[1] from the drop-down list and click **Add** to add it to the bottom of the list of codecs for this media profile.

4. Click **OK**.
5. To enable **Microsoft Teams Media Profile**, under Media Profiles, click **Add** and do the following:

Note:
If Media Bypass is OFF in Microsoft Teams Configuration,you must enable Support ICE with Full. If it is ON, then select Support ICE with Lite. This ensures optimal configuration for your system without any unnecessary complications.

Field	Description
Name	Enter a Media Profile name. For example, Teams.

[1] Codecs must be adjusted according to the region where the SBC is installed.

Field	Description
Media protocol	Select **SRTP only** from the drop-down list.
Support ICE	Check the **Support ICE** checkbox. The configuration of this option depends on the deployment: • In a single-arm or a multi-arm (Firewall NAT mode) deployment, select **FULL** from the drop-down list. • In a multiple-arm (Firewall Bridged mode) deployment, select **LITE** from the drop-down list. **Note**: For more information on the deployment scenarios, refer to Deployment Scenarios on page 4.
RTP/RTCP Multiplex in offer	Select the **RTP/RTCP Multiplex in offer** checkbox.
SRTP configuration	In the **SRTP crypto context negotiation** field, select the **SDES** checkbox and select **SDES AES-128** only from the drop-down list.
RTCP configuration	Do the following: a. In the **RTCP Mode** field, ensure that the default option **Bypass** is selected from the drop-down list. b. In the **RTCP generation timeout** field, enter the time (in seconds) that the media application must wait for an RTCP on the same direction before it starts generating them.

Field	Description
Codec	Select **G711A 8kHz - 64 kbps** (for Europe) or **G711U 8kHz - 64 kbps** (for US-NA), **G729 8 kHz - 8 kbps**, and **G722 8 kHz - 64 kbps** from the drop-down list and click **Add** to add it to the bottom of the list of codecs for this media profile.

6. Click **OK**.
7. To enable the **MiVoice Business Media Profile**, under Media Profiles, click **Add** and configure the following:

Field	Description
Name	Enter a Media Profile name. For example, MiVB.
Media protocol	Select **SRTP only** from the drop-down list.
Support ICE	Check the **Support ICE** checkbox. Select **Full** from the drop-down list.
RTP/RTCP Multiplex in offer	Select the **RTP/RTCP Multiplex in offer** checkbox.
SRTP configuration	In the **SRTP crypto context negotiation** field,select the **SDES** checkbox and select **SDES Both** from the drop-down list.
RTCP configuration	Do the following: a. In the **RTCP Mode** field, ensure that the default option **Bypass** is selected from the drop-down list. b. In the **RTCP generation timeout** field, enter the time (in seconds) that the media application must wait for an RTCP on the same direction before it starts generating them.
Codec configuration	Enable the **Allow unconfigured codecs** option.

8. Click **OK**.

9. 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.
10. Click **OK** to save the configuration.
11. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

6.8 Configuring Remote Endpoints

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.

Specifically, you need to follow the instructions provided in the chapters mentioned below, in the specified order:

Create SIP Service Provider Profiles (SSPs)

1. Create one SIP Service Provider Profile for MiVoice Business:MiVoice Business SIP Service Provider Profile configuration on page 52
2. Create one SIP Service Provider Profile for Microsoft Teams: Microsoft Teams SIP Service Provider Profile configuration on page 53

Configure Remote endpoints settings

1. Create one MiVoiceBusiness remote endpoint: MiVoice Business Remote Endpoint configuration on page 54
2. Configure three remote endpoints for the Microsoft Teams main access interface: Microsoft Teams Remote Endpoints configuration on page 56

> **Note**:
> Microsoft Teams provides three remote endpoints, and you can configure one or more depending on your needs. In this scenario, for redundancy, it is recommended to configure all three available remote endpoints.

Prerequisite

1. You must select the **Standalone with internal SIP Stack** option from the **Comm System Type** drop-down menu, under VoIP > SIP Server Settings.
2. To avoid network delays, you have ensured that the value in the SSP OPTIONS timeout (ms) field under Timers and Thresholds is 5000.

For more information, refer to Configuring SIP Server settings on page 58.

6.8.1 MiVoice Business SIP Service Provider Profile configuration

The following configuration must be applied to the MiVB Remote Endpoint Profile to handle both Microsoft Teams -> MIVB calls as well as Microsoft Teams -> PSTN 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 **MIVB**.
6. Under **SIP Privacy**, from the **Privacy Support** drop-down menu, select **Full**.
7. Under **SIP User Agent**, in the **SIP User Agent towards SSP** field, select **Passthru** from the drop-down list.
8. Under **Outgoing SIP manipulation**, click **Manipulation.**

   The **SIP SP Manipulation** window pops up.

   a. Click **Add**.
   b. In the **Matching digits** field, enter **+1**.
   c. In the **Min/Max Length** field, enter **5/14**.
   d. In the **Number of digits to delete** field, enter **2**.
   e. From the **Call-type** drop-down menu, select **SIP-Provider**.

      This single entry will handle both Microsoft Teams > MiVB extensions (4-digits) and Microsoft Teams > PSTN calls. Since MS Teams inserts a "+1" on outgoing calls, this rule will intercept calls going to MiVB that fit the pattern of "+1" plus anywhere from 4 to 12 digits. Additionally, it will strip the first two digits ("+1") before sending to MiVB.

Note:
The Max Length can be adjusted accordingly in countries with longer telephone numbers or to accommodate international dialing.

Examples:

- Microsoft Teams user dials "2077". Microsoft Teams sends "+12077" to OSSBC, which removes first two digits and passes "2077" to MiVB, which rings extension 2077.
- Microsoft Teams user dials "918007221301". Microsoft Teams sends "+1918007221301". OSSBC removes first two digits and passes "918007221301" to MiVB, which routes the call via ARS to the PSTN.

f. Click **OK** to save the settings. You are directed back to the **SIP Service Provider Profile** window.

9. Under **Incoming SIP Manipulation**, in the **Calling Party Number** field, select **From header user and display name part** from the drop-down list.
10. Under **TLS**, in the **TLS Signaling** field, select **Pass-Thru** from the drop-down list.
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.

6.8.2 Microsoft Teams SIP Service Provider Profile configuration

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 **Teams**.
7. From the **Default SSP Profile** drop-down menu, select **MSTeams.**
8. Locate the **SIP Privacy** area.From the **Privacy Support** drop-down menu, select **Full**.
9. Under the **SIP Service Address** area, check the **Use SIP Address for identifying header** checkbox.

10. Check the following checkboxes:
    - **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**
11. 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.

12. Locate the **SIP User Agent** area. From the **SIP User Agent towards SSP** drop-down menu, select **Passthru.**
13. Under **Flags**, select the following checkboxes:
    - **Do not send Invite without SDP**
    - **Preserve To and From headers per RFC2543**
    - **Send Contact header in OPTIONS**
    - **Avoid sending 183 messages**
    - **Avoid sending 180 message (for 60s)**
14. Under **TLS**, from the **TLS Signaling** drop-down menu, select **Transport=tls.**
15. Under **SIP Connect**, select the **Send user=phone in SIP URI** checkbox.
16. Click **OK** to save the configuration.
17. Click **OK**.
18. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

6.8.3 MiVoice Business Remote Endpoint configuration

Follow the steps below to configure a MiVoice Business remote endpoint.

Prerequisite: You have created a MiVoiceBusiness SIP 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:

Menu item	Action
Name	Enter a unique name for the MiVoice Business remote endpoint. For a MiVB remote endpoint configuration, enter a name such as MiVB.
Type	From the drop-down list, select **SSP**.
Profile	From the drop-down list, select the MiVoice Business profile. For example, MiVB.
Access realm profile	From the drop-down list, select the MiVoice Business access realm profile. For example, MiVB.
Core realm profile	From the drop-down list, select: • **Main-Core-Realm – ipv4**.

7. Under the **SSP OPTIONS** area, select the **Enable SSP connectivity check** checkbox and in the OPTIONS interval (sec) field, enter 60.

Note:
This option is displayed only after configuring the Prerequisite.

8. Under the **Remote Location Information** area, from the **Signaling address type** drop-down list, select **IP address or FQDN**.
9. Under the **Remote Location domain list** area, click **Add.**

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

- Under **General**, configure the following:

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

Menu item	Action	Notes
Remote port	Enter the remote port for communication between MiVB and Microsoft Teams.	
Remote transport	From the drop-down list, select the information you provided in the SIP Peer Transport field in the Network Elements form from within the MiVoice Business system.	

10. Under **Media Configuration**, from the **Media profile** drop-down, select the media profile for the MiVB.
11. Click **OK**.

    You are directed back to the **Remote endpoint configuration** window.
12. Under **Remote Location Identification/Routing**, do the following:

    - 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, 50015.
    - In the **Incoming Routing Prefix** field, you must enter the incoming route prefix to route calls to Microsoft Teams. For example, +30214 or 4444.
13. Click **Add**.
14. Click **OK**.
15. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

6.8.4 Microsoft Teams Remote Endpoints configuration

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

Prerequisite: You have created a Microsoft Teams SIP 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.
Type	From the drop-down list, select **SSP**.
Profile	From the drop-down list, select the Microsoft Teams profile. For example, Teams.
Access realm profile	From the drop-down list, select the **Main-access-Realm** profile.
Core realm profile	From the drop-down list, select **Main-Core-Realm-ipv4**.

7. Under the **SSP OPTIONS** area, select the **Enable SSP connectivity check** checkbox.
8. In the **OPTIONS interval (sec)** field, enter 60.
9. Under the **Remote Location Information** area, from the **Signaling address type** drop-down list, select **IP address or FQDN**.
10. Under the **Remote Location domain list** area, click **Add.**

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

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

12. In the **Remote Location Domain** page that opens, under **General**, do the following:
    - In the **Remote URL** field, enter the URL of the remote endpoint or domain. The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name) or as Logical-Endpoint-ID.
    - In the **Remote port** field, enter the endpoint's SIP port information as provided by the PSTN provider.
    - In the **Remote transport** field, select the remote transport protocol provided by the PSTN provider from the drop-down list.
13. Under **TLS,** do the following:
    - From the **TLS mode** drop-down menu, select **Mutual authentication**.
    - From the **Certificate profile** field, select the TLS certificate profile for teams. For example,Teams.
14. Under **Media Configuration**, from the **Media profile** drop-down menu, select the media profile for Microsoft Teams. For example, Teams.
15. Click **OK**.

    You are directed back to **Remote Endpoint configuration** window.
16. Under **Remote Location Identification/Routing**, 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 CoreRealm Port are unique for each remote endpoint. For example, 51000.
17. Click **OK**.
18. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

If needed, repeat steps 5-18 to add two more Microsoft Teams remote endpoints:

- sip.pstnhub.microsoft.com
- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

6.9 Configuring SIP Server settings

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 MiVoice Business and Microsoft Teams.

To accomplish this, you must create one group for MiVoice Business 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 4.

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

2. From the **Comm System Type** drop-down menu, select **Standalone with internal SIP Stack.**

> **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 36.

3. To avoid network delays, ensure that the value in the SSP OPTIONS timeout (ms) field under Timers and Thresholds is 5000.
4. Under **Direct Routing Configuration**, click **Configure**.

   The Direct Routing window pops up.
5. Create the MiVoice Business Group:

   a. In the **Group name** field, enter the group name for MiVoice Business. For example, MiVB.
   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 **SSP**.
   d. Locate the **Endpoints for Group '[Group name]'** area, as depicted in the following figure.

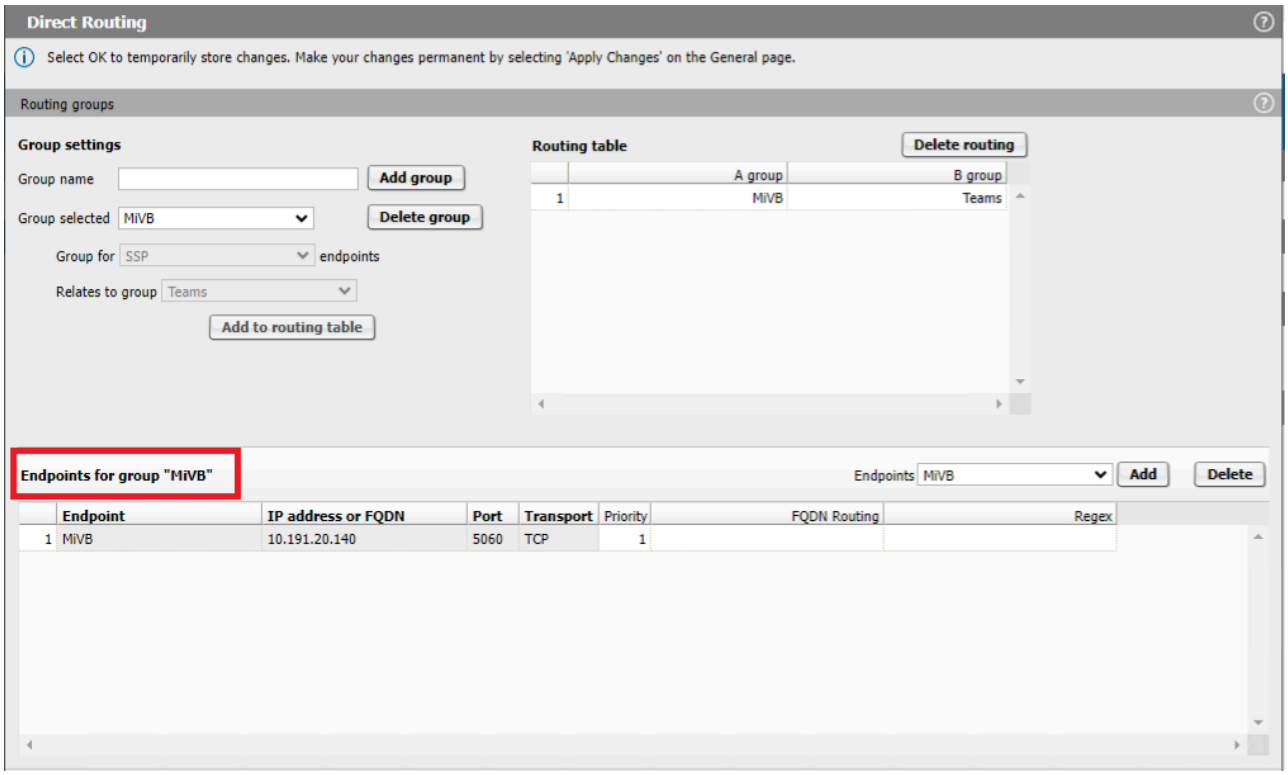


Figure 20: MiVoice Business Direct Routing Group

   e. From the **Endpoints** drop-down on the right, select the MiVoice Business group, such as **MiVB**, and click **Add**.

6. Create the Microsoft Teams Group:

   a. In the **Group name** field, enter the group name for Microsoft Teams. For example, Teams.
   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 Endpoints configuration on page 56 and click **Add**.
7. Relate the MiVoice Business group to the Microsoft Teams group:

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

      The endpoint is added to the Routing table.
   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.

      The endpoint is added to the Routing table.

   Note:

   The following combinations of types are allowed to associate the groups:

   - MS Teams with SSP, and vice-versa.
   - Gateway with SSP, and vice-versa.

   The Endpoints for the group <group name for the endpoint> are displayed automatically.
8. Click **OK**.
9. Click **OK** to save the configuration.
10. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

6.10 Configuring Port and Signaling Settings

To configure the port and signaling settings, do the following:

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

2. Under **Port Range**, do the following:

   a. Under **Media independent RTP ports**, in the **Port min** and **Port max** fields enter the defined port range for RTP to allow both incoming and outgoing UDP traffic in the external firewall to Microsoft Teams.
   b. Under the **Subscribers dynamic SIP ports** field, enter the **Port min** and **Port max** fields enter the SIP port range to be used as core port of remote endpoints. The valid value for Min and Max is between 50000 and 54999.

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

   c. Under **Signaling and Transport Settings**, do the following:

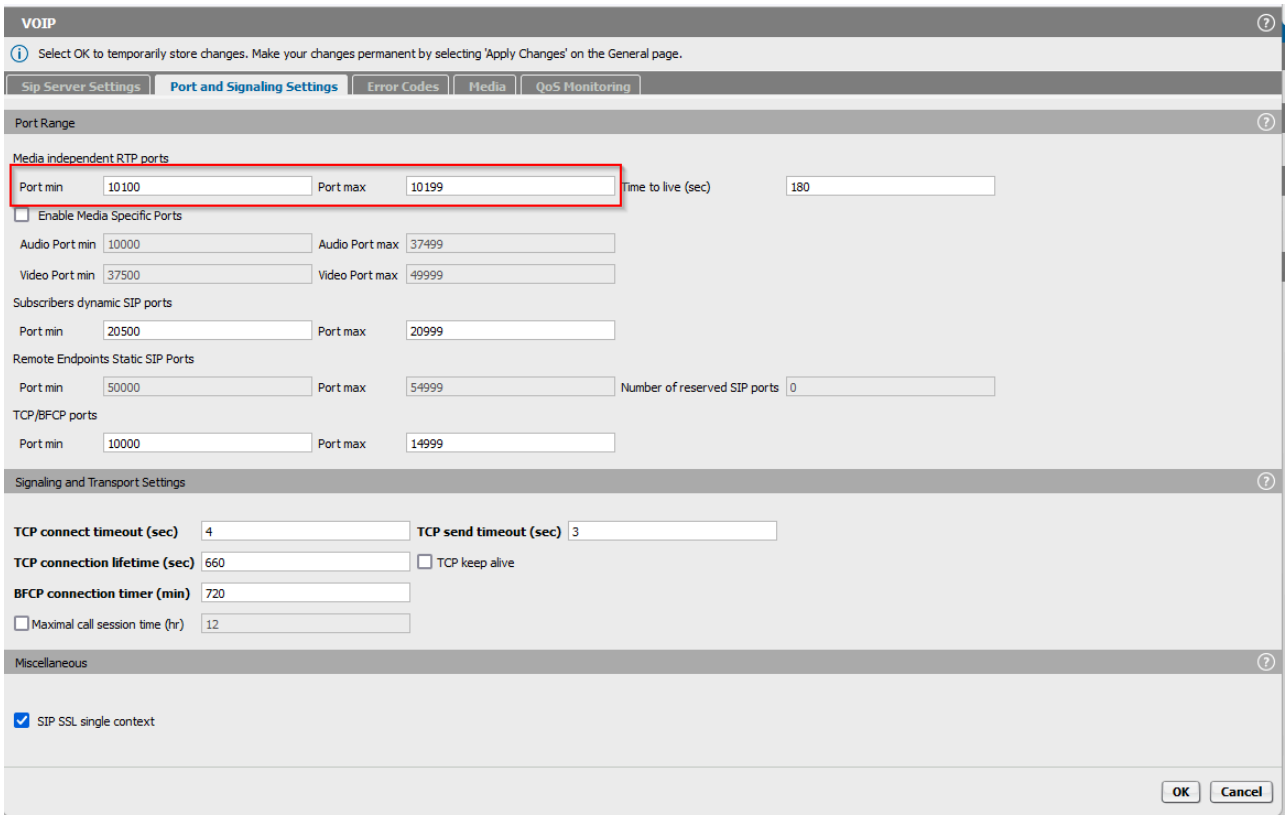
      i. In the **TCP connect timeout (sec)** field, enter the time in seconds before an outgoing attempt to connect will be stopped.
      ii. In the **TCP send timeout (sec)** field, enter the time in seconds after a TCP connection will be closed if it is not available.
      iii. In the **TCP connection lifetime (sec)** field, enter the lifetime in seconds for TCP connections, any TCP connection which is inactive for the lifetime will be automatically closed.
      iv. In the **BFCP connection timer (min)** field, enter the duration timer for a BFCP connection that is established over TCP or TLS.

      Note:
      The value is entered in minutes. The range must be between 60 and 1440 minutes, with a default value of 720 minutes (12 hours).

      v. Under **Miscellaneous**, select the **SIP SSL single context** checkbox to save SIP Server shared memory.

      Note:
      Enabling this option allows the SIP Server's child processes to share the same SSL context.

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



6.11 Configuring Error Codes

If the code for rerouting is not selected, SBC will send a "486 Busy Here" message to the caller, indicating a busy signal.

To verify that error code **486 Busy Here** is not selected do the following:

1. In the SBC local management portal, navigate to **VoIP** > **Error Codes** tab in the navigation tree under **Administration**.
2. Ensure that the **Enable routing for all codes** and **Disable routing for all codes** checboxes are not selected.
3. In the **Items/Page** field, select 200 from the drop-down list. This displays all the errors available in the system.
4. Ensure that the **486 Busy Here** checkbox is not selected.
5. Click **OK** to save the configuration.
6. Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

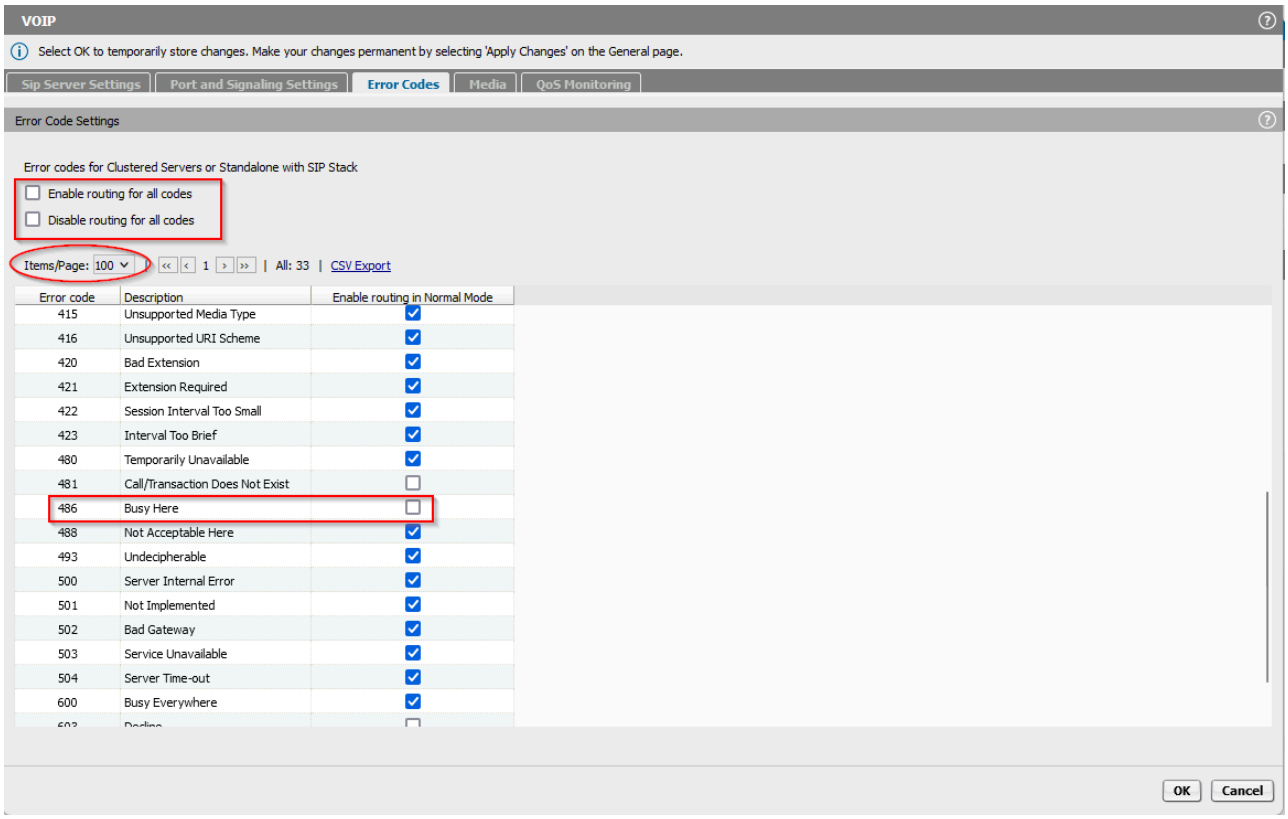


Figure 21: Error Codes configuration

Configuring Microsoft Teams 7

This chapter contains the following sections:

- Configuring Direct Routing
- Configuring Voice Routes
- Configuring Voice Routing Policies
- Assigning a PSTN Number to the User
- Configuring User's Voice Routing Policy

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 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 on page 41.

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 2: 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 on page 53.
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 .
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
Location based routing and media optimization	
Media bypass	Environment specific value. For information on deployment options, see Deployment Scenarios on page 4.
Bypass mode	Always

Parameter	Sample Value
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.

7.2 Configuring Voice Routes

Add and associate a voice route with the OpenScape SBC established in Configuring Direct Routing on page 64. Additionally, create a Dial number pattern for this voice route to facilitate communication within the Microsoft Teams environment.

MS Teams should be programmed to simply pass all dialed digits to the OSSBC without modification (though it will still add "+1" by default). All digit modification will be handled by the OSSBC and MiVB. As such, a single Voice Route should be programmed as shown below, with ".*" as the dialed number pattern.

To configure voice routes:

1. In **Microsoft Teams admin center**, navigate to the **Voice > Direct Routing**.
2. Select **Voice routes**.
3. Click **Add**. Configure the following:

Parameter	Action
Voice route	Enter a name for your voice route, such as **Route all to OSSBC**.

Parameter	Action
Description	Enter the description for the voice route, such as **Route all to OSSBC**.
Priority	Enter **1**
Dialed number pattern	Enter **.***
SBCs enrolled	Click **Add SBCs** to add an SBC. Select the SBC you want to add and click **Apply**.
PSTN usage records	a. Click **Add PSTN usage** to add the PSTN records. b. Click **+Add**. c. Enter **OSSBC** as PSTN usage record. d. Select the PSTN usage record that you created. e. Click **Save and apply**.

4. Click **Save**.

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

7.3 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.

7.4 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.

7.5 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 67.
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.

Appendix A: Restrictions and Known Issues 8

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

Feature	Issue Description
User Impact (Product Limitations)	
Display Conference participants	When creating a conference, the participants are not displayed on the device in the Display Conference Participants feature. Is displayed how many are the participants (i.e., 3-way conference).
Delays Microsoft Teams	Occasionally, in Microsoft Teams users experience a consistent delay of 1-2 seconds when connecting the audio with MiVoice Business.

Feature	Issue Description
Reject Call Option	MiNET devices do not have a reject call option available.
Hold Info	If the other party (that is, Microsoft Teams user) sets the call on Hold, MINET device does not display in the screen Hold Informational message.
Hunt - Ring Groups	MiVoice Business does not support adding external numbers to groups. Additionally, the numbers must be limited to a maximum of 7 digits.
Do Not Disturb External	Enabling the DND (Do Not Disturb) feature on MINET devices does not hinder the reception of incoming external calls, and it also does not impact the user's capability to initiate calls.
MS Teams On Hold - Recall	When a call is placed on hold by Microsoft Teams and terminates unexpectedly, Microsoft Teams does not automatically recall the user. It is important to note that Microsoft Teams does not provide support for recalling users when a call is put on hold and then terminated.
G711 codec	In MiVoice Business, the codec labeled G711 is a mandatory selection and cannot be excluded from the list of available codecs.
Semi Attendance Microsoft Teams	Conducting a semi-attended consult (cancel second consult call) on the Teams client is not possible. The available options are limited to attended and blind transfer.
Early Media (Firefox)	Firefox is unable to understand 183 – Session in Progress with SDP message, thus the MS Teams user is hearing the ringing tone, instead of the network announcement. According to Microsoft forum, Firefox is not a fully supported browser for Microsoft Teams.
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 requ ired by some emergency providers to retrieve the correct user location.
User Impact (Issues Resolution Work in Progress)	
Ringback Tone not Heard	When MS Teams calls a mobile number and the PSTN provider delays to send the RTP packets for ringback tone then the ringback tone is not heard. This only occurs while using MS Teams web client to call a mobile number, when registered to a specific provider. OSSBC-14329 has been created to provide a solution to this problem. In addition, no ringback tone is heard occasionally, when calling MiVB device. The root cause was identified to a specific MS Teams SIP server.

Feature	Issue Description
Call Forwarding Info	When making an external call with MINET devices, the caller is not notified if the call is being forwarded to another number. Similarly, Microsoft Teams does not provide any information about the redirection to the caller. Furthermore, when Microsoft Teams sends an INVITE to MiVoice Business, there directing phone number included in the History-Info header is not used. MIVB-38878 is created for this issue. Additionally, MiVoice Business does not send any Diversion or History-Info header, including the redirecting number, to Microsoft Teams through OS SBC. OSSBC-14170 has been created for this issue.
SIP Error Codes	All SIP error codes from MiVoice Business are converted by SBC to "480Temporarily Unavailable". OSSBC-14152 has been created to address the issue.
MiVB Converts Wrongly the Early Media SIP Messages	The external number is busy or not available the SIP service provider sends 181and then 183 with SDP. Under these circumstances MiVoice Business converts "181 call is being for warded" from SIP service provider to "180 Ringing". Thus, the user will first hear ringing (which is wrong) and then the network announcement. Issue is investigated in MiVB-40297.
Configuration Topics	
Ringback Tone - PRACK	MiVoice Business be default requires PRACK response for 180 Ringing SIP message, wh ich is currently not supported by OS SBC. Thus, proper configuration should be applied i n MiVoice Business, not to expect PRACK message (Disable Reliable Provisional Respon ses = yes, in SIP Peer Profile), for ringback tone to be heard. OSSBC-14323 has been cre ated to support PRACK response in OS SBC.
Endpoint Offline	Due to network delays the responses of SIP OPTION messages were received with delay and the endpoint was set offline. This is addressed by setting SIP OPTION timeout to 5000ms.
Ports Core Realm	The administrator should change the SIP-TLS ports of the Core Realm to another unused port (for example 5081), to use 5061 on the Access and Admin realm configuration.
Call Forward No Answer to MS Teams	When MINET device is configured to forward the call to MS Teams user, when there is not answer, the forward fails because of MiVoice Business be default sends RTP instead of SRTP. To address the issue the following commands should be applied to MiVoice Business, connected using SSH application (i.e., Putty). • mcdDebug • g_allowfakesrtpoffer=1
Park Call from MS Teams to PSTN	If the PSTN provider does not support inactive media streams, the option Suppress Use of SDP Inactive Media Streams in SIP Peer Profile should be enabled in MiVoice Business.
Areas Not Covered	
Micollab Integration	Micollab Features not tested as part of this testing.
DTMF	Out-of-band DTMF was tested using RFC4733/RFC2833. MS Teams does not use SIP INF O method to send DTMF events.

Appendix B: Default User Name and Password

9

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.

Mitel
Powering connections
mitel.com

Copyright 2024, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation, including itself and subsidiaries and authorized entities. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.