

MiVoice 5000 - Integration with Microsoft Teams Through OpenScape Session Border Controller

06/2025

IMPLEMENTATION GUIDE



NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 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

Mitel® is a registered trademark of Mitel Networks Corporation.

All trademarks mentioned in this document are the property of their respective owners, including Mitel Networks Corporation. All rights reserved.

®,™ Trademark of Mitel Networks Corporation

©Copyright 2025, Mitel Networks Corporation

All rights reserved

CONTENTS

1	ABOUT THE DOCUMENT	3
1.1	ABOUT THIS DOCUMENT	3
1.2	RELATED DOCUMENTATION	3
1.3	INTENDED AUDIENCE	3
1.4	DISCLAIMER	3
2	PRESENTATION	4
2.1	OVERVIEW	4
2.2	DEPLOYMENT SCENARIOS	4
2.2.1	SINGLE ARM CONFIGURATION	4
2.2.2	MULTI ARM CONFIGURATION	5
2.2.3	NETWORK REALMS CONFIGURATION	7
2.3	SOFTWARE VERSIONS	7
3	CONFIGURING THE MIVOICE 5000 SERVER	8
3.1	PREREQUISITE	8
3.2	CONFIGURING TRUNK GROUP	8
3.3	CONFIGURING DIALING PLAN	9
3.4	CONFIGURING CONFERENCE AND TRANSFER FUNCTIONS (OPTIONAL)	11
4	INSTALLING OPENScape SBC	12
4.1	USING OVA FILE	12
4.1.1	PREREQUISITE	12
4.1.2	INSTALLING OPENScape SBC USING OVA FILE	12
4.1.3	CONFIGURING IP ADDRESS	13
4.1.4	VERIFYING SBC SOFTWARE STATUS	14
4.2	USING OVF FILES	14
4.2.1	PREREQUISITE	14
4.2.2	GENERATING ISO IMAGE WITH USB STICK	15
4.2.3	INSTALLING SBC USING OVF FILE	16
4.2.4	VERIFYING SBC SOFTWARE STATUS	16
5	CONFIGURING OPENScape SBC	17
5.1	VERIFYING LICENSE	17
5.1.1	PREREQUISITE	18
5.1.2	PROCEDURE	19
5.2	CONFIGURING NETWORK/NET SERVICES	20
5.2.1	PREREQUISITE	20
5.2.2	PROCEDURE	20
5.3	CONFIGURING THE NETWORK/NET SERVICES DNS SERVER	24
5.4	CONFIGURING CERTIFICATES	24
5.4.1	GETTING CERTIFICATES AND KEY FILES	25
5.4.2	IMPORTING OPENScape SBC CERTIFICATES	25
5.5	CONFIGURING FIREWALL	26
5.5.1	PREREQUISITE (SINGLE-ARM DEPLOYMENT)	27
5.5.2	PREREQUISITE (MULTI-ARM DEPLOYMENT)	27
5.5.3	FIREWALL SETTINGS CONFIGURATION	27
5.6	ENABLING CODEC SUPPORT FOR TRANSCODING	29
5.7	CONFIGURING MEDIA PROFILES	29
5.8	CONFIGURING REMOTE ENDPOINTS	32
5.8.1	PREREQUISITE	32
5.8.2	MIVOICE 5000 SIP SERVICE PROVIDER PROFILE CONFIGURATION	32
5.8.3	MICROSOFT TEAMS SIP SERVICE PROVIDER CONFIGURATION	33
5.8.4	MIVOICE 5000 REMOTE ENDPOINT CONFIGURATION	35
5.8.5	MICROSOFT TEAMS REMOTE ENDPOINT CONFIGURATION	37
5.9	CONFIGURING SIP SERVER SETTINGS	38
5.10	CONFIGURING PORT AND SIGNALING SETTINGS	40

5.11	CONFIGURING ERROR CODES.....	41
6	CONFIGURING MICROSOFT TEAMS	43
6.1	PREREQUISITE	43
6.2	CONNECTING OPENScape SBC TO DIRECT ROUTING	43
6.3	VERIFYING SSP CONNECTIVITY STATUS	44
6.4	ASSIGNING A PSTN NUMBER TO THE USER.....	44
6.5	CONFIGURING DIRECT ROUTING	45
6.6	CONFIGURING VOICE ROUTES	46
6.7	CONFIGURING VOICE ROUTING POLICIES.....	47
6.8	CONFIGURING USER'S VOICE ROUTING POLICY	48
7	APPENDIX	49
7.1	RESTRICTIONS AND KNOWN ISSUES.....	49
7.2	DEFAULT USER CREDENTIALS FOR OPENScape SBC	51

1 ABOUT THE DOCUMENT

1.1 ABOUT THIS DOCUMENT

This document provides a reference to Mitel Authorized Solutions providers for configuring the MiVoice 5000 to integrate Microsoft Teams through OpenScape SBC. The different devices can be configured in various configurations depending on your VoIP solution.

1.2 RELATED DOCUMENTATION

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

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

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

- [MS Teams Solution Guide \(HTML\)](#)

For additional information on the MiVoice 5000, refer to Mitel Document Center:

- [MiVoice 5000 Technical Documentation](#)

1.3 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 5000, Microsoft Teams, and OpenScape SBC.

1.4 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.

2 PRESENTATION

2.1 OVERVIEW

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 5000 and OpenScape SBC with Microsoft Teams. Additionally, it describes the steps required for configuring Emergency Calls.

2.2 DEPLOYMENT SCENARIOS

2.2.1 SINGLE ARM CONFIGURATION

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.

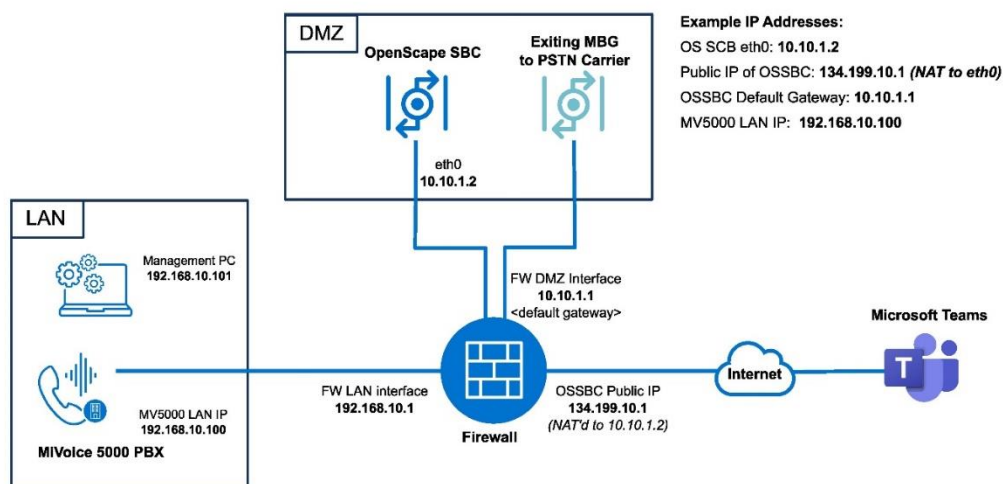


Figure 1: Single-Arm Configuration

Note that an MBG server cannot be used with integrations involving MiV5000 platform. In this case, the PSTN point can be directly connected to the MiVoice 5000 server or through the MiVoice 5000 SBC server.

The following figure depicts the single-arm configuration without an MBG.

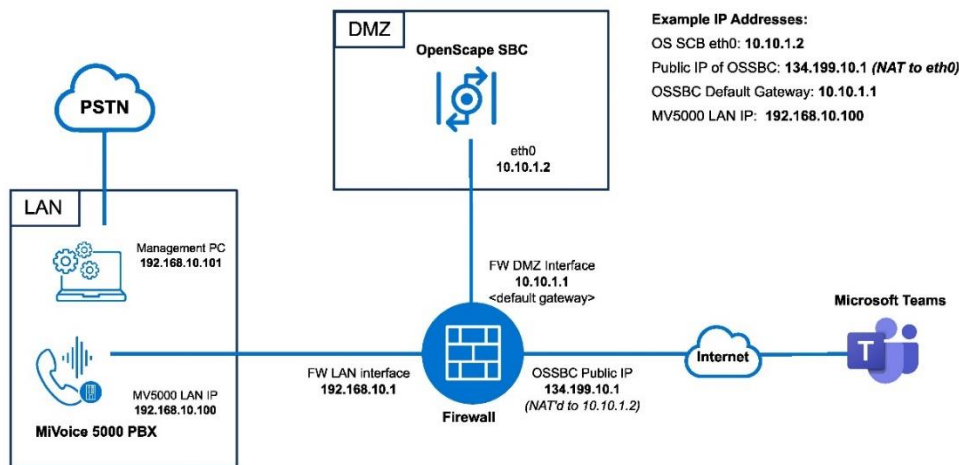


Figure 2: Single-Arm Configuration, without MBG

2.2.2 MULTI 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 and **ICE-FULL** for **Firewall NAT** mode because Microsoft Teams receives the external address of the firewall in the SDP.

The following figures depict the multiple-arm deployment scenarios.

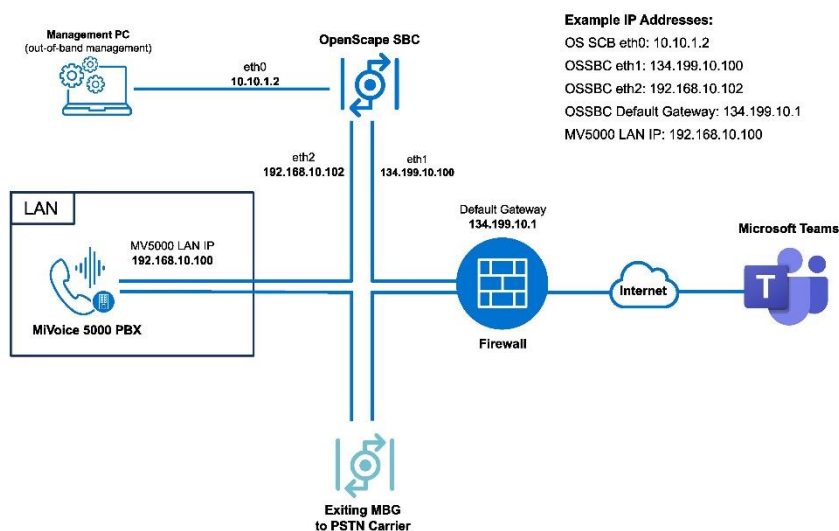


Figure 3: Multiple-Arm Configuration - Firewall Bridged Mode

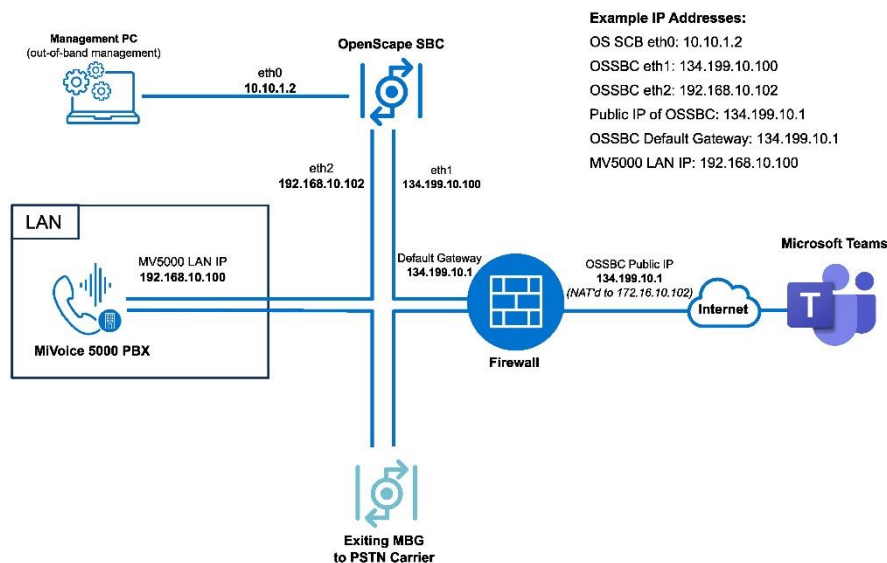


Figure 4: Multiple-Arm Configuration: Firewall NAT Mode

Note that an MBG server cannot be used with integrations involving MIV5000 platform. In this case, the PSTN point can be directly connected to the MiVoice 5000 server or through the MiVoice 5000 SBC.

The following figures depict the multi-arm configurations without an MBG server.

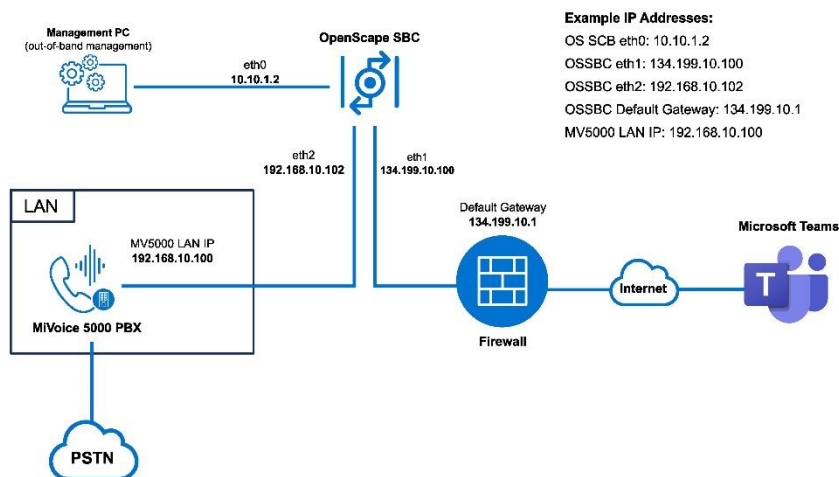


Figure 5: Multiple-Arm Configuration - Firewall Bridged Mode, without MBG

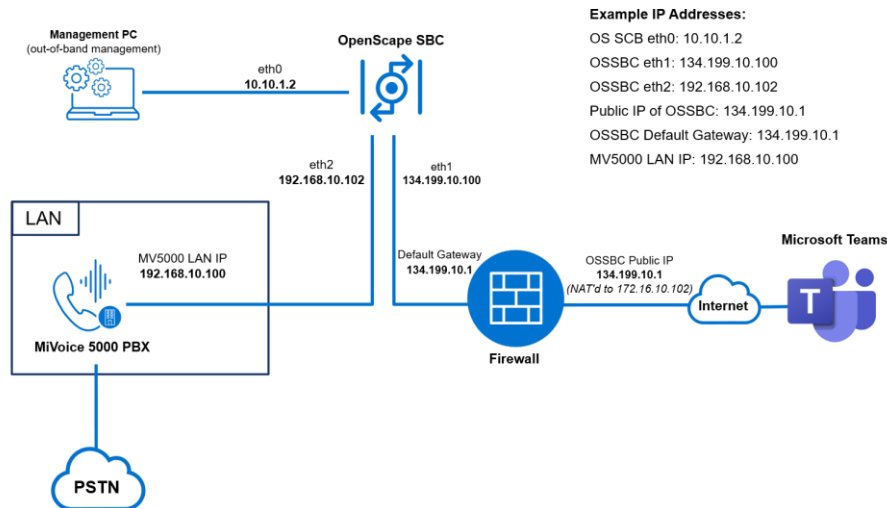


Figure 6: Multiple-Arm Configuration: Firewall NAT Mode, without MBG

2.2.3 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

2.3 SOFTWARE VERSIONS

PRODUCT	MINIMUM SOFTWARE VERSION
MiVoice 5000	8.2
IP Phone 69XXw	SIP 6.3.3.57
OpenScape SBC	11.0 (11 R0.05.00)
Microsoft Teams Web Client / Desktop Client / Mobile clients Android and iOS	V2

3 CONFIGURING THE MIVOICE 5000 SERVER

3.1 PREREQUISITE

Ensure sufficient MiVoice 5000 Internet Links are available and assigned to the MiVoice 5000. Internet Links can be verified in the menu **Telephony service>System>Info>Licenses**.

The number of licenses in the Internet Links field denotes the maximum number of Internet Links sessions that can be configured in MiVoice 5000 for use with all service providers, applications, and SIP trunking devices.

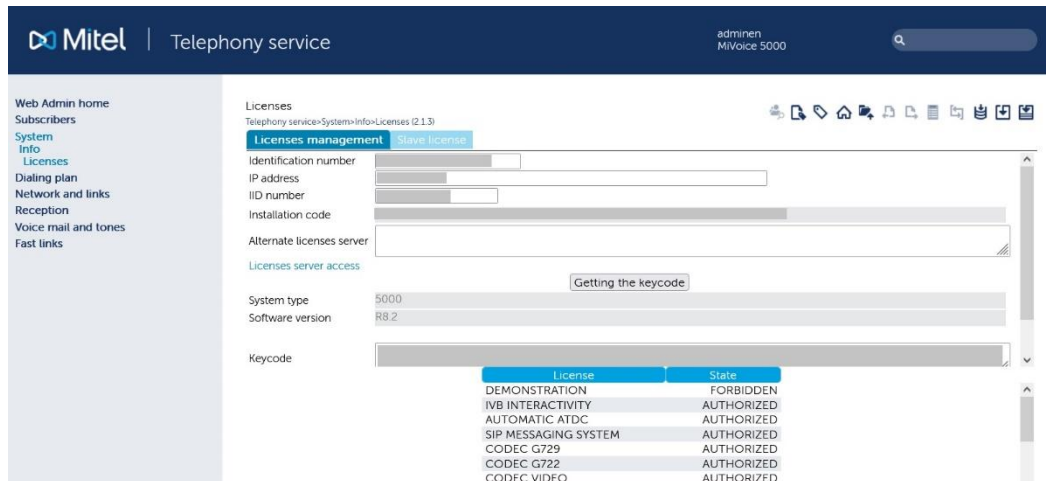



Figure 7 – MiVoice 5000 Licenses Menu

For more information on the MiVoice 5000 Web Admin, refer to the document **Mitel 5000 Server – Operating Manual**.

3.2 CONFIGURING TRUNK GROUP

This section describes how to configure the **Trunk Attributes** to direct incoming calls to an answer point in the MiVoice 5000 system.

Menu **Telephony service>Network and links>Network>Trunk groups>Names**

- Enter a name for the new trunk in one of the empty fields **Trunk group**.
- Click the Trunk Group link corresponding to the newly created trunk to access the Characteristics menu.
- Select **Trunks groups>Characteristics** which redirects directly to the configuration of the trunk signaling characteristics
- Check that the Signaling characteristics are as followed:
 - Physical type: VOICE IP
 - Nature: BOTHWAY
 - Signaling type: SIP
 - Subtype: STANDARD
- Click the Characteristics button.
The Web Admin displays the trunk characteristics.
- Click the  button to switch to the advanced mode.

- Configure the characteristics as followed:

Field	Action
Protocol	In the dropdown menu, select the TLS option.
SIPS support	Enable the option.
Proxy n° 1	Enter the IP address of the OS SBC. A new field appears. In the port field, enter the port dedicated to. The default port is 5061.
Audit out of speech	Enable the option.
Identity sending management	Under this section: <ul style="list-style-type: none"> • Enable the number (PAI) in E.164 format option. • Enable the update of name/number (UPDATE) option. • Enable the number (To) in E.164 format option.
Name Management	Enable the option.
Support PRACK (100rel)	Disable the option.
Priority calls if transit	Enable the option.
Incoming digit translator number	Enter a number according to the configuration. This parameter requires configuring other menus of the MiVoice 5000 Web Admin. Refer to section 3.3 – Configuring Dialing Plan .
Transfer to	In the dropdown menu, select the Disabled option.
CAC IP Address	Enter the MiVoice 5000 IP Address.

3.3 CONFIGURING DIALING PLAN

This document assumes that there is already a PSTN carrier configured on the MiVoice 5000.

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 MiVoice 5000 user who wants to call that Microsoft Teams user will dial "17025551212". For suggestions on ways to shorten this under certain conditions, see if there is a way to do it on MiVoice 5000.

Microsoft Teams users can dial external PSTN numbers using the prefix "1" and directly dial MiVoice 5000 extensions without using any prefixes.

Menu **Telephony service>Dialing plan>Direction name**

Figure 8 – Direction names menu

In one of the **Private direction** fields:

- Enter a name for the private direction. For example, OS SBC.
This action creates the new private direction.
- Click the hyperlink corresponding to the private direction for the OS SBC.
A pop up appears.
- Select the menu **Telephony service>Dialing plan>User dialing plan>Access to directions**.
- In the **Access code** field, enter the access code for outbound calls.

Menu **Telephony service>Dialing plan>Incoming call dialing plan>Access to directions**

- In the **By its name** dropdown menu, select the private direction for the OS SBC.
- In the **Access code** field, enter the same access code as in the menu **Telephony service>Dialing plan>User dialing plan>Access to directions**.

Menu **Telephony service>Network and links>Network>Translators>Outgoing: called party number**

- In the **Digit translator number** field, enter a translator number from 1 to 48.



Note: To see the first free number for this parameter, click the **Digital translator number** hyperlink.

- Click Select the item.
The MiVoice 5000 Web Admin displays the parameters of this translator number.
- In the parameters page:

- In the **Digit to translate** field, enter ABC.
- In the **to direction** dropdown menu, select the OS SBC direction.
- In the **and digits** field, enter 0ABC(18).

3.4 CONFIGURING CONFERENCE AND TRANSFER FUNCTIONS (OPTIONAL)

This section describes how to configure the **Transfer** to direct incoming calls to an answer point in the MiVoice 5000 system.

Menu **Telephony service>Subscribers>Rights>General settings, Rights tab.**

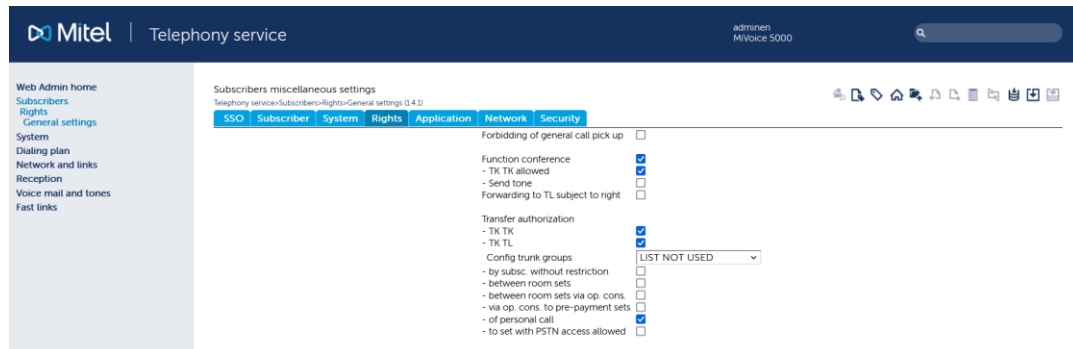


Figure 9 – Subscribers miscellaneous settings

CONFERENCE OPTIONS

For conferences, check that:

- The **Function conference** parameter is enabled,
- The **TK TK allowed** parameter is enabled.

TRANSFER OPTIONS

For transfer authorization, check that:

- The **TK TK** parameter is enabled,
- The **TK TL** parameter is enabled,
- The **Config trunk group** parameter is on LIST NOT USED.

4 INSTALLING OPENScape SBC

4.1 USING OVA FILE

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

4.1.1 PREREQUISITE

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

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

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



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

4.1.2 INSTALLING OPENScape SBC USING OVA FILE

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

- Log in to the VMWare ESXi Host Client.
- From the left side navigation tree, click on Virtual Machines.
- On the main page, click on Create / Register VM.
- Choose Select creation Type as Deploy a virtual machine from an OVF or OVA file.
- Click NEXT.
- Enter the virtual machine name on the Enter a name for the virtual machine field.
- Click on Click to select files or drag/drop to upload the OVF file.
- Select the image_oss-11.00.XX.YY.ova file that is downloaded in section **4.1.1 - Prerequisite**.
- Click NEXT.
- On the Select Storage page, select the datastore and click on NEXT.
- Configure the Deployment options.
 - Configure Network mappings:
 - Set LAN as an environment-specific value.
 - Set WAN as an environment-specific value.
 - Set Disk provisioning as Thick Lazy Zero.
 - Select Power on automatically.
- Click NEXT.
- 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.
- 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.

4.1.3 CONFIGURING IP ADDRESS



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



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.

To configure the default IP address:

- Log in to the SBC server as a root user. For information on default user name and password, refer to section **7.2 – Default User credentials for Openscape SBC**.



Note: The SBC server uses the QWERTY keyboard layout. To switch to the AZERTY layout, log in to the SBC server as a root user. Then enter the following command:

localectl set-keymap fr

- 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.*
- 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.

- Log in to the SBC GUI with the first IP address configured (For example, `https://10.10.1.2/`) as **administrator**.
- Navigate to the Network/Net Services > Settings.

The Network/Net Services pop-up window appears.

- 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 section **2.2 - Deployment Scenarios** for comparison with your actual deployment IP addresses.

- On the Core realm configuration panel:

Click the Add button.

Configure the IP address as 10.10.1.2. This parameter is environment specific, for the management.

Configure the Subnet mask as 255.255.255.0. This parameter is environment specific.

- On the Access and Admin realm configuration panel:
 - Click the Add button.
 - Configure the IP address as 176.16.10.102. This parameter is environment specific, for the DMZ.
 - Configure the Subnet mask as 255.255.255.0. This parameter is environment specific.
 - Repeat the steps for the IP address and Subnet mask for the LAN.
- On the Routing panel, set Default gateway address as 176.16.10.1. This parameter is environment specific.
- Click Ok and then click on Apply Changes.
- A pop-up window appears for the system restart; click OK on all the pop-up windows.

4.1.4 VERIFYING SBC SOFTWARE STATUS



Note: It is recommended to verify the software status 10 minutes after the SBC installation.

To verify the SBC software status:

- Log in to the SBC server as root.
 - Execute the following command to change the permission to root:
 - su
 - Execute the following command to verify the status of the SBC software:
 - pmc show
- The status of the software must be as follows:
- **Status: STABLE**

To verify the SBC status in GUI:

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

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

4.2 USING OVF FILES

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

4.2.1 PREREQUISITE



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

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

- Ensure that you have downloaded the latest available vApps_oss-11.00.XX.YY.zip package from the Software Download Center.
- The server hardware is installed.

- The VMware and vSphere Host client is operational.



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

4.2.2 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 section 2.2 - Deployment Scenarios.

To generate the ISO image:

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

The OSS USB Stick Setup window is displayed.

- Configure the OSS USB Stick Setup.
 - 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.



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.

- Configure the SBC Network Configuration:
 - From the Hardware Type drop-down menu, select Virtual OSS 20000.
 - Set Hostname as an environment-specific value.
 - 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.

Set the IPv4 address as 10.10.1.2. This is an environment specific value.
Set the IPv4 netmask as 255.255.255.0. This is an environment specific value.
Set the IPv4 gateway as 172.16.10.1. This is an environment specific value.
From the Interface dropdown menu, select WAN Interface.

Set the IPv4 address as 172.16.10.102. This is an environment specific value.

Set the IPv4 netmask as 255.255.255.0. This is an environment specific value.

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.

4.2.3 INSTALLING SBC USING OVF FILE

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

- Extract the vApps_oss-11.0X.YY.ZZ.zip file. The vApps_oss-11.0X.YY.ZZ folder is generated.
- Log in to the VMWare ESXi Host Client.
- From the left side navigation tree, click on Virtual Machines.
- On the main page, click on Create / Register VM.
- Choose Select creation Type as Deploy a virtual machine from an OVF or OVA file.
- Click NEXT.
- Enter the virtual machine name on the Enter a name for the virtual machine field.
- Click on Click to select files or drag/drop to upload the OVF file.
- Navigate to the vApps_oss-11.0X.YY.ZZ/vApps/OSS-20000 folder.
- Select both the OSS.ovf and OSS-disk1.vmdk files.
- Click NEXT.
- On the Select Storage page, select the datastore.
- Click NEXT.
- Configure the Deployment options.
 - Configure Network mappings:
 - Set LAN as an environment-specific value.
 - Set WAN as an environment-specific value.
 - Set Disk provisioning as Thin.
 - Deselect Power on automatically.
- Click NEXT.
- 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.

4.2.4 VERIFYING SBC SOFTWARE STATUS

To verify the SBC software status, refer to section **4.1.4 - Verifying SBC Software Status**.

5 CONFIGURING OPENScape SBC

This section describes the configuration required for connecting the OpenScape Session Border Controller (OSSBC) with MiVoice 5000 and Microsoft Teams. For the OpenScape SBC configurations required for Emergency Calls, refer to Configuring an E911 Solution. The instructions provided apply to both single-arm and multi-arm deployment scenarios, unless clearly stated otherwise. For more information, refer to section **2.2 - Deployment Scenarios**. 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 section **7.2 - Default User Credentials for Openscape SBC**. For restrictions and known issues, refer to section **7.1 - Restrictions and Known Issues**.

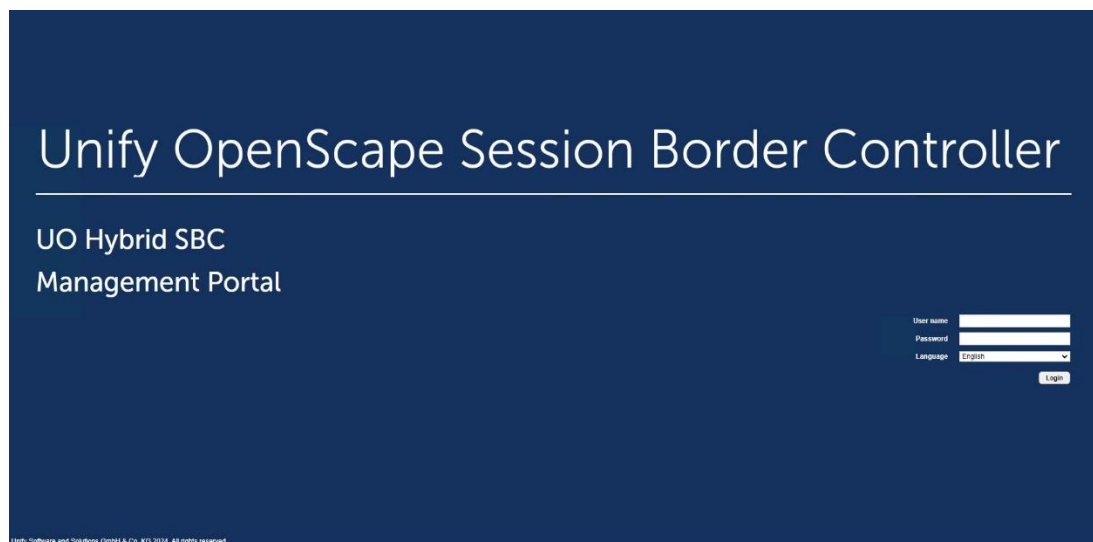


Figure 10: OpenScape SBC Login Page

5.1 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 change such as adding a VPN or extra IPs to network interfaces etc.), DNS, Gateway and Timezone.

5.1.1 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:

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



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

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | **DNS** | NTP | Traffic Shaping | QoS

Client

Refresh DNS

DNS server IP address **Add** Alias **Add**

Delete **Delete**

Server

☒ **Enable DNS server** **DNS configuration**

☐ **Enable customization** **Administer custom files**

Figure 11: Enabling the DNS Server

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

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings License Branding

General

License server License server port

Hardware ID

Logical ID

Advanced Locking ID

Figure 12: Generating ALI

- 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.

5.1.2 PROCEDURE

To verify the licenses:

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

Administration.

The **System** window pops up.

- Under **License Information**, do the following:
 - 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
 - Click **Upload** to upload the licenses.
- 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 section 5.1.1 - Prerequisite.

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 13: 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, refer to section 6.5 - Configuring Direct Routing.

5.2 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 MV5000 subnet (access to MV5000).
- A second one for communication with Internet (access to Microsoft Teams).

For more information, refer to section **2.2 – Deployment scenarios**.

5.2.1 PREREQUISITE

- To configure the SIP-UDP, SIP-TCP and SIP-TLS values, you must select the **Standalone with internal SIP Stack** option from the **Comm System Type** drop-down menu, under VoIP > SIP Server Settings.
- To avoid network delays, you have ensured that the value in the SSP OPTIONS timeout (ms) field under Timers and Thresholds is 5000.
- For the single arm configuration, it is recommended to create a whitelist of the IP addresses for the system management to protect the access via SSH and Web. For more information, refer to the document [OpenScape SBC V11 Security Checklist](#).

For more information, refer to section **5.9 – Configuring SIP Server Settings**.

5.2.2 PROCEDURE

- Log in to the SBC local management portal using the local administrative username and password. Refer to section **7.2 – Default User Credentials for Openscape SBC**.
- Navigate to the **Network/Net Services > Settings** tab in the navigation tree under **Administration**.

The **Network/Net Services** window pops up.

- Under the **Physical Network Interface** area, configure the following depending on the deployment:
 - Single-arm deployment
 - 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.

- Multi-arm deployment

Ensure that the following options are **Enabled**: eth0, eth1, 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 5000.

- Optionally, under Interface Configuration > Core realm configuration:

- Single-arm deployment:

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

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



- Multi-arm deployment:

The Core realm configuration for the interface (i.e. eth0) is completed during the installation. Ensure that:

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

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

Settings	Action
Type	<p>From the drop-down menu, select from the following options:</p> <p>Single-arm deployment:</p> <ul style="list-style-type: none"> • For Internet access, select SA Main IPv4 <p>Multi-arm deployment:</p> <ul style="list-style-type: none"> • 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.
Interface	<p>Single-arm deployment: Leave the default setting (eth0).</p> <p>Multi-arm deployment: Select the network interface. For example, eth1.</p>

Settings	Action
IP address	For accessing Microsoft Teams, enter the Access IP of the SBC located in the same subnet with the firewall.  Note: Multi-arm deployment: see note below the table for configuring this setting for MiVoice 5000.
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: Multi-arm deployment: When configuring the SIP TLS for MV5000, ensure that it matches the corresponding value configured in the MV5000 network elements. For example, enter 5061 for both the TLS port configuration in MV5000 and the corresponding SBC setting.


- Repeat the previous step to add the **MiVoice 5000** network interfaces.



IMPORTANT: For MV5000, the IP address setting needs to be configured as follows:

Enter the IP for accessing MV5000. For more information, refer to section 2.2 – Deployment scenarios.

- 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.
Realm	Select access

Settings	Action
Signaling network ID	Select the appropriate signaling network ID that you created previously under Access and Admin realm configuration . For example, Main-Access-IPv4.
Media network ID	Select the appropriate media network ID that you created previously under Access and Admin realm configuration . For example, Main-Access-IPv4.

- Repeat the previous step to add the realm profile for MiVoice 5000.
- Under **Routing**, enter the gateway IP address for Main IPv4 in the **Default gateway address** field.
- This step is optional in a single arm configuration, but mandatory for a multi arm configuration.

To create a route to a destination other than the default gateway, 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.

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



Note : For more information, refer to the [OpenScape SBC V11 Configuration Guide](#).

- If you have selected the **Enable redundancy** checkbox:
 - Enter the default gateway IP address in the **Core link connectivity check IP address** field.
 - Check the **Enforce call context mirroring based on LAN MTU size** checkbox.
- Click OK.
- Click Apply Changes to apply this configuration.

5.3 CONFIGURING THE NETWORK/NET SERVICES DNS SERVER

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

- In the SBC local management portal, navigate to **Network/Net Services > DNS** tab in the navigation tree under **Administration**.
- In the **DNS server IP address** under the Client area, enter the DNS server of the firewall network and click **Add**.
- Optionally, if your PSTN provider uses a specific DNS server, enter the DNS server's IP address in the **DNS Server IP Address** field and click **Add**.



Note: You can add up to 3 DNS servers.

- Optionally, to manually refresh the DNS client, click **Refresh DNS**.
- Click **OK** to save the configuration.
- Click **Apply Changes**.

Figure 14: DNS Tab

5.4 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. For more information, refer to

the Microsoft document [List of Participants - Microsoft Trusted Root Program](#).

5.4.1 GETTING CERTIFICATES AND KEY FILES

Perform the following procedure if the third party is CA:

- Get the certificates from third party authority.
- Import the certificates to OpenScape SBC. To import the certificates, refer to section **5.4.2 – Importing OpenScape SBC Certificates**.



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.

In some cases, the setup requires to manually generate a CSR file to ask for the certificate.

5.4.2 IMPORTING OPENScape SBC CERTIFICATES

To import the OpenScape SBC certificates:

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

The **Security** window pops up.

- Click **Certificate management**.

The **Certificate Management** window pops up.

- Scroll down to locate the **Certificates Upload** area and configure the following:
 - Under **CA certificates**, click **Choose File**, select the CA certificate file, click **Open**, and then click **Upload** to upload the CA certificate file.
 - 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.
 - Under **Key files**, click **Choose File**, select the private key file, click **Open**, and then click **Upload** to upload the private key certificate file.
- Scroll up to locate the **Certificate Profiles** area and click **Add** to configure the certificate profile.
- In the **Certificate Profile** window that opens, configure certificate profile for **Microsoft Teams**.
 - 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 uploaded during this procedure.

Field	Action
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.
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.

- Under **Validation**, configure the following:
 - In the Certificate **Verification** dropdown menu, select **Full**.
 - Check the **Revocation Status** box.
 - Check the **Identity Check** box.
- Under **Renegotiation**, if checked, uncheck the **Enforce TLS session renegotiation** option.
- Under **TLS version**, from the **Minimum TLS version** drop-down menu, select **TLS V1.2**.
- Under **Cipher Suites**, configure the following:
 - From the **Perfect Forward Secrecy** drop-down menu, select **Preferred PFS**.
 - From the **Encryption** drop-down menu, select **Preferred AES-128**.
 - From the **Mode of Operation** drop-down menu, select **Preferred GCM**.
- Click **OK**.
- In the **Certificate Management** page that opens, click **OK** and then click **Apply Changes** to save the certificate configuration.

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.

5.5 CONFIGURING FIREWALL

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

Depending on the system deployment (single-arm or multi-arm), note the prerequisites for the configuration steps. For more information, refer to section **2.2 – Deployment scenarios**.

To configure the firewall settings, refer to the section **5.5.3 – Firewall Settings Configuration**.

5.5.1 PREREQUISITE (SINGLE-ARM DEPLOYMENT)

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

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

- Add a network interface in your firewall for accessing the local network.
- Create a new DMZ LAN interface, to access the network where MV5000 is located.
- Configure network equipment to route the traffic between new DMZ LAN interface and the local network (MV5000).
- Allow traffic between the DMZ LAN interface and the local network, and vice versa.
- Create firewall rules to allow traffic between MV5000 – SBC and vice versa for the TLS port assigned (i.e., 5061) and the RTP port range. The TLS ports depend on the configuration of SIP ports used by MiVoice 5000 (refer to the section **5.8.4 - MiVoice 5000 Remote Endpoint configuration**). RTP ports depends on configuration of RTP ranges (refer to section **5.10 - Configuring Port and Signaling Settings**). The default ports are 20000-49999.
- 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) (refer to the section **5.8.4 - MiVoice 5000 Remote Endpoint configuration**) and by access realm SIP ports of SBC (refer to section **5.2 -Configuring Network/Net Services**). The RTP ports depend on the configuration of RTP ranges; (refer to section **5.10 - Configuring Port and Signaling Settings**). 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.

5.5.2 PREREQUISITE (MULTI-ARM DEPLOYMENT)

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

- 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. Refer to section **5.8.5 - Microsoft Teams Remote Endpoint configuration** and by access realm SIP ports of Session Border Controller. Refer to section **5.2 - Configuring Network/Net Services**.
- The RTP ports depend on the configuration of RTP range. Refer to section **5.10 - Configuring Port and Signaling Settings**. 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.

5.5.3 FIREWALL SETTINGS CONFIGURATION

This section describes how to configure the firewall settings based on your system deployment. For more information, refer to section **2.2 - Deployment Scenarios**.



Note: In single-arm deployment, configure the firewall settings for each of the following:

- **MiVoice 5000**
- **Main, for the Internet access (Microsoft Teams)**

In multi-arm deployment, configure the firewall settings for Main only.

To configure the firewall settings:

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

The **Security** window pops up.

- Click **Add**.

The **Firewall Configuration** window pops up.

- 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 MV5000.

- 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.

- Check the **Enable port forwarding** checkbox.

- Under Incoming networks connections:

- 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 5000 configuration, block the SNMP incoming network connection.

HTTPS

SSH

ICMP

SIP

TLS

RTP/sRTP



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

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

ICMP

SIP

TLS

RTP/sRTP

- Under the **External Firewall** area, check the **External Firewall** checkbox.

- In the **Firewall external IP** field, enter the external firewall IP address.



IMPORTANT: For the MiVoice 5000 configuration, the firewall's external IP must match the corresponding IP configured in MiVoice 5000 (IP of

firewall's LAN interface). In the main configuration, the firewall's external IP is the public IP address of the firewall.

- Click **OK**.

5.6 ENABLING CODEC SUPPORT FOR TRANSCODING

You might need to enable Codec support for transcoding if there is a different Codec selection between MiVoice 5000 and Microsoft Teams.

To enable Codec support for transcoding:

- In the SBC local management portal, navigate to **Features** in the navigation tree under Administration.
- Select the **Enable Codec Support for Transcoding** check box on the page that opens.
- Click **Configure**.
Clicking on the **Configure** option launches the Codecs window where various checkboxes for codecs, such as OPUS, can be enabled or disabled.
- 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.

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

5.7 CONFIGURING MEDIA PROFILES



Note: This configuration applies to both single-arm and multi-arm deployments. For more information, refer to section 2.2 - Deployment Scenarios.

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

- Microsoft Teams
- MiVoice 5000

To configure the media profiles:

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

The **Media Profiles** window pops up.

- 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.
RTP/RCP Multiple in offer	Select the RTP/RCP Multiplex in offer checkbox.
SRTP configuration	Select SDES Both .
RTCP configuration	Do the following: <ul style="list-style-type: none"> 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. The default value is 4 seconds.
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 Click Add to add it to the bottom of the list of codecs for this media profile.

- Click **OK**.
- 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**, enable **Support ICE with Full**. If it is **ON**, then select **Support ICE with Lite**. This ensures optimal configuration for the system without any unnecessary complications.

Category	Field	Description
General	Name	Enter a Media Profile name. For example, Teams.
	Media protocol	Select SRTP only from the drop-down list.

Category	Field	Description
	Support ICE	<p>Check the Support ICE checkbox.</p> <p>The configuration of this option depends on the deployment:</p> <ul style="list-style-type: none"> 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. <p> Note: For more information on the deployment scenarios, refer to section 2.2 – Deployment Scenarios.</p>
	RTP/RTCP Multiplex in offer	Select the RTP/RTCP Multiplex in offer checkbox.
Codec configuration	Allow unconfigured codecs	Enable the Allow unconfigured codecs option.
	Codec	<p>Select G722 8 kHz - 64 kbps from the drop-down list.</p> <p>Click Add to add it to the bottom of the list of codecs for this media profile.</p> <p>Repeat the process for the codec G711A 8kHz - 64 kbps (for Europe) or G711U 8kHz - 64 kbps (for US-NA).</p> <p> Note: Make sure the G722 Codec priority is 1. Use the Move up and Move down buttons to rearrange the codec order.</p>

- Click **OK**.
- To enable the **MiVoice 5000 Media Profile**, under Media Profiles, click **Add** and configure the following:

Category	Field	Description
General	Name	Enter a Media Profile name. For example, MV5000.
	Media protocol	Select Strict Pass-Thru from the drop-down list.

- Click **OK**.
- 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.

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

5.8 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)

- Create one SIP Service Provider Profile for MiVoice 5000: refer to section **5.8.2 - MiVoice 5000 SIP Service Provider Profile configuration**.
- Create one SIP Service Provider Profile for Microsoft Teams: refer to section **5.8.3 - Microsoft Teams SIP Service Provider Profile configuration**.

Configure Remote endpoints settings

- Create one MiVoice 5000 remote endpoint: refer to the section **5.8.4 - MiVoice 5000 Remote Endpoint configuration**.
- Configure three remote endpoints for the Microsoft Teams main access interface: refer to the section **5.8.5 – Microsoft Teams Remote Endpoint configuration**.



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.

5.8.1 PREREQUISITE

- Go to the menu VoIP > SIP Server Settings. In the **Comm System Type** drop-down menu, select the **Standalone with internal SIP Stack** option from.
- Under **Timers and Thresholds**, ensure that the value in the **SSP OPTIONS timeout (ms)** field is **5000**. This parameter aims at avoiding network delays.

For more information, refer to section **5.9 - Configuring SIP Server Settings**.

5.8.2 MIVOICE 5000 SIP SERVICE PROVIDER PROFILE CONFIGURATION

The following configuration must be applied to the MV5000 Remote Endpoint Profile to handle both Microsoft Teams -> MV5000 calls as well as Microsoft Teams -> PSTN Calls.

- 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.

- Check the **Enable Remote Endpoints** checkbox.
- Click **Configure** next to the Enable Remote Endpoints checkbox.
- The **Remote endpoints** window pops up.
- Under the SIP Service Provider Profile area, click **Add**.

The **SIP Service Provider Profiles** window pops up.

- In the **Name** field, enter **MV5000SSP**.
- Under **SIP Privacy**, from the **Privacy Support** drop-down menu, select **Full**.
- Under **SIP User Agent**, in the **SIP User Agent towards SSP** field, select **Passthru** from the drop-down list.
- Under **Outgoing SIP manipulation**, click **Manipulation**.
- The **SIP SP Manipulation** window pops up.
 - Click **Add**.
 - In the **Matching digits** field, enter **+1**.
 - In the **Min/Max Length** field, enter **5/14**.
 - In the **Number of digits to delete** field, enter **2**.
 - From the **Call-type** drop-down menu, select **SIP-Provider**.
 - This single entry will handle both Microsoft Teams > MV5000 extensions (4-digits) and Microsoft Teams > PSTN calls. Since MS Teams inserts a "+1" on outgoing calls, this rule will intercept calls going to MV5000 that fit the pattern of "+1" plus anywhere from 3 to 12 digits. Additionally, it will strip the first two digits ("1") before sending to MV5000.



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 MV5000, which rings extension 2077.

Microsoft Teams user dials "918007221301". Microsoft Teams sends "+1918007221301". OSSBC removes first two digits and passes "918007221301" to MV5000, which routes the call to the PSTN.

- Click **OK** to save the settings. You are directed back to the **SIP Service Provider Profile** window.
- Under **Incoming SIP Manipulation**, in the **Calling Party Number** field, select **From header user and display name part** from the drop-down list.
- Under **TLS**, in the **TLS Signaling** field, select **Pass-Thru** from the drop-down list.
- Click **OK** to save the configuration.
- Click **OK**.
- Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

5.8.3 MICROSOFT TEAMS SIP SERVICE PROVIDER CONFIGURATION

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

- 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.

- Check the **Enable Remote Endpoints** checkbox.
- Click **Configure** next to the Enable Remote Endpoints checkbox.

The **Remote endpoints** window pops up.

- Under the **SIP Service Provider Profiles** area, click **Add**.
- The **SIP Service Provider Profile** window pops up.
- Locate the **General** area.
- In the **Name** field, enter **TeamsSSP**.
- From the **Default SSP Profile** drop-down menu, select **MSTeams**.
- Locate the **SIP Privacy** area. From the **Privacy Support** drop-down menu, select **Full**.
- Under the **SIP Service Address** area, check the **Use SIP Service Address for identity headers** checkbox.
- In the **SIP service address** field, enter the FQDN address assigned to SBC.



Note: The FQDN you enter here must match the one configured in Microsoft Teams. For more information, refer to section 6.5 - Configuring Direct Routing. The current diagram in section 2.2.1 – Single arm configuration does not include the SBC's FQDN. Therefore, it is important to ensure that the FQDN resolves correctly to the public IP of the SBC, such as in sbc.example.com.

- 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**
- Locate the **SIP User Agent** area. From the **SIP User Agent towards SSP** drop-down menu, select **Passthru**.
- 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)**
- Under **TLS**, from the **TLS Signaling** drop-down menu, select **Transport=tls**.
- Under **SIP Connect**, select the **Send user=phone in SIP URI** checkbox.
- Click **OK** to save the configuration.
- Click **OK**.
- Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

5.8.4 MIVOICE 5000 REMOTE ENDPOINT CONFIGURATION



Note: Before continuing, make sure a MiVoice 5000 SIP Service Provider Profile exists in the configuration.

Follow the steps below to configure a MiVoice 5000 remote endpoint.

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

The **Features** window pops up.

- Check the **Enable Remote Endpoints** checkbox.
- Click **Configure** next to the Enable Remote Endpoints **checkbox**.

The **Remote Endpoints** window pops up.

- Scroll down to locate the **Remote endpoint configuration** area.
- Click **Add**.

The **Remote Endpoint configuration** window pops up.

- Under the **Remote Endpoint Settings** area, configure the following:

Menu item	Action
Name	Enter a unique name for the MiVoice 5000 remote endpoint. For a MV5000 remote endpoint configuration, enter a name such as MV5000RE .
Type	From the drop-down list, select SSP .
Profile	From the drop-down list, select the MiVoice 5000 profile. For example, MV5000.
Access realm profile	From the drop-down list, select the MiVoice 5000 access realm profile.
Core realm profile	From the drop-down list, select the Main-Core- Realm-ipv4 profile.

- Under the **SSP OPTIONS** area:
 - Select the **Enable SSP connectivity check** checkbox.
 - In the **OPTIONS interval (sec)** field, enter **60**.



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

- Under the Remote Location Information area, from the Signaling address type drop-down list, select **IP address or FQDN**.
- 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	Example
Remote URL	Enter the IP of the remote endpoint for MiVoice 5000.	The URL can be entered as IP address (IPv4/I Pv6), as domain (FQDN or domain name) or as Logical-Endpoint-ID.	192.168.10.100, as shown in Figure 1, in section 2.2 - Deployment Scenarios .
Remote port	Enter the remote port for communication between MV5000 and Microsoft Teams.	Default port: 5061	
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 5000 system.	Default option: TLS	

- Under **Media Configuration**, from the **Media profile** drop-down, select the media profile for the MV5000.
- Click **OK**.
You are directed back to the **Remote endpoint configuration** window.
- Under **Remote Location Identification/Routing**, configure 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.



Note: The port range is between 50000 and 54999.

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

5.8.5 MICROSOFT TEAMS REMOTE ENDPOINT CONFIGURATION



Note: Before continuing, make sure a Microsoft Teams SIP Service Provider Profile exists in the configuration.

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

- 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.

- Check the **Enable Remote Endpoints** checkbox.
- Click **Configure**.

The **Remote Endpoints** window pops up.

- Scroll down to locate the **Remote endpoint configuration** area.
- Click **Add**.

The **Remote Endpoint configuration** window pops up.

- Under the **Remote Endpoint Settings** area, configure the following:

Menu item	Action
Name	Enter a unique name for the remote endpoint. For example, TeamsRE .
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 access realm profile for internet.
Core realm profile	From the drop-down list, select the Main-Core- Realm-ipv4 profile .

- Under the **SSP OPTIONS** area:
 - Select the **Enable SSP connectivity check** checkbox.
 - In the **OPTIONS interval (sec)** field, enter 60.
- Under the **Remote Location Information** area, from the **Signaling address type** drop-down list, select **IP address or FQDN**.
- 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 or domain: sip.pstnhub.microsoft.com	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 .	

- 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.
- Under **Media Configuration**, from the **Media profile** drop-down menu, select the media profile for Microsoft Teams. For example, Teams.
- Click **OK**.
You are directed back to **Remote Endpoint configuration** window.
- 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.
- Click **OK**.
- Click **Apply Changes** in the main window to confirm the changes to the OpenScape SBC appliance.

If needed, repeat the steps in the **Remote Endpoint Configuration** menu to add two more Microsoft Teams remote endpoints:

- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com_

5.9 CONFIGURING SIP SERVER SETTINGS

When in **Standalone with Internal SIP Stack** mode, 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 5000 and Microsoft Teams.

To accomplish this, you must create one group for MiVoice 5000 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 section 2.2 – Deployment scenarios.

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



Note: For the OpenScape SBC V11R0.6.0, when you select **Standalone with internal SIP stack**, set the **SIP-TCP** and **SIP-TLS** ports in the core realm configuration to 0. For more information, refer to section 5.2 - **Configuring Network/Net Services**.

- To avoid network delays, ensure that the value in the **SSP OPTIONS timeout (ms)** field under **Timers and Thresholds** is **5000**.
- Under **Direct Routing Configuration**, click **Configure**.
- The Direct Routing window pops up.
- Create the Microsoft Teams Group:
 - In the **Group name** field, enter the group name for Microsoft Teams. For example, MTG.
 - Click **Add group**.
 - The **Group selected** field displays the created group name.
 - From the **Group for** drop-down menu, select **MS Teams**.
 - Locate the **Endpoints for Group '[Group name]'** area.
 - From the **Endpoints** drop-down menu on the right side, select the Microsoft Teams endpoint(s) created in section 5.8.5 - **Microsoft Teams Remote Endpoint configuration** and click **Add**.
 - Click **OK**.
- Create the MiVoice 5000 Group:
 - In the **Group name** field, enter the group name for MiVoice 5000. For example, MV5000.
 - Click **Add group**.
 - The **Group selected** field displays the created group name.
 - From the **Group for** drop-down menu, select **SSP**.
 - Locate the **Endpoints for Group '[Group name]'** area, as depicted in the following figure.

Direct Routing

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Routing groups

Group settings

Group name: Add group

Group selected: M5000G Delete group

Group for: SSP endpoints

Relates to group: MTG Add to routing table

Routing table

Delete routing

	A group	B group
1	M5000G	

Endpoints for group "M5000G"

Endpoints: MV5000RE Add Delete

Endpoint	IP address or FQDN	Port	Transport	Priority	FQDN Routing	Regex
1 MV5000RE	10.102.19.2	5061	TLS	1		

OK Cancel

Figure 15: MiVoice 5000 Direct Routing Group

- From the **Endpoints** drop-down on the right, select the MiVoice 5000 group, such as **MV5000**, and click **Add**.
 - Click **OK**.
 - Relate the MiVoice 5000 group to the Microsoft Teams group:
 - From the **Relates to Group** drop-down menu, select the Microsoft Teams group, such as **Teams**.
 - Click **Add to routing table**.
 - The endpoint is added to the Routing table.
 - Optional: To modify the details of a routing group, such as changing the priority or adding a regex, double-click on the entry to modify under the **Routing table**.
 - Click **OK**.
- 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.

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

5.10 CONFIGURING PORT AND SIGNALING SETTINGS

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

- In the SBC local management portal, navigate to **VoIP > Port and Signaling Settings** in the navigation tree under **Administration**.
- Under **Port Range**, do the following:
 - 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.
 - 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 suggested values for Min and Max are between 20000 and 25999



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

- Under Signaling and Transport Settings, do the following:
 - In the **TCP connect timeout (sec)** field, enter the time in seconds before an outgoing attempt to connect will be stopped.
 - In the **TCP send timeout (sec)** field, enter the time in seconds after a TCP connection will be closed if it is not available.
 - 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.

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).

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.

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

The screenshot shows the 'VOIP' configuration window with the 'Port and Signaling Settings' tab selected. The window contains several sections for configuring ports and signaling parameters.

Port Range

- Media independent RTP ports: Port min (10000), Port max (49999), Time to live (sec) (180)
- ☐ Enable Media Specific Ports
- Audio Port min (10000), Audio Port max (37499)
- Video Port min (37500), Video Port max (49999)
- Subscribers dynamic SIP ports: Port min (10000), Port max (49999)
- Remote Endpoints Static SIP Ports: Port min (50000), Port max (54999), Number of reserved SIP ports (0)
- TCP/BFCP ports: Port min (10000), Port max (14999)

Signaling and Transport Settings

- TCP connect timeout (sec) (4), TCP send timeout (sec) (3)
- TCP connection lifetime (sec) (660), ☐ TCP keep alive
- BFCP connection timer (min) (720)
- ☐ Maximal call session time (hr) (12)

Miscellaneous

At the bottom right, there are 'OK' and 'Cancel' buttons.

Figure 16 – Ports and Signaling Settings

5.11 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:

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

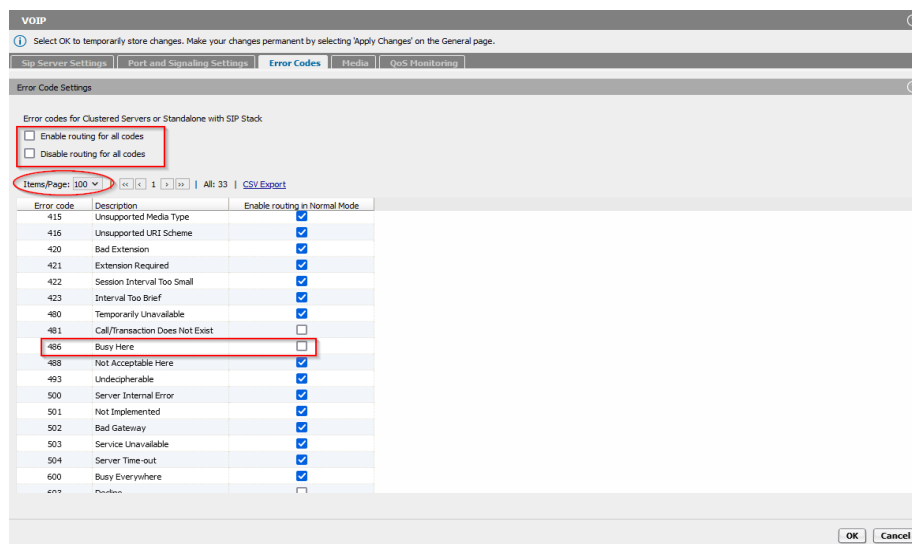


Figure 17: Error Codes configuration

6 CONFIGURING MICROSOFT TEAMS

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: 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.

6.1 PREREQUISITE

Ensure to have a valid Microsoft Teams admin account.

Ensure to 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.

In the Microsoft Teams administration portal (<https://admin.teams.microsoft.com>), add your domain. This process requires administrator rights in your domain, to perform the validation with Microsoft Teams.

6.2 CONNECTING OPENScape SBC TO DIRECT ROUTING

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

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



Note: For other parameters use the default value in the system, for more information, refer to the Microsoft document [Connect your Session Border Controller \(SBC\) to Direct Routing](#).

Table 5: Destination Configuration

Field	Sample Value
Enabled	Turn On
SIP signaling port	5061 This value must be same as the Microsoft Teams value (eth) configured in. Refer to section 5.2 -Configuring Network/Net Services .
Send SIP options	Turn Off

Field	Sample Value
Forward call history	Turn On
Forward P-Asserted-Identity (PAI) header	Turn On
Media bypass	Environment specific value. For information on deployment options, refer to section 2.2 - Deployment Scenarios .
Bypass mode	Always

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

6.3 VERIFYING SSP CONNECTIVITY STATUS

To verify the SSP connectivity status in OpenScape SBC:

- In the SBC management portal, navigate to **Administration > System Status**.
- On **SSP Status**, click **Show**. The **SSP connectivity Status** pop-up window is displayed.
- Ensure that the **SSP Trunk Names** (MiVoice 5000, Microsoft Teams, and PSTN) are displayed and the **Status** is shown in green as depicted in the following figure.

The screenshot shows the Unify OpenScape Session Border Control Management Portal. On the left, the 'Administration' menu is visible, with 'System Status' selected. The main panel shows the 'General - SBCBYOT' configuration page. A pop-up window titled 'SBCBYOT - SSP Connectivity Status - Google Chrome' is displayed, showing the 'SSP Connectivity Status' table. The table has the following data:

Status	SSP Trunk Name	Default Home DN	URI	SSP Connectivity Check	SSP Registration Status
Connected	MX-ONEtoSSP		sip:10.100.21.85:5061;transport=tls	Connected	Not Available
Not Available	CompanyFlex	+49199296000000003	sip:tel.t-online.de;transport=tls	Not Available	Registered
Connected	MX-ONEtoTeams		sip:10.100.21.85:5061;transport=tls	Connected	Not Available
Connected	Teams_SP3		sip:sip3.pstnhub.microsoft.com:5061;transport=tls	Connected	Not Available
Connected	Teams_SP2		sip:sip2.pstnhub.microsoft.com:5061;transport=tls	Connected	Not Available
Connected	Teams_SP1		sip:sip.pstnhub.microsoft.com:5061;transport=tls	Connected	Not Available

Figure 18: SSP Connectivity Status

6.4 ASSIGNING A PSTN NUMBER TO THE USER

- To assign a PSTN number to the user:
- In the Microsoft Teams admin center, navigate to **Users > Manage Users**.
- In the **Manage Users** page, select the user to update.
- Navigate to **Account > General Information**.
- Click **Edit**.
- In the **Phone number type**, select the **Choose the type of phone number** option from the drop-down list.

- In the **Assigned phone number** field, enter the Direct Routing number to assign to the user. For example, 17025551212.



Note: Avoid making any changes in the Phone Number Extension field.

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

6.5 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, refer to section **5.4 - Configuring Certificates**.



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

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

Table 6: Direct Routing Configuration

Field	Sample Value
SBC settings	
Add an FQDN for the SBC	The FQDN must be the FQDN address identifying the network domain for Microsoft Teams provided in the SIP service address field in Microsoft Teams SIP Service Provider Profile configuration.
Enabled	Turn On
SIP signaling port	5061 This value must be same as the Microsoft Teams value (eth) configured in section 5.2 -Configuring Network/Net Services .
Forward call history	Turn On
Forward P-Asserted-Identity (PAI) header	Turn On

Field	Sample Value
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, refer to section 2.2 – Deployment scenarios .
Bypass mode	Always
Preferred country or region for media traffic	Auto
Location based routing	Off
Gateway site ID	None
Proxy SBC	None

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

6.6 CONFIGURING VOICE ROUTES

Add and associate a voice route with the OpenScape SBC established in section **6.5 - Configuring Direct Routing**. Additionally, create a Dial number pattern for this voice route to facilitate a communication within the Microsoft Teams environment.

To configure voice routes:

- In the Microsoft Teams admin center, navigate to **Voice > Direct Routing**.
- Select **Voice routes**.
- Click Add. The following table lists a sample configuration:

Table 7: Voice Routes Configuration

Parameter	Sample Value
Add a name for your voice route	Enter a name for the voice route.
Description	Enter the name and description for the voice route.
Priority	Enter the priority of the voice route based on the number of voice routes. The default value is 1.
Dialed number pattern	Enter the dialed number pattern of the voice route. For example, <code>^\(+30[0-9]{10})\$</code> .
SBCs enrolled	<ul style="list-style-type: none"> Click Add SBCs to add an SBC. Select the SBC you want to add Click Apply.
PSTN usage records	<ul style="list-style-type: none"> Click Add PSTN usage to add the PSTN records. Click +Add. Enter the PSTN usage record. For example, MitelAth1. Select the PSTN usage record that you created. Click Save and apply.

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



Note: For more information on voice routes configuration, refer to the Microsoft documentation [Configure call routing for Direct Routing](#).

6.7 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:

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



Note: For more information on voice routing policy configuration, refer to the Microsoft documentation [Configure call routing for Direct Routing](#).

6.8 CONFIGURING USER'S VOICE ROUTING POLICY

To configure Microsoft Teams user voice routing policy:

- In the **Microsoft Teams admin center**, navigate to **Users > Manage users**.
- Select the user to configure the voice routing policy.
- Click the **Policies** tab. The policy entries are displayed.
- Select the policy and click on **Edit**.
- From the **Voice routing policy** drop-down list, select the voice policy created in section **6.7 -Configuring Voice Routing Policies**.
- Click **Apply** to assign the voice routing policy to the Microsoft Teams user.



Note: For more information about configuring users' voice routing policies, refer to the Microsoft document [Configure call routing for Direct Routing](#).

7 APPENDIX

7.1 RESTRICTIONS AND KNOWN ISSUES

The following table lists the restrictions and known issues when Microsoft Teams is integrated with MiVoice 5000 through OpenScape SBC.

Feature	Issue Description
User Impact (Product Limitations)	
Timer in Microsoft Teams	The timer of Microsoft Teams when someone answers a call does not start from 0. It seems that the timer starts during ringing.
Hold Information	Hold information not displayed in Microsoft Teams or the device, when the other party sets you on hold.
Delays Microsoft Teams	Occasionally, in Microsoft Teams users experience a consistent delay of 1-2 seconds when connecting the audio with MiV5000.
Clear Call Microsoft Teams	Occasionally the call is not cleared, when using android mobile app. The problem is not reproduced when using web, desktop, or iOS application. This should be addressed by Microsoft Teams support team.
Toggle Consult Calls	When using web Microsoft Teams, and the active call hung up, then the box to retrieve the held call disappears. You need to initiate a new call for the box to appear. This should be addressed by Microsoft Teams support team.
Microsoft 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.
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.
Call Forwarding Info	When making an external call with a device, 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.
Hung up During on Hold	MiVoice 5000 does not allow you to hung up the call, when the call is on hold.

Feature	Issue Description
Anonymous Calls	MiVoice 5000 does not support anonymous calls. You can either select to show the actual number or the business number.
Music on Hold	In MiVoice 5000 setting MOH without music, cannot be configured in a proper manner.
Recall During Park	MiVoice 5000 does not recall the device during Park if you hung up the device. A park call indication is shown on the device.
Conference up to 3 Parties	MiVoice 5000 supports conference calls up to 3 parties.
Call Pickup (Parallel Ringing)	You cannot create a call pickup group for parallel ringing in MiVoice 5000. This option is only available in the hunt group configuration.
Reject Calls	In MiVoice 5000 there is transfer to reception concept. Thus, when the Ignore button is selected, it will try to redirect the call and does not send Busy tone.
Hunt - Ring Groups	MiVoice 5000 does not support adding external numbers to hunt groups.
Emergency Calls	<p>In the emergency calls from Microsoft Teams users, the user location information provided by Microsoft is bypassed to the IP PBX in the SIP message inside SDP body for PIDF-LO. The ELIN code inside this message is not copied to the SIP PAI header which may be required by some emergency providers to retrieve the correct user location.</p> <p>The emergency calling is not supported when using Microsoft Teams web client. Microsoft Teams desktop application or mobile application could be used instead, based on the following URL for supported clients. For more information, refer to the official Microsoft Teams page for Emergency calling.</p>
Configuration Topics	
Anonymous Call PSTN	The PSTN provider used, does not accept incoming anonymous calls and replies with 403 – Forbidden.
PRACK SIP Message	PRACK SIP message is not supported by the PSTN provider used.
Hold – Retrieve	Hold – retrieve occasionally failed, when using SIP firmware 6.4.0.136. In the latest firmware the problem was not reproduced.
PAI Header	The PSTN provider used does not support PAI header in initial SIP INVITE message.

Feature	Issue Description
SIPS Support	The OpenScape SBC does not support SIPS support option, enabled by default in MiVoice 5000 when using TLS protocol.
G711 codec PSTN	The PSTN provider used prefers G711 coder, thus it was given priority to that codec in MiVoice 5000.
G722 codec MS Teams	Microsoft Teams prefers G722 codec, thus it was given priority 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 SIPOPTION 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.
Transcoding	The Openscape SBC transcoding feature is not part of the current solution with the MiVoice 5000.

7.2 DEFAULT USER CREDENTIALS FOR OPENScape SBC

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

USERNAME	PASSWORD
administrator	Asd123!.
root	T@R63dis
service	BF0bpt@x
guest	1cIENtk=

For information on OpenScape SBC Security Checklist, refer to the document [OpenScape SBC V11 Security Checklist](#).