



A MITEL
PRODUCT
GUIDE

Unify OpenScape Session Border Controller

OpenScape SBC V11 with Survivable Branch Appliance (SBA)

Installation Guide

July 2024

Notices

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

Trademarks

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

© Copyright 2024, Mitel Networks Corporation

All rights reserved

History of Changes

Issue	Date	Summary
1	10/2023	First issue of the guide.
2	07/2024	Rebranded to Mitel layout.

Contents

History of Changes	3
1. Introduction	6
1.1. About this Guide	6
1.2. Setup Requirements	6
2. Configuring SBA on Windows Server	8
2.1 Microsoft configurations.....	8
3. Installing SBA Binary	9
3.1 DNS resolution	10
3.2 Certificate Requirements	10
3.2.1 Certificate Installation	10
4. Configuring the Azure Active Directory SBA Application	12
5. Configuring Direct Routing SBA	15
6. Configuring the SBA Application	17
7. Configuring the OpenScape SBC	20
7.2 Additional Information	21

1. Introduction

The Survivable Branch Appliance (SBA) is an application developed by Microsoft and integrated with the OpenScape Session Border Controller (OSSBC) to enable and maintain calls between the Microsoft Teams Client and the Public Switched Telephone Network (PSTN) in cases of internet outage.

If a client site uses Direct Routing to connect to the Microsoft Phone System, there may be internet connection disruption. During these temporary interruptions, the "branch" at the client site loses connection to the Microsoft Cloud via Direct Routing. However, the intranet within the site remains fully functional, allowing users to maintain their connectivity with the PSTN.

The functionality of the Microsoft Teams Client will be limited to the following PSTN call functions:

- Making PSTN calls via local SBA/SBC with media flowing through the SBC.
- Receiving PSTN calls via local SBA/SBC with media flowing through the SBC.
- Hold and Resume of PSTN calls.

No other Microsoft Teams Client features will be available. For more information on the functionality of the SBA appliance, please refer to the official Microsoft page [SBA for Direct Routing](#). For additional information on Direct Routing, please refer to the official Microsoft pages [Plan Direct Routing](#) and [Configure Direct Routing](#).

Important: This system does not work if the user uses the Teams Client via the web.

1.1. About this Guide

This installation guide outlines the SBA, covering the installation on a Windows Server and the essential configurations in Azure Active Directory, in the SBA Application, in the Direct Routing SBA, and the necessary settings in the SBC. For the setup requirements, please refer to 1.2. Setup Requirements.

The following abbreviations are used in this guide:

Abbreviation	Meaning
SBA	Survivable Branch Appliance
SBA Server	Survivable Branch Appliance application on the Windows Server
DR SBA	Direct Routing Survivable Branch Appliance

Intended audience

It is intended for users familiar with installing and upgrading a Microsoft Windows Server. This familiarity should include downloading and installing additional packages for this guide.

1.2. Setup Requirements

Before installing the SBA, ensure that your system meets the following requirements:

1. Operating System
The SBA requires a machine running Windows Server.
Supported versions include Windows Server 2022 Standard.

2. Hardware Compatibility:

The SBA can be installed on either physical hardware or a virtual machine (VM).

Note: For optimal performance and compatibility, it is highly recommended to use the OpenScape Kontron 550 hardware with Windows Server 2022 Standard.

3. Supported Microsoft Teams Clients:

-

The SBA is supported only for the following Microsoft Teams clients:

- Teams Windows desktop
- Teams MacOS desktop

The SBA also has usage restrictions due to its reliance on 24-hour validity authentication tokens. It can support outages for up to 24 hours from the last token renewal. For more information, please refer to the official Microsoft page [SBA for Direct Routing](#).

2. Configuring SBA on Windows Server

Certain configurations are necessary to ensure a successful SBA installation and smooth integration.

2.1 Microsoft configurations

Microsoft requires the following configurations:

Direct Routing SBC Configuration: Ensure that the **DR SBC** is set to "Media Bypass".

1. Go to the [Microsoft Teams admin center](#) → Voice → Direct Routing → SBC Settings.
2. Edit the SBC to activate "Media bypass" on the *Location based routing and media optimization* session.

•

TLS 1.2: Enable TLS 1.2 on the server to ensure secure communication on SBA Server.

Firewall Port Settings: Allow the following TCP ports in your firewall settings, related to SBA Server:

- 3443
- 4444
- 8443
- 443

Also, ensure that UDP port 123 is allowed.

SBC Port: Allow port 5061 or the port configured on the SBC for SBA communication.

Additionally, ensure that both the Windows Server and the firewall have been appropriately configured. Refer to the Table 1 below for a summarized overview of the necessary firewall configurations.

Traffic Type	From	To	Source Port	Destination Port
Income TCP	MS Teams Clients	DR-SBA	Any	3443
Income TCP	MS Teams Clients	DR-SBA	Any	4444
Income TCP	MS Teams Clients	DR-SBA	Any	8443
Outgoing HTTPS	SBA	Azure Ips	Any	443
Outgoing TCP	SBA	SBC	Any	5061 (See SBC)

Outgoing HTTPS	SBC	DR-SBA	Any	5061
----------------	-----	--------	-----	------

Table 1 Firewall configurations

3. Installing SBA Binary

The installation of the SBA application is completed by the "run installer" method. After transferring the SBA installer package to the Windows server, proceed by clicking "Next" until the installation procedure is finished. If needed, there is an option available to modify the SBA installation directory. For reference, Figure 1 provides a screenshot illustrating one of the steps within this process.

Note: The SBA application will be provided by Unify.

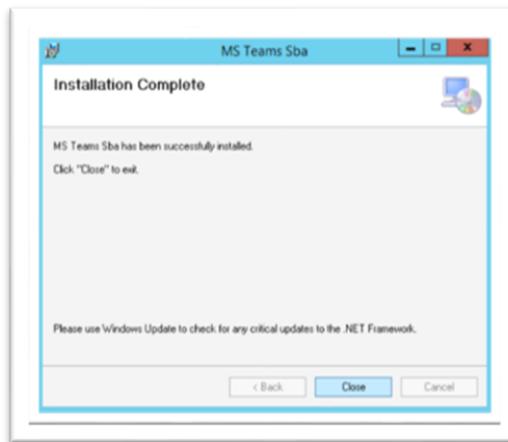


Figure 1 Successful installation of the MS Teams Sba

After completing the installation, verify if the service is running as shown in Figure 2. If it's not running, make sure to check if all the necessary components are installed.

Task Manager					
File Options View					
Processes Performance Users Details Services					
Name	PID	Description	Status	Group	
lsvc		Geolocation Service	Stopped	netsvcs	
LicenseManager	1124	Windows License Manager Service	Running	LocalService	
lltdsvc		Link-Layer Topology Discovery Mapper	Stopped	LocalService	
lmhosts	1192	TCP/IP NetBIOS Helper	Running	LocalServiceNetworkRestricted	
LSM	776	Local Session Manager	Running	DcomLaunch	
MapsBroker		Downloaded Maps Manager	Stopped	NetworkService	
McpManagementService		McpManagementService	Stopped	McpManagementServiceGroup	
Microsoft Teams SBA	7524	Microsoft Teams SBA	Running		
MicrosoftEdgeElevationService		Microsoft Edge Elevation Service (Micr...)	Stopped		
mpssvc	2344	Windows Defender Firewall	Running	LocalServiceNoNetworkFirewall	

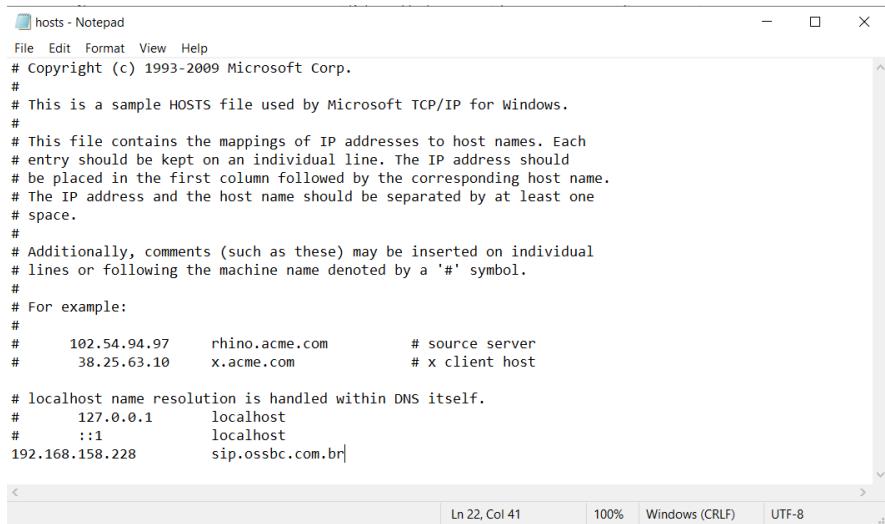
Figure 2 MS Teams Sba: confirmation of successful installation

After the binary installation, check the DNS resolution and certificate inclusion configurations. Please refer to chapters **3.1 DNS resolution** and **3.2 Certificate Requirements**.

3.1 DNS resolution

To ensure proper setup and use the SBA Server, it is necessary to establish a Fully Qualified Domain Name (FQDN). This FQDN can be either public or private.

Hint: In case of communication loss, the FQDN of the DR SBC will not resolve because there will not be an external DNS server available to the SBA Server. To address this issue, you need to edit the Windows Server host file and add the FQDN of the SBC for local resolution. The file path is:
C:\Windows\System32\drivers\etc



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com        # source server
#      38.25.63.10      x.acme.com            # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
192.168.158.228      sip.ossbc.com.br
```

Figure 3 Windows Server host file

3.2 Certificate Requirements

A certificate is necessary for TLS negotiation between the SBC and the Teams client. To align with Microsoft's requirements, make sure that the certificate adheres to the following criteria:

- 1. Assign the Certificate to both SBC and SBA:** The certificate should be assigned to the SBC and the SBA.
- 2. Public or Private:** The certificate can be either public or private.
- 3. Include the SBA's FQDN:** The Fully Qualified Domain Name (FQDN) of the SBA must be present in the common name (CN) or Subject Alternative Name (SAN) of the TLS certificate.

3.2.1 Certificate Installation

To install the certificate and ensure a successful installation for secure communication between the SBC and the Client Teams, follow the steps below:

Step 1: Import the Certificate

Import the certificate into the Windows Server Certificate Store:

- Click on the **Start** button and then select **Run**.
- Enter **certmgr.msc** by navigating to **Console Root → Certificates (Local Computer) → Personal → Certificates**

- Right-click to open the context menu, select **All tasks**, and then **Import**.

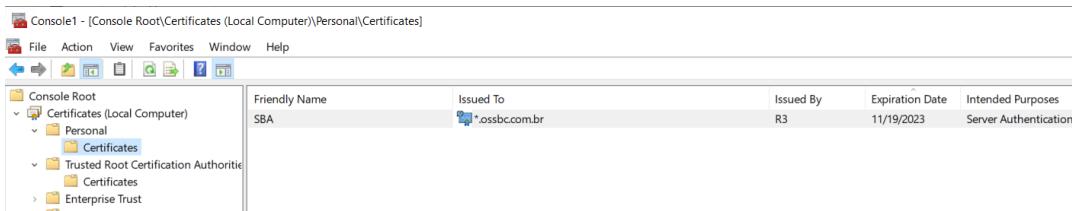


Figure 4 Console Root: Certificates

Step 2: Import the Root CA Certificate

Import the Root CA Certificate from the Certificate Signaling Authority that signs the certificate. This Root CA Certificate should be in the **Trusted Root Certificate Authorities** location.

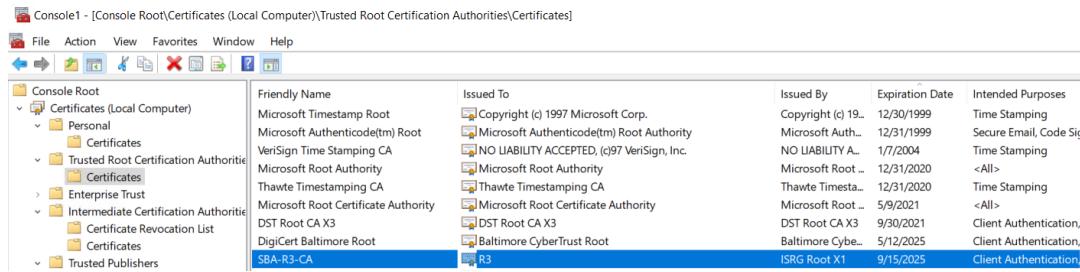


Figure 5 Console Root: Trusted Root Certificate Authorities

4. Configuring the Azure Active Directory SBA Application

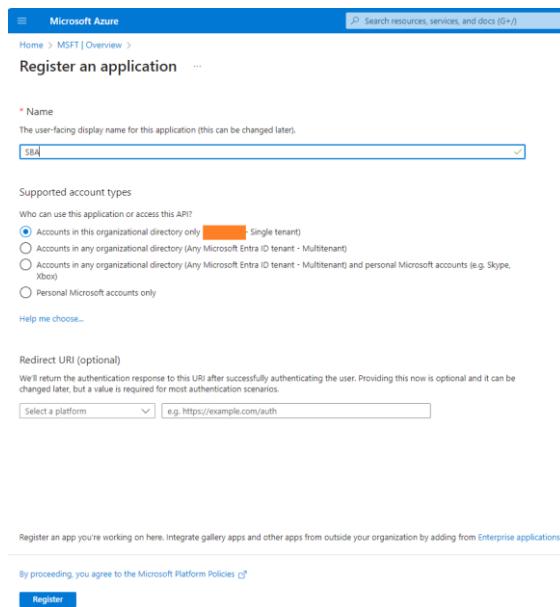
To ensure the SBA can access data from Microsoft 365, it must be registered in Azure Active Directory. It's important to note that only one application registration is needed to cover all SBAs within a tenant. To complete this registration and configure the DR SBA, the following information is required:

1. **Application Name:** Any name of your choice.
2. **Supported Account Types:** Account in this organizational directory only.
3. **Web Redirect URI:** <https://login.microsoftonline.com/common/oauth2/nativeclient>
4. **Implicit Grant Tokens:** Access tokens and ID tokens.
5. **API Permissions:** Skype and Teams Tenant Admin:
 - Access -> Application Permissions -> application_access_custom_sba_appliance
6. **Client Secret:** You can use any description and set expiration.

Note: Please make sure to save the Application ID (Client) and Client Secret, as they will be used in the application configuration.

- Follow the steps outlined below to register and configure the SBA using the Azure portal:
<https://portal.azure.com>.

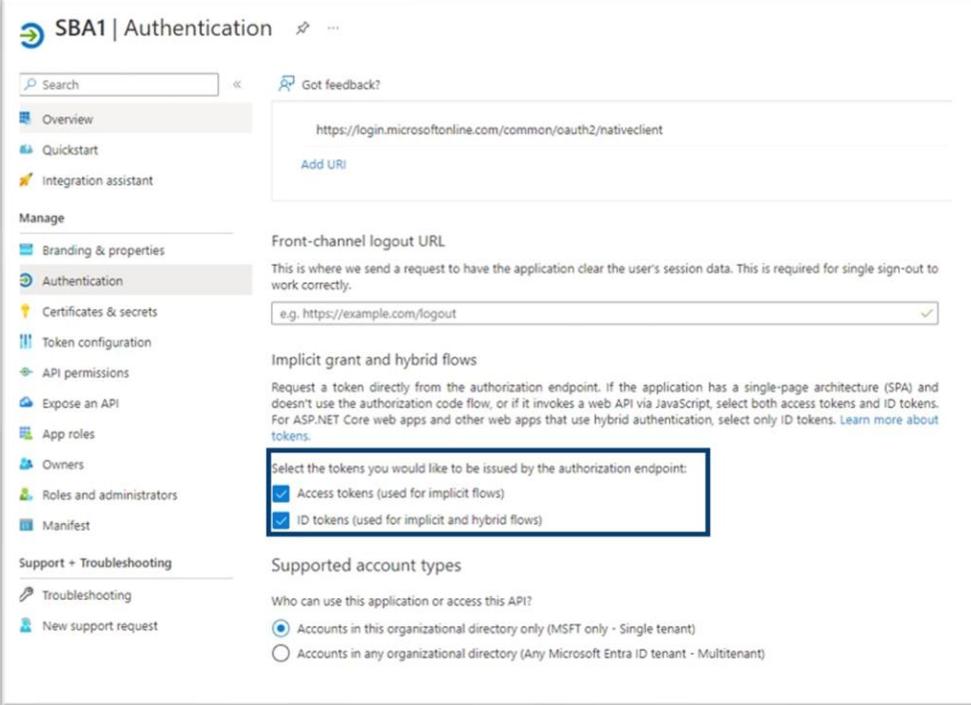
Step 1: Register an application



The screenshot shows the 'Register an application' page in the Azure portal. The 'Name' field is filled with 'SBA'. Under 'Supported account types', the radio button for 'Accounts in this organizational directory only' is selected. Under 'Redirect URI (optional)', a dropdown menu shows 'Select a platform' and 'e.g. https://example.com/auth'. At the bottom, there is a note about enterprise applications and a link to platform policies, followed by a 'Register' button.

Figure 6 App Registration

Step 2: Define Implicit Grant Tokens

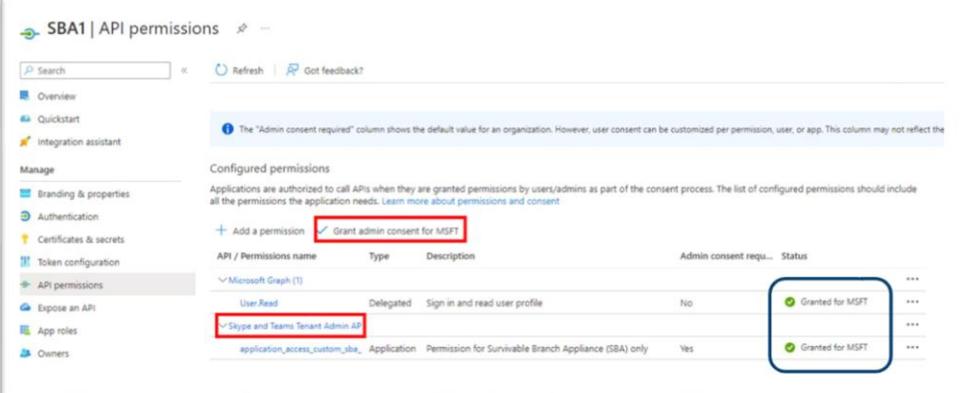


The screenshot shows the 'SBA1 | Authentication' blade in the Azure portal. The 'Manage' sidebar is open, showing 'Authentication' as the selected option. The main area is titled 'Implicit grant and hybrid flows' and contains the following configuration:

- Front-channel logout URL:** `https://login.microsoftonline.com/common/oauth2/nativeclient`
- Implicit grant and hybrid flows:** A note explaining the difference between access tokens and ID tokens for single-page applications (SPA) and hybrid authentication.
- Select the tokens you would like to be issued by the authorization endpoint:** A box containing two checked checkboxes:
 - Access tokens (used for implicit flows)
 - ID tokens (used for implicit and hybrid flows)
- Supported account types:** A note about who can use the application or access the API, with two radio button options:
 - Accounts in this organizational directory only (MSFT only - Single tenant)
 - Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Figure 7 Grant Tokens selection

Step 3: Define API Permissions

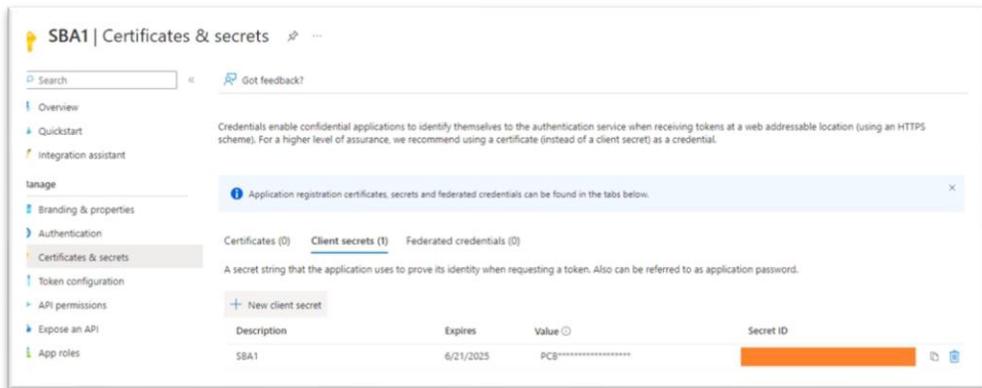


The screenshot shows the 'SBA1 | API permissions' blade in the Azure portal. The 'Manage' sidebar is open, showing 'API permissions' as the selected option. The main area is titled 'Configured permissions' and contains the following table:

API / Permissions name	Type	Description	Admin consent req...	Status
User.Read	Delegated	Sign in and read user profile	No	Granted for MSFT
Skype and Teams Tenant Admin	Delegated	Sign in and read user profile	Yes	Granted for MSFT

Figure 8 API Permissions

Step 4: Create the Client Secret



SBA1 | Certificates & secrets

Overview Quickstart Integration assistant

Manage

Authentication Certificates & secrets Token configuration API permissions Expose an API App roles

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
SBA1	6/21/2025	PCB*****	 

Figure 9 Client Secret creation

After completing these steps, the overview screen will be as shown in Figure 10:



SBA1

Overview Quickstart Integration assistant

Manage

Branding & properties Authentication

Delete Endpoints Preview features

Essentials

Display name	: SBA1
Application (client) ID	: 
Object ID	: 
Directory (tenant) ID	: 

Supported account types : [My organization only](#)

Client credentials : 0.certificate_1.secret

Redirect URIs : 1.web.0.spa.0.public client

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : SBA1

Figure 10 Overview screen

5. Configuring Direct Routing SBA

SBAs and the branch survivability policies need to be created using PowerShell Teams cmdlet for Teams and subsequently assigned to Teams users. This configuration is essential for informing the Teams client about the availability of SBAs at each branch.

To perform these tasks, you will require several PowerShell libraries, which can be installed using the following commands:

```
> Install-Module -Name PowerShellGet -Force -AllowClobber
```

```
> Install-Module -Name MicrosoftTeams -Force -AllowClobber
```

The settings must be made according to the following steps:

Step 1: Create the SBAs

- **Command:** New-CsTeamsSurvivableBranchAppliance
- **Parameters:**
 - -Fqdn: SBA FQDN
 - -Description: SBA Description

Example:

```
> New-CsTeamsSurvivableBranchAppliance -Fqdn sba1.ossbc.com.br -Description "SBA 1"
```

Identity: sba1.ossbc.com.br

Fqdn: sba1.ossbc.com.br

Site:

Description: SBA 1

Step 2: Create the Teams Branch Survival Policy

- **Command:** New-CsTeamsSurvivableBranchAppliancePolicy
- **Parameters:**
 - -Identity: Policy Identity
 - -Fqdn: SBA FQDN

Example:

```
> New-CsTeamsSurvivableBranchAppliancePolicy -Identity CPH -BranchApplianceFqdns "sba1.ossbc.com.br"
```

Identity: Tag:CPH

BranchApplianceFqdns: {sba1.ossbc.com.br}

Step 3: Assign a Policy to a User

- **Command:** Grant-CsTeamsSurvivableBranchAppliancePolicy
- **Parameters:**
 - -PolicyName: Policy Identity
 - -Identity: Teams user

Example:

```
> Grant-CsTeamsSurvivableBranchAppliancePolicy -PolicyName CPH -Identity sbc01@8lpr0.onmicrosoft.com
```

For more detailed commands and information, please refer to the official Microsoft page [SBA for Direct Routing](#).

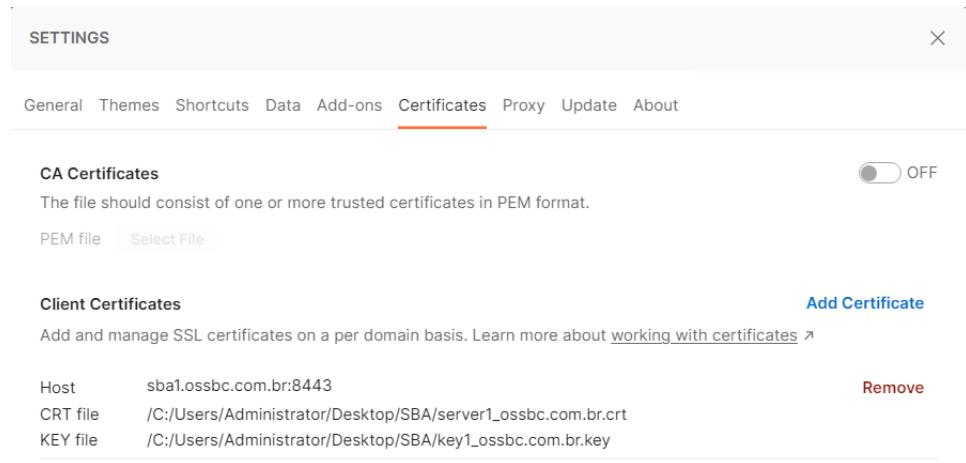
6. Configuring the SBA Application

After completing the preceding steps, the basic SBA configuration will be completed. At this point, please confirm that the SBA Server is up and running. The SBA Application configuration is achieved through an API, and a client is required to execute the commands. One example of a REST API client is the Postman program.

The Postman is available on the page: <https://www.postman.com/downloads/>

The commands use the PUT or GET to send or receive the configuration parameters to/from the SBA Application. The 200 OK and 202 OK Accepted are the successful response messages.

The SBA Application uses port 8443 for HTTPS communication. When using POSTMAN, ensure that your client certificate is included in the application's settings.



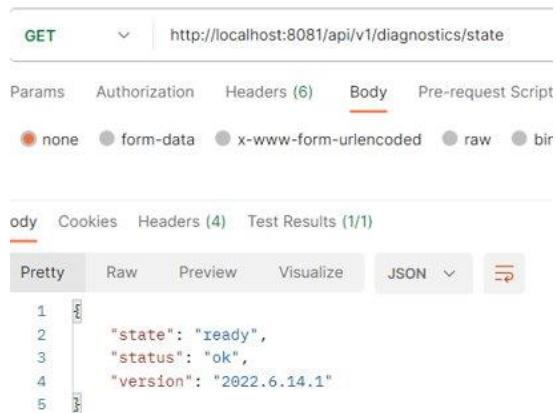
When querying the HTTPS API, use the FQDN:PORT or IP:PORT combination in the URI address.

The API command list is as follows:

- **GET** <http://localhost:8081/api/v1/diagnostics/state>

- **Method:** GET

Provides the SBA state. The initial state is “waiting initial parameters” and after the configuration, the state is “ready”



```
1 "state": "ready",
2 "status": "ok",
3 "version": "2022.6.14.1"
```

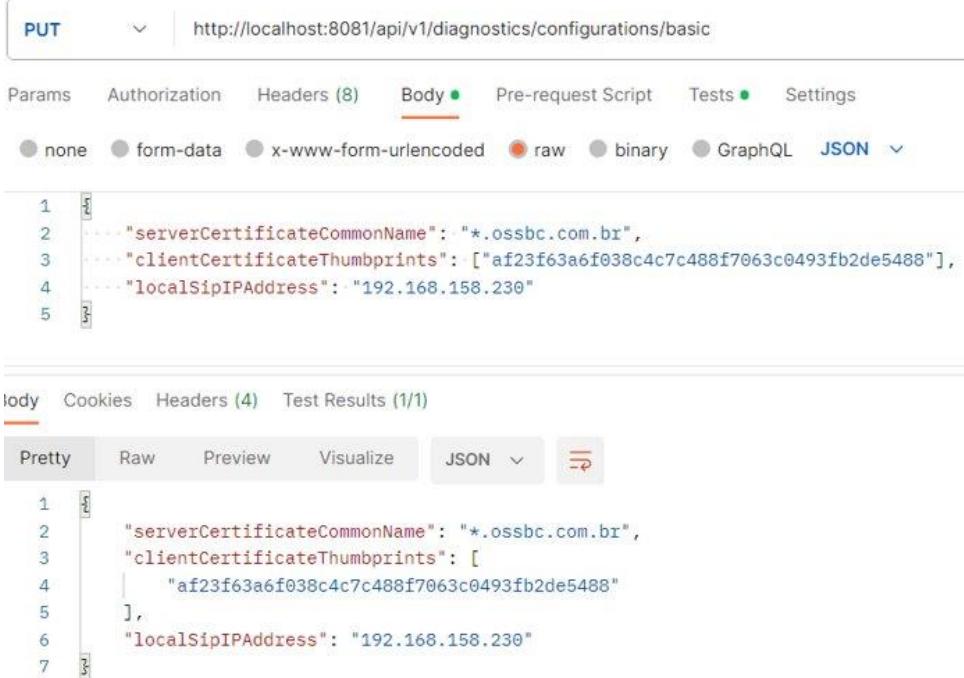
- **PUT** <http://localhost:8081/api/v1/diagnostics/configurations/basic>

- **Method:** PUT and GET

- **Parameters:**

- serverCertificateCommonName: SBA Certificate common name.
- clientCertificateThumbprints: SBC Certificate Thumbprint
- localSipIPAdress: SBA IP address

Provides the basic configuration to SBA.



```

1  {
2    "serverCertificateCommonName": "*.osssbc.com.br",
3    "clientCertificateThumbprints": [
4      "af23f63a6f038c4c7c488f7063c0493fb2de5488"
5    ],
6    "localSipIPAddress": "192.168.158.230"
7  }
  
```

- **PUT** <https://192.168.158.230:8443/api/v1/configurations/general>

- **Method:** PUT and GET

- **Parameters:**

- **identity:** SBA FQDN configured on DR SBA

- **tenant:** Identity of your Tenant

- **logger:**

- **directory:** SBA Log directory
- **level:** SBA log level:
 - Critical, Error, Warning, Information, Debug, Trace, None.
- **maxArchiveFiles:** Log file range: 24-10000

Provides the configuration to SBA.

PUT <https://192.168.158.230:8443/api/v1/configurations/general>

Params Authorization Headers (8) **Body** Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL **JSON**

```
1 {
2   "identity": "sba1.ossbc.com.br",
3   "tenantId": [REDACTED],
4   "logger": {
5     "directory": "C:\\SBA\\logs",
6     "level": "Debug",
7     "maxArchiveFiles": 720
8   }
9 }
```

- **PUT <https://sba1.ossbc.com.br/api/v1/configurations/secure>**

- Method: PUT
- Parameters:
 - applicationId: The application ID (client)
 - appSecret: The Client Secret from DR SBA

Provides security information to SBA and is necessary for the tenant information synchronization.

PUT <https://sba1.ossbc.com.br:8443/api/v1/configurations/secure>

Params Authorization Headers (8) **Body** Pre-request Script Tests Settings

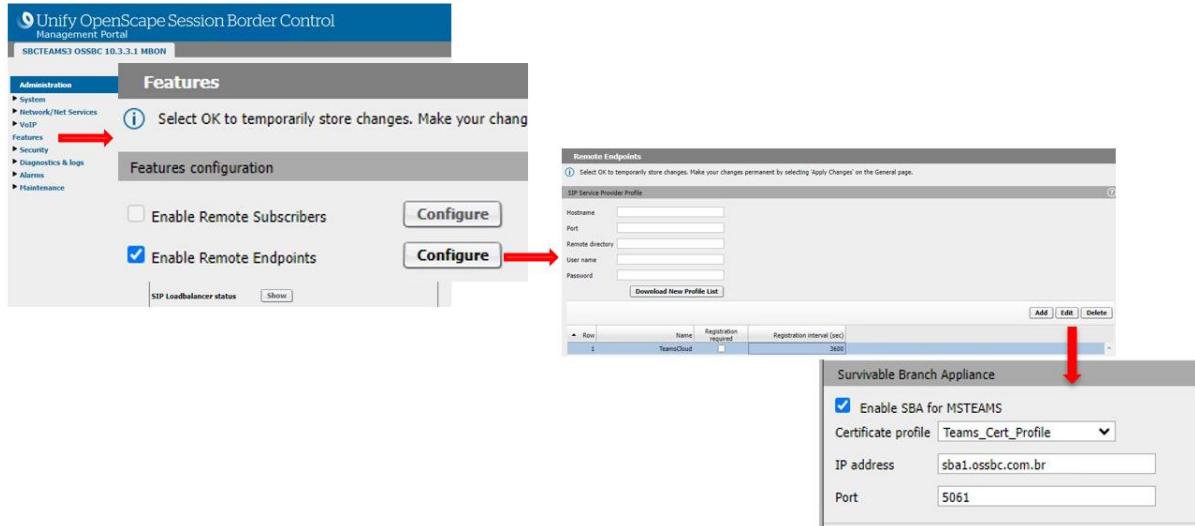
none form-data x-www-form-urlencoded raw binary GraphQL **JSON**

```
1 {
2   "applicationId": [REDACTED],
3   "appSecret": [REDACTED]
4 }
```

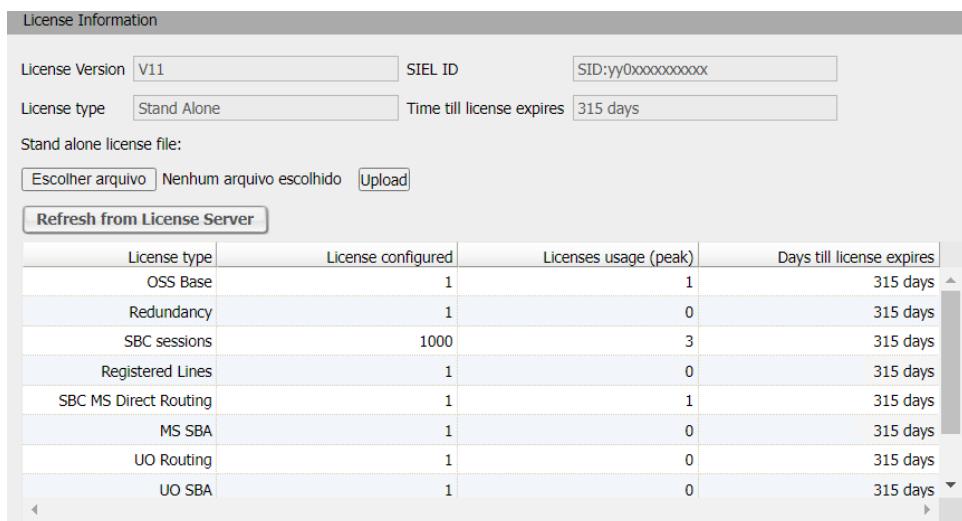
After the SBA configuration, the MS Teams service should be restarted.

7. Configuring the OpenScape SBC

The SBA configuration on the SBC must be done by enabling SBA in the SIP Service Provider Profile GUI.



OSSBC V11, SBC MS Direct Routing, and MS SBA licenses are required to enable the SBA Feature.



The following parameters must be informed:

- Certificate profile:** the certificate must be the same as the one added on the SBA Server. It is recommended to use a specific certificate for the SBA.
- IP address:** the IP or FQDN of the SBA Server. It is highly recommended to use the FQDN
- Port:** by default, SBA uses port 5061

Survivable Branch Appliance

Enable SBA for MSTEAMS

Certificate profile

IP address

Port

7.2 Additional Information:

The SBC uses the fork mechanism to send SIP messages to the SBA. Therefore, for the correct feature function, the MS Teams endpoints must be configured as follows:

1. The endpoint audit must be disabled when using SBA.
2. In BYOT, the endpoint connection check must be disabled.