

Microsoft Teams Direct Routing Survivable Branch Appliance (DR-SBA)

Version 1.1.x

Table of Contents

Notice	vi
Security Vulnerabilities	vi
WEEE EU Directive	vi
Customer Support	vi
Stay in the Loop with AudioCodes	vi
Abbreviations and Terminology	vi
Notes and Warnings	vii
Related Documentation	vii
Document Revision Record	vii
Documentation Feedback	viii
1 Introduction	1
1.1 Overview	1
1.2 Main Benefits	2
1.3 Specifications	2
1.3.1 Mediant 800C DR-SBA	3
1.3.2 Mediant 1000B DR-SBA	4
1.3.3 Virtual Appliance DR-SBA	5
Part I	7
Hardware Description	7
2 Verifying Package Contents	8
2.1 Mediant 800C DR-SBA	8
2.2 Mediant 1000B DR-SBA	8
2.3 Virtual Appliance DR-SBA	8
3 Physical Description for OSN-Based Devices	9
3.1 Mediant 800C DR-SBA	9
3.1.1 Front-Panel Description	9
3.1.2 Rear-Panel Description	10
3.2 Mediant 1000B DR-SBA	11
3.2.1 Front-Panel Description	11
3.2.2 Rear-Panel Description	12
Part II	13
Preparing DR-SBA at Datacenter	13
4 Introduction	14
4.1 Ready and working Direct Routing SBC	14
4.2 DR-SBA FQDN and Certification	14
4.3 Admin User with Manage Roles	14

4.4	Azure AD App Registration	14
4.5	Application Secret	18
5	Teams DR-SBA Setup	20
5.1	Deploying DR-SBA Image with VMware vSphere Hypervisor (ESXi).....	20
5.2	Deploying DR-SBA Image with Hyper-V Hypervisor	24
5.3	Authentication Method for the SBA Management Interface	30
5.4	Logging into DR-SBA and Enabling DR-SBA License	31
5.4.1	Licensing the Product	33
5.5	Network Setup.....	36
5.6	Change Local Administrator Password	38
5.7	Set Date and Time	38
5.8	Join to Domain.....	39
5.9	Log in to Teams	40
5.10	Add or Select Teams DR-SBA	41
5.10.1	Add DR-SBA via PowerShell	41
5.10.2	Add DR-SBA via Login to Tenant.....	42
5.10.3	Select Existing Teams DR-SBA FQDN	43
5.11	Teams DR-SBA Certificate	44
5.11.1	Import PFX File.....	44
5.11.2	Request CSR.....	44
5.11.3	Assign Certificate	45
5.12	Application ID and Application Secret	45
6	SBC Setup	47
6.1	Add Proxy Set	48
6.1.1	Configure Proxy Addresses.....	49
6.1.2	Add IP Group	50
6.2	Terminate SIP OPTIONS and Refer.....	50
6.3	Add IP-to-IP Routing from Teams DR-SBA to PSTN	51
6.4	Add Forking for PSTN Calls to Teams and Teams DR-SBA.....	51
7	Teams Branch Survivability Policy.....	52
8	Assigning Teams Branch Survivability Policy to Users	53
9	Firewall	54
10	Using DR-SBA Management Interface	56
10.1	Viewing General DR-SBA Details on Dashboard	57
10.2	DR-SBA Configuration.....	59
10.2.1	Viewing and Configuring Network Interfaces	59
10.2.2	Changing Login Password	61
10.2.3	Configuring Date and Time.....	62
10.2.4	Configuring SNMP.....	63

10.2.4.1	OVOC in Public Cloud.....	64
10.2.5	Configuring Certificates	64
10.2.6	Access List.....	65
10.2.7	Configuring Teams Online	67
10.2.8	Configuring Voice Application	68
10.3	SBC/Gateway-Related Operations.....	71
10.3.1	Viewing SBC/Gateway Information	71
10.3.1.1	Viewing SBC/Gateway Details	71
10.3.2	Accessing the SBC/Gateway's Web Interface.....	72
10.4	Performance Monitoring	72
10.4.1	Viewing Registered Users Statistics.....	72
10.4.2	Viewing General DR-SBA Server Statistics.....	73
10.5	Maintenance	74
10.5.1	Stopping and Starting DR-SBA Services.....	74
10.5.2	Restarting DR-SBA Server	75
10.5.3	Configuring Syslog	76
10.5.4	Viewing Logged DR-SBA Management Interface Activities.....	77
10.5.5	Viewing Logged Teams DR-SBA Activities	78
10.5.6	Viewing Logged Teams DR-SBA Configuration Activities	79
10.5.7	Generating DR-SBA Test Alarms.....	80
10.5.8	Restoring DR-SBA to Factory Defaults Remotely	81
10.6	Logging Out	82
11	Configuring Token Expiration Grace Period.....	83
12	Configure DR-SBA Web to Work with HTTPS.....	85
13	Running an Anti-Virus Software.....	87
14	Known Issues.....	88
15	DR-SBA Troubleshooting	89
15.1	Validate Tenant is Enabled for DR-SBA.....	89
15.2	Ensure User is Enabled for DR-SBA.....	89
15.3	Verify which DR-SBA the Client Retrieves Based on Policy	89
15.4	Verify if Client can Send Keep-Alive Messages to DR-SBA	89
15.5	DR-SBA to SBC SIP OPTIONS Not Responding.....	90
15.6	Collect Required Information to Report an Issue	90
15.7	One-Way Voice	90
15.8	LMO (Local Media Optimization) not Working	90
15.9	Validating Active Users.....	91
15.10	Clearing Alarm Due to Computer Name Change	91
16	Q&A	93
16.1	Multiple DR-SBAs per Site	93

16.2	Different Management and Media Interfaces	93
17	Re-image DR-SBA from USB.....	94
17.1	Burn DR-SBA via USB	94
17.2	COM Console.....	95
17.3	KVM/VGA Systems	95
17.4	Teams DR-SBA Update Procedure	96
17.5	Recovery USB Update (for OSN-based devices).....	96
18	Survivability PSTN Calling using Cellular Backup	97
19	Creating a Bootable USB Dongle	101

Notice

Information contained in this document is believed to be accurate and reliable at the time of publishing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of published material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: November-04-2025

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Throughout this manual and unless otherwise specified, the term *device* refers to the Mediant 800C and Mediant 1000B DR-SBA.

Notes and Warnings



The device is an INDOOR unit and thus, must be installed ONLY indoors. In addition, Ethernet port interface cabling must be routed only indoors and must not exit the building.



Installation of this device must be in a weather protected location of maximum ambient temperature of 40°C.



This device must be installed only in a restricted access location.



Service of the device must be made only by qualified service personnel.



The device must be connected only to a grounded AC mains power socket.

Related Documentation

Document Name
Microsoft Teams Direct Routing SBA Release Notes
Mediant SBC with Microsoft Teams Direct Routing Enterprise Model

Document Revision Record

LTRT	Description
33440	Initial document release.
33441	Command typo CsTeamsSurvivableBranchAppliancePolicy; updated to Ver. 1.0.22.
33442	Update for the DR-SBA Virtual Appliance installation for Ver. 1.0.112.
33443	Update to Section “Application Secret” for Client Secret expiration settings.
33444	Update to Sections: Package Contents-Virtual Appliance; Deploying DR-SBA Image with VMware vSphere Hypervisor (ESXi); Firewall Chapter.
33445	Update to Section: Running Anti-Virus Software.
33446	Updated note in Available Mediant DR-SBA Models section; updated Add a Permission figure; added a note to Teams DR-SBA Certificate.
33447	Updated note in Teams DR-SBA Certificate section; updated note in Available Mediant DR-SBA Models section.
33448	Updated screenshots in Sections 4.4, 4.5 and 4.6; updated command in Appendix.
33449	Supported Mediant 800 models; rear panel of Mediant 800C; OSNs; firewall; VMware; miscellaneous editing.
33480	Mediant 800 Console port description.

LTRT	Description
33481	Dashboard updated.
33482	Updated Known Issues and note in the Firewall section.
33483	Changed title to Administrator's Manual; added Changing MAC Addresses from 'Dynamic' to 'Static For Hyper-V section; added Teams Direct Routing SBA Update Procedure; added Recovery USB Update section.
33484	IVR removed; firewall for SRTP; section added for multiple DR-SBAs per site; section added for different management and media interfaces.
33485	Firewall rule for PC management station to DR-SBA.
33486	Added Sections 17 "Survivability PSTN Calling using Cellular Backup".
33487	Added sections 14.9 "Validating registered Users".
33488	Troubleshooting alarm due to computer / server name change.
33489	Creating bootable USB; SNMP settings for OVOC and OVOC in cloud
33490	OSN USB port functionality
33491	Q&A Multiple DR-SBAs updated re single/multiple SBCs.
33492	MSFT SBA service 2024.7.26.2 - New SBA capabilities and Firewall changes
33493	Update to the Known Issues for Token authentication.
33494	Updated to Ver. 1.1.018; new section on configuring Voice Application; new section Token expiration grace; known issues updated; miscellaneous
33495	Known issue added about routing extension numbers
33496	Note added regarding non-support for Microsoft GCC High
33497	DR SBA can also be installed as virtual server with Windows server 2022
33498	Added section 5.3 Authentication Method for the SBA Management Interface

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at <https://online.audiocodes.com/documentation-feedback>.

1 Introduction

This document provides step-by-step instructions on installing and configuring AudioCodes Direct Routing Survivable Branch Appliances (DR-SBA) application running on AudioCodes Mediant 800C or Mediant 1000B SBA, or as a Virtual Appliance DR-SBA with Mediant VE/CE SBC.



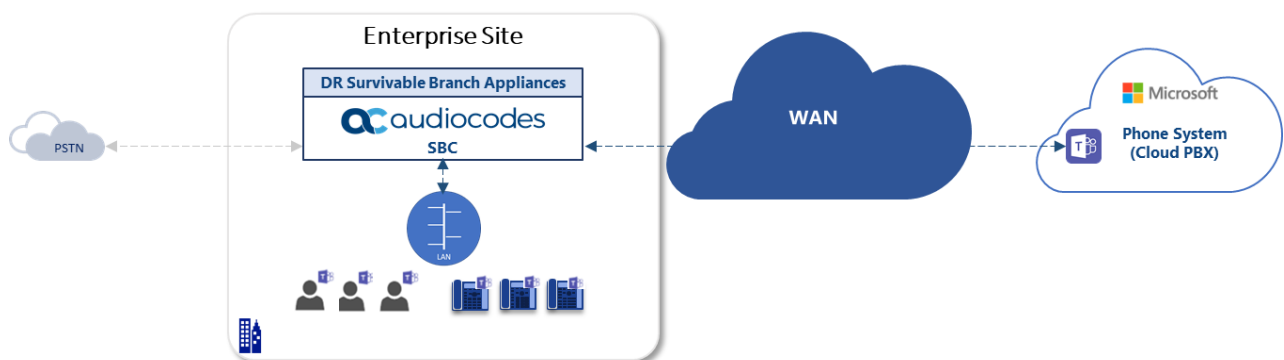
This document is applicable only to Microsoft Teams.

1.1 Overview

Mediant SBA (referred to as the *device* in this document) is an essential element for multi/single-site deployments of Teams and is fully **certified by Microsoft**. The device provides HQ/branch office site voice calling resiliency during Wide Area Network (WAN) failure scenarios where loss of connectivity occurs with Teams Cloud Service.

During survivability, the device maintains local call connectivity call (Dial a Number) among Microsoft Teams users located at the site. It also provides call connectivity between users and the PSTN (SIP/E1/T1 Trunk or FXS/FXO) during a WAN failure (E1/T1 if interfaces are ordered with the device).

Figure 1: DR-SBA at Branch Office in Teams Environment



AudioCodes offers the following DR-SBA devices:

- Mediant 800C DR-SBA
- Mediant 1000B DR-SBA
- Virtual Appliance DR-SBA
- The Virtual Appliance DR-SBA is deployed as a Windows Server 2019 or 2022 virtual machine on VMware ESXi or Microsoft Hyper-V.

Mediant 800C and Mediant 1000B are 1U chassis, providing Microsoft Teams resiliency as well as optional, PSTN Gateway and Session Border Controller (SBC) capabilities. They also provide optional, direct connectivity to Analog Devices through customer ordered FXS port interfaces.

The device provides an embedded, Web-based management tool called *SBA Management Interface* for installing and configuring DR-SBA functionality. The tool also provides a setup wizard, allowing quick-and-easy initial DR-SBA installation.

AudioCodes can also offer a UMP solution to manage the Users Teams Policies (as Teams Branch Survivability Policy) as well as Lifecycle management.

The DR-SBA application is installed on a generic single-board computer module—Open Solution Network (OSN)—housed in the device chassis. The OSN allows you to host multiple third-party applications. The DR-SBA application runs on Windows Server 2019 or 2022 operating system.

The OSN provides the following network interface cards (NIC):

- Up to four "external" NICs (RJ-45 connectors). Ethernet port #1 and #2 create a teaming interface which is enabled by default (192.168.0.20). These NICs are used to connect the DR-SBA application to your network. This connection also allows you to connect to the local SBC/Gateway.
- One "internal" NIC. This NIC connects to the internal chassis switch and is enabled, and DHCP-client enabled. This NIC, like the external NICs, is used to connect the DR-SBA application to your network. This connection also allows you to connect to the local SBC/Gateway.



Installation of any third-party software, except that which is included in the Mediant 800C and Mediant 1000B DR-SBA package purchased from AudioCodes, on the device's OSN server must first be approved by AudioCodes.



DR-SBA doesn't support deployment in Microsoft 365 GCC High cloud environments.

1.2 Main Benefits

The device offers the following main benefits:

- Ensure uninterrupted Teams voice calls for HQ and branch offices
- Secured SIP trunk connectivity with an embedded qualified E-SBC
- Hosting communications-enabled business processes (CEBP) applications such as call recording and Fax Server (according to platform)
- PSTN connectivity in parallel and as fallback to SIP Trunk connectivity
- Full modularity and interface flexibility, including digital spans, analog ports and BRI interfaces
- Fully interoperability with AudioCodes SBC's, supports emergency calling standards, including E911/ ELIN and Local Media Optimization (LMO)

1.3 Specifications

This section lists the specifications of the available DR-SBA models.



- If you have a Mediant 800C or Mediant 1000B DR-SBA model with Lync/Skype for Business Server or CCE (Mediant 800C), refer to the [Product Notice](#) for upgrading to Microsoft Teams.
- When upgrading from an existing Skype SBA (or earlier), we recommend you check the SSD's health and replace it with a new card if the total number of writes to the SSD is greater than 30 TB.

1.3.1 Mediant 800C DR-SBA

Table 1: Mediant 800C DR-SBA Specifications

Item	Description
Maximum PSTN Capacity (Channels)	120
Maximum Number of SBC Sessions	400
Ability to Host Additional Business Applications	Yes (Only for the EO model)
Modularity	Fixed with software scalability options
Digital Interfaces	Up to 4 E1/T1 spans
LAN	4 GE interfaces
OSN Platform	<p>OSN module:</p> <ul style="list-style-type: none"> ■ Standard model: <ul style="list-style-type: none"> ✓ Intel Atom C3558 4 cores ✓ 8G RAM ✓ 128 SSD ■ EO model: <ul style="list-style-type: none"> ✓ Intel Atom C3758 8 cores ✓ 16G RAM ✓ 256 SSD <p>The OSN provides the following interfaces:</p> <ul style="list-style-type: none"> ■ 4 GE interfaces ■ 1 USB 3.0 port ■ 1 micro-USB port (console)
IPv6 Support	Yes
Physical Dimensions	1RU
Power Supply	Single or dual AC power supply
Storage options	SSD

1.3.2 Mediant 1000B DR-SBA

Table 2: Mediant 1000B DR-SBA Specifications

Item	Description
Maximum PSTN Capacity (Channels)	192
Maximum Number of SBC Sessions	150
Ability to Host Additional Business Applications (SBA v2)	Yes
Modularity	Modular
Digital Interfaces	<ul style="list-style-type: none"> ■ 1, 2, 4, 6, 8 T1/J1 spans ■ 1, 2, 4, 6 E1 spans ■ Optional 1+1 or 2+2 fallback spans
Analog FXO and FXS Interfaces	<ul style="list-style-type: none"> ■ 4, 8, 12, 16, 20, 24 FXS/FXO ports ■ 4 ports per module ■ One lifeline port per FXS module
BRI Interfaces	<ul style="list-style-type: none"> ■ 4, 8, 12, 16, 20 BRI lines ■ 4 BRI lines (8 calls) per module S/T interfaces
LAN	Up to 6 x 10/100 Base-TX Ethernet LAN ports configured in 1+1 redundancy or as individual ports
OSN Platform	<ul style="list-style-type: none"> ■ OSN server (OISN4B): <ul style="list-style-type: none"> ✓ 16-GB RAM ✓ USB 2.0 port for connecting peripheral devices such as DR-SBA Dongle, USB hub (to which keyboard and mouse can be connected) ✓ 2 x Gigabit Ethernet interface (RJ-45) for connection to the network ✓ Console (serial) port (micro-USB) for serial communication ✓ HDMI interface (19-pin Type D, micro-HDMI port) for connection to graphic display monitor ■ HDMX module for solid-state drive (SSD)
IPv6 Support	Yes
Physical Dimensions	1RU
Power Supply	Single or dual AC power supply
Storage options	SSD (supports dual SSD)

1.3.3 Virtual Appliance DR-SBA

Table 3: Minimum Virtual DR-SBA Specifications

Item	Description
Platforms	<ul style="list-style-type: none">■ Microsoft HyperV 2016, 2019, or 2022■ VMware ESXi 6.7 and later
Guest OS	Windows Server 2019 or 2022
CPU	2 cores
RAM	8-Gb RAM
Storage	50 Gb
LAN	1 LAN



The SBC is not included in the Virtual DR-SBA and should be installed and purchased separately according to Customer requirements.

Part I

Hardware Description

2 Verifying Package Contents

2.1 Mediant 800C DR-SBA

Ensure that your device package is shipped with the following items:

- Four anti-slide bumpers for desktop installation
- 19-inch rack mounting kit (two flanges and six screws)
- One AC power cable
- (Optional) E1/T1 splitter cable adapter for T1 WAN interface (customer-ordered item)
- USB dongle for DR-SBA software upgrade and recovery procedure (Teams image)
- Microsoft Windows 2019 license (in envelope and label affixed to module)
- (Optional) 1 x micro-USB to USB cable adaptor 1.5m for serial connections (for Mediant 800 without VGA connector in the rear panel)

Check, retain and process any documents. If any items are missing or damaged, please contact your AudioCodes sales representative.

2.2 Mediant 1000B DR-SBA

Ensure that your Mediant 1000B DR-SBA package is shipped with the following items:

- 4 x Anti-slide bumpers for desktop installation
- 19-inch rack mounting kit (two flanges and six screws)
- 1 x micro-HDMI (Type D) to standard-HDMI (Type A) 1.5m cable adaptor for monitor connections
- 1 x micro-USB to USB cable adaptor 1.5m for serial connections
- 1 or 2 AC power cables (depending on customer order)
- 1 x USB dongle for DR-SBA software upgrade and recovery procedure (Teams Image)
- Microsoft Windows 2019 license (in envelope and label affixed to module)

Check, retain and process any documents. If any items are missing or damaged, please contact your AudioCodes sales representative.

2.3 Virtual Appliance DR-SBA

Ensure that you have downloaded the virtual disk file (OVA) containing the DR-SBA image for deploying a virtual appliance on VMware, or the VHDX file for deploying on Hyper-V from [AudioCodes download portal](#).



The Microsoft Windows 2019 or 2022 license for the virtual machine must be provided by the Customer.



The OVA package was officially tested on VMware Version 6.7 Update 03 and on VMware Version 7.0 Update 02.

3 Physical Description for OSN-Based Devices

This section provides a brief description of the front and rear panels of the device. For a detailed description, refer to the following documents:

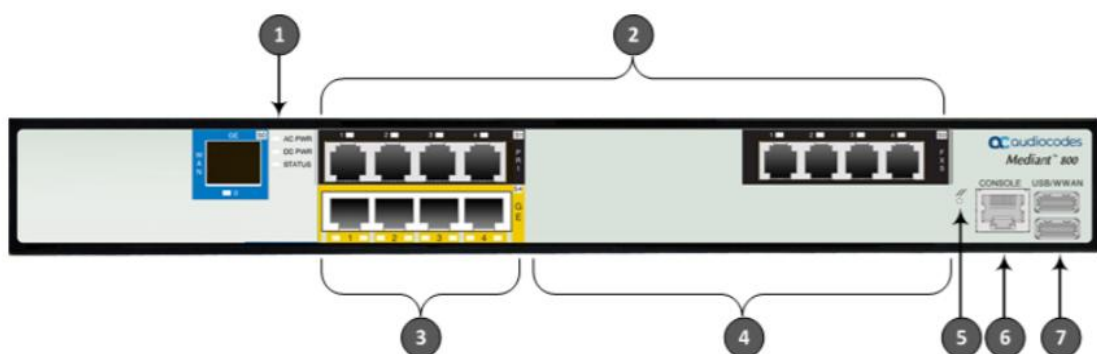
- Mediant 800 Gateway and SBC Hardware Installation Manual
- Mediant 1000B Gateway and SBC Hardware Installation Manual

3.1 Mediant 800C DR-SBA

3.1.1 Front-Panel Description

The front panel of the device provides various port interfaces for the **optional** SBC-Gateway functionality.

Figure 2: Mediant 800C Front Panel



- The telephony interfaces are customer-ordered items and not shipped by default.
- The figure above is used only as an example. The number and type of interfaces depend on the ordered configuration.

Table 4: Front-Panel Description

Item #	Label	Description
1	POWER / STATUS	LEDs indicating the status of power and reboot/initialization.
2	FXS / FXO / BRI / PRI	Telephony port interfaces that can include one or a combination of the following, depending on the ordered model: <ul style="list-style-type: none"> ■ FXS port interfaces (RJ-11) ■ FXO port interfaces (RJ-11) ■ ISDN BRI port interfaces (RJ-45) ■ ISDN PRI (E1/T1) port interfaces (RJ-48)
3	GE	Up to four 10/100/1000Base-T (Gigabit Ethernet) LAN ports for connecting IP phones, computers, or switches.
4	FE	Eight Fast Ethernet (10/100Base-TX) RJ-45 LAN ports for connecting IP phones, computers, or switches. The supported port features are the same as the GE ports (see Item #6 above). <p>Note: The Fast Ethernet ports are available only on "pure" SBC Mediant 800 (i.e., without PSTN / Gateway interfaces).</p>

Item #	Label	Description
5	-	Reset pinhole button for resetting the device and optionally, for restoring the device factory defaults.
6	CONSOLE	RS-232 port (RJ-45) for serial communication.
7	USB/WWAN	Two USB ports used for various functionalities such as saving debug captures to a USB storage device.


3.1.2 Rear-Panel Description

The rear panel of the device provides the interface to the OSN server on which the DR-SBA runs.

Figure 3: Mediant 800C Rear Panel



Table 5: Rear-Panel Description

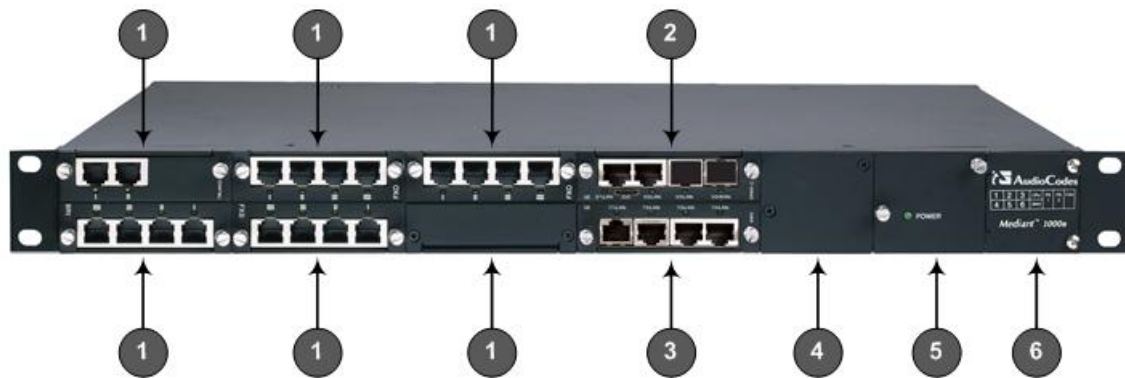
Item #	Label	Description
1	USB	USB 3.0 port (Standard-A type) for connecting a USB storage device to the OSN server.
2	OSN PWR	LED indicating power status of the OSN server.
3	-	Reset button for resetting the OSN server.
4	CONSOLE	Micro-USB port for serial communication (CLI) with the OSN server.
5	GE 1-4	Four 10/100/1000Base-T Ethernet ports (RJ-45) for connecting directly to the OSN server.
6	DC IN 12V 10A	(Optional) DC power inlet for accepting a DC terminal block plug. Note: Use only the AC/DC power adaptor supplied by AudioCodes to connect the DC inlet.
7		Protective earthing screw.
8	100-240V 50-60Hz	3-Prong AC power supply entry. Note: The device can be ordered with dual Power Supply entries.

3.2 Mediant 1000B DR-SBA

3.2.1 Front-Panel Description

The front panel of the device provides various port interfaces for the **optional** SBC-Gateway functionality.

Figure 4: Front Panel



- The telephony interfaces are customer-ordered items and not shipped by default.
- The figure above is used only as an example. The number and type of interface modules depend on the ordered configuration.

Table 6: Front-Panel Description

Item #	Label / Module	Component Description
1	FXS, FXO, BRI, TRUNKS, MPM	(Optional) Telephony and DSP resource modules: <ul style="list-style-type: none"> ■ FXS module ■ FXO (or FXO G) module ■ BRI module ■ TRUNKS (E1/TE/J1) module ■ MPM module (provides additional DSP resources) Note: The modules are customer-ordered items.
2	CRMX	CRMX module, providing the following: <ul style="list-style-type: none"> ■ Gigabit Ethernet ports ■ RS-232 serial port ■ Reset pinhole button
3	SWX	(Optional) LAN Extension (SWX) module, providing four Gigabit Ethernet ports. Note: The module is a customer-ordered item.
4	Power 1	(Optional) Spare Power Supply module slot. Note: The module is a customer-ordered item.
5	Power 2	Main Power Supply module.
6	-	Extractable Fan Tray module with a schematic displayed on its front panel showing the chassis' slot numbers.

3.2.2 Rear-Panel Description

The rear panel of the device provides the modules for the OSN server on which the DR-SBA runs.

Figure 5: Rear Panel

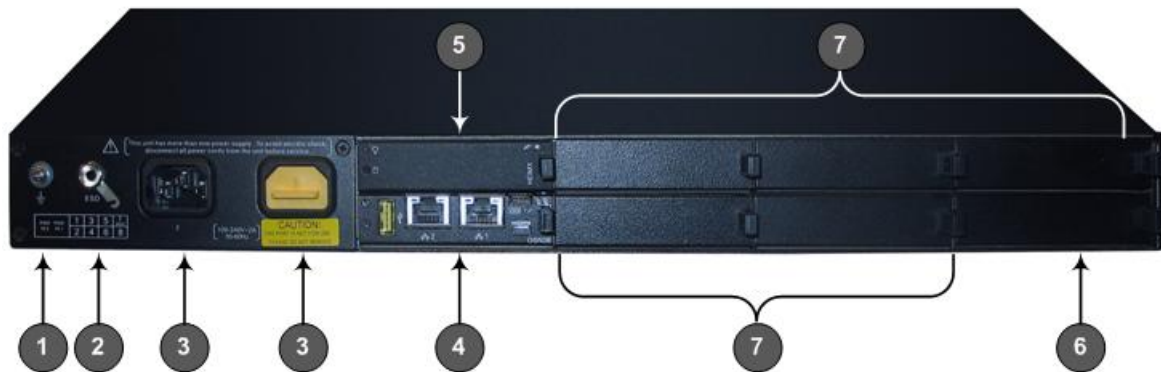



Table 7: Rear-Panel Description

Item #	Label	Description
1		Protective earthing screw.
2	ESD	Electrostatic Discharge (ESD) socket.
3	100-240V~1A	Dual AC Power Supply Entries.
4	OSN	OSN4B module: <ul style="list-style-type: none"> ■ USB 2.0 port for connecting peripheral devices such as DR-SBA Dongle, USB hub (to which keyboard and mouse can be connected). ■ 2 x Gigabit Ethernet interface (RJ-45) for connecting to the network. ■ Console (serial) port (micro-USB) for serial communication. ■ HDMI interface (19-pin Type D, micro-HDMI port) for connecting to graphic display monitor.
5	HDMX	Main hard-disk drive (HDD) or Solid-State Drive (SSD) AMC module for OSN server platform.
6	HDMX	Slot for second (optional) HDD or SSD for OSN server platform.
7	-	Unused and covered AMC module slots.

Part II

Preparing DR-SBA at Datacenter

4 Introduction

Before you can install and configure the device at your Site Office, you need to check the following guidelines.

4.1 Ready and working Direct Routing SBC

The SBC needs to be configured for Media Bypass to ensure that media flows directly between the Microsoft Teams client in the branch site and the SBC.

Refer to one of the following documents:

- **Enterprise Solution:** Connecting AudioCodes' SBC to Microsoft Teams Direct Routing Enterprise Model
- **Service Provider Solution:** Connecting AudioCodes SBC to Microsoft Teams Direct Routing Hosting Model Configuration Note

4.2 DR-SBA FQDN and Certification

The FQDN for the DR-SBA is configured in the certificate (you can use a .pfx certificate file or use the DR-SBA GUI to create a CSR). This certificate must be trusted by the end points that host the Teams client and by the SBC.

DR-SBA allows you to upload and assign certificates with the DR-SBA FQDN in the SAN and not on CN.



The DR-SBA certificate and FQDN must be trusted by the SBC and by the Teams clients. You can also use a private CA for the certificate and a local DNS for the FQDN. Although private certificate is supported from Version 1.0.22, it is recommended to use a **public certificate**.

4.3 Admin User with Manage Roles

DR-SBA installation requires M365 users with Teams Administrator roles and role that allow to create Azure App Registration.

4.4 Azure AD App Registration

Create App Registration in Azure AD and note **applicationId** and **appSecret** for the later install steps. Customers can either use the same Azure App Registration for all the SBAs in the Tenant or create a specific App Registration per DR-SBA.

To register and Azure AD App Registration:

1. Sign-in to Azure portal with tenant administrator user and create new App registration (Azure Active Directory > App registrations > New registration) – the same App Registration can be used for all the tenant DR-SBAs, add name for the new application and select “Accounts in this organizational directory only – single tenant” under Supported account types. Select Register and note the Application ID for the next steps.

Figure 6: App Register

Dashboard > audiocodes.be >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

SBA-Connector ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (audiocodes.be only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Figure 7: Application ID and Tenant ID

Dashboard > audiocodes.be >

SBA-Connector

Search (Ctrl+/)

Overview | Quickstart | Integration assistant | Manage | Branding | Authentication | Certificates & secrets | Token configuration | API permissions | Expose an API | App roles | Preview | Owners | Roles and administrators | Pr... | Manifest | Support + Troubleshooting | Troubleshooting

Delete | Endpoints | Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : SBA-Connector
 Application (client) ID :
 Directory (tenant) ID :
 Object ID :
 Supported account types : My organization only
 Redirect URIs : Add a Redirect URI
 Application ID URI : Add an Application ID URI
 Managed application in L. : SBA-Connector

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn](#)

Call APIs

Build more powerful apps with rich user and business data

Documentation

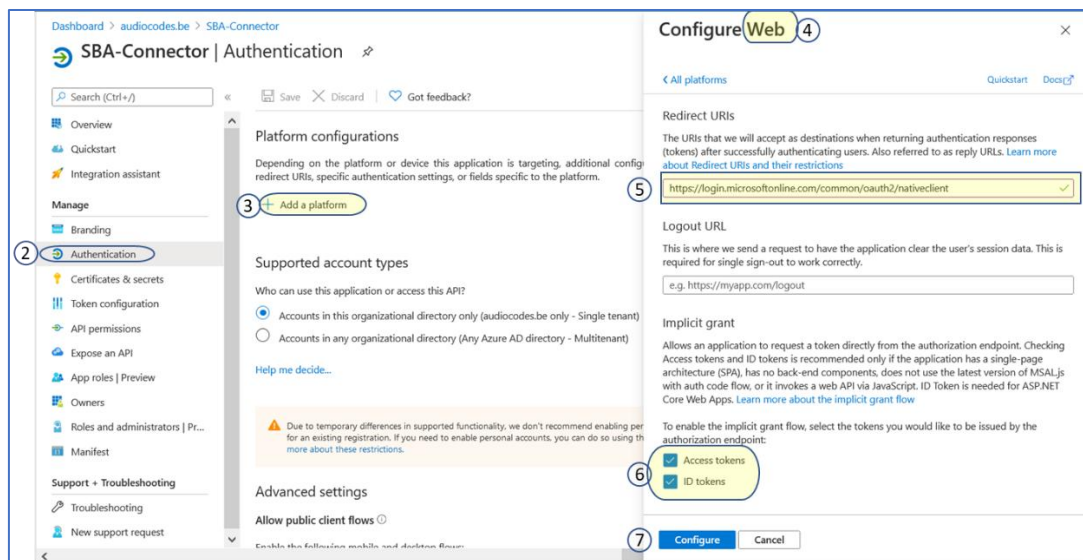
[Microsoft identity platform](#)
[Authentication scenarios](#)
[Authentication libraries](#)
[Code samples](#)
[Microsoft Graph](#)
[Glossary](#)
[Help and Support](#)

2. Select the **Authentication** tab.
3. Select **Add Platform**.
4. Select **Web**.
5. Insert <https://login.microsoftonline.com/common/oauth2/nativeclient> into Redirect URIs
6. Select the “Access tokens” and “ID tokens” check boxes.
7. Select **Configure**.



“Add a Platform” is only required for the 1st URI. If a Web Platform has already been created, select **Add URI**.

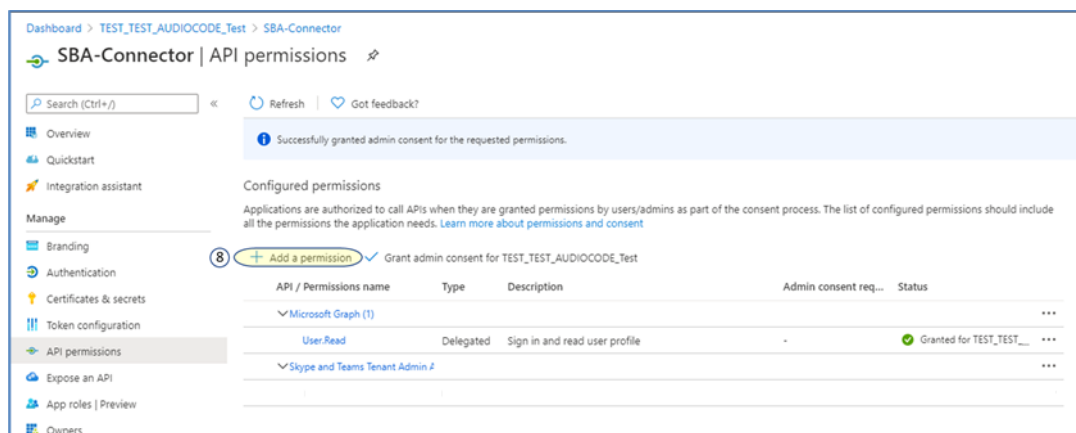
Figure 8: Add URI



8. Adding application_access_custom_sba_appliance API permissions:

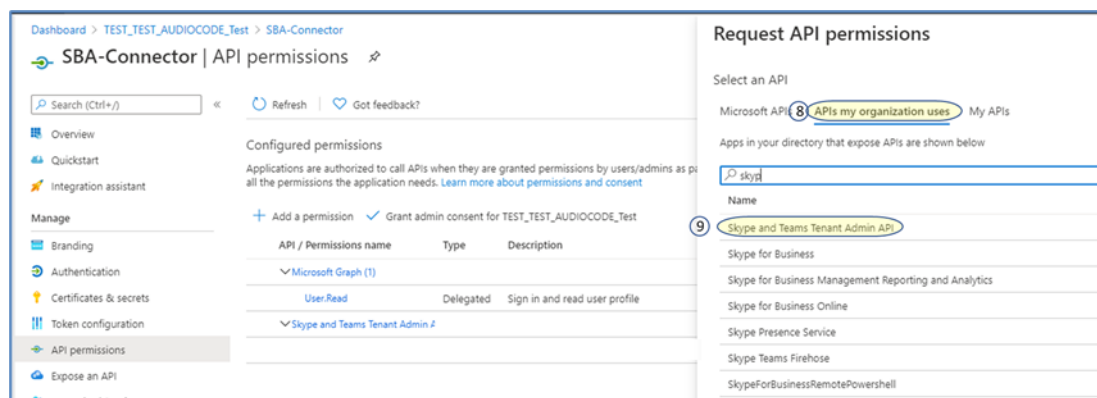
- Click **Add a permission** and then select the **APIs my organization uses** tab.

Figure 9: Add a Permission



9. In the search box type: "Skype and Teams Tenant Admin API"

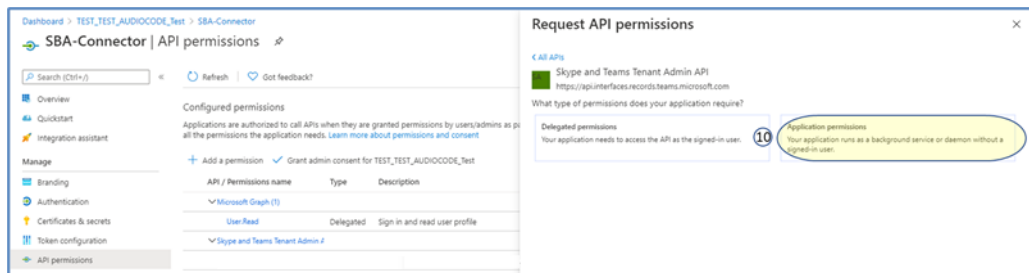
Figure 10: Add a Permission



10. Select this API and on the next page select **Application permissions**, check "application_access_custom_sba_appliance API" and then click **Add permission**.

11. Add new Application permissions:

Figure 11: Add a Permission



12. Select the new permission you added, select the “Grant admin consent for...” and then select yes.

Figure 12: Add a Permission

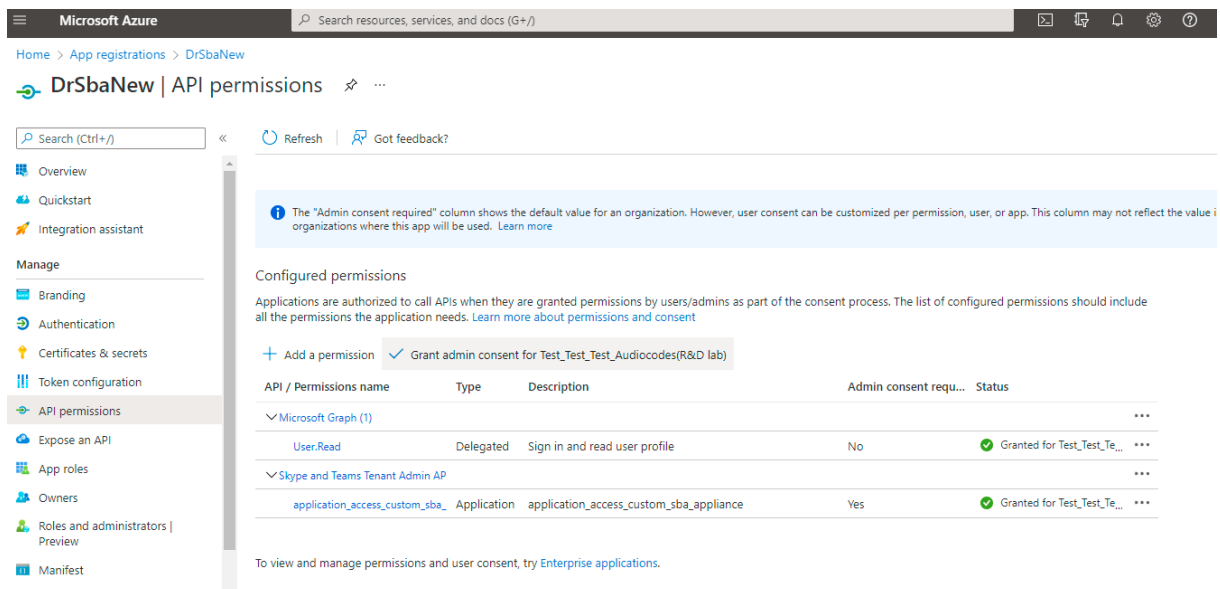
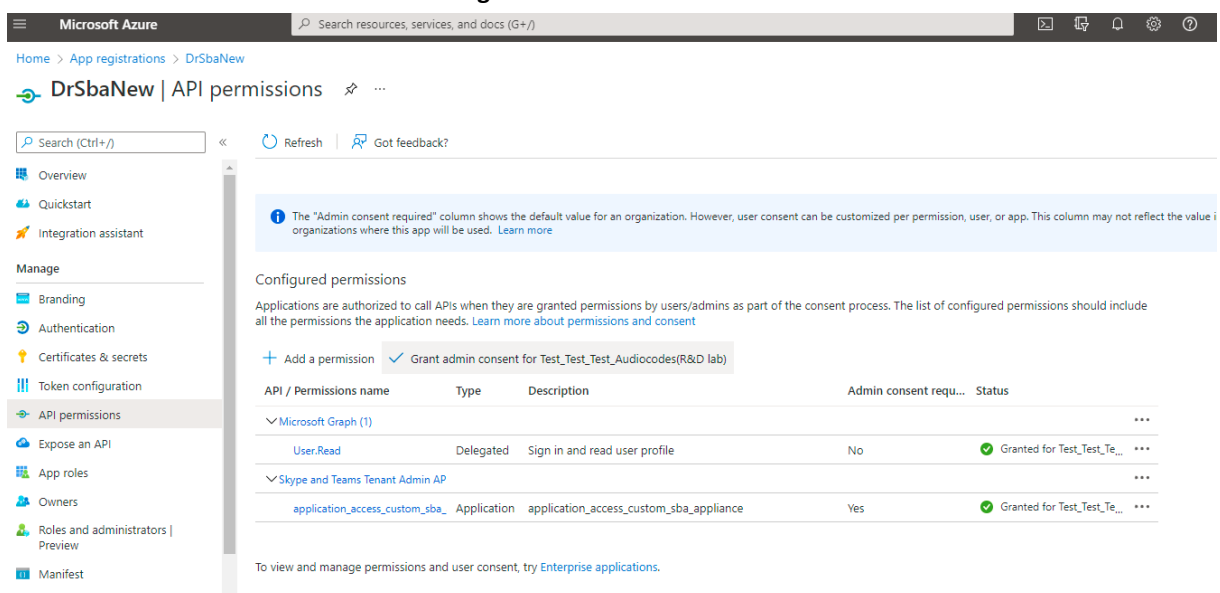


Figure 13: Add a Permission



4.5 Application Secret

This section describes how to create an Application secret.

To create an Application secret:

1. In the Navigation pane, open **Certificates & secrets**.
2. Select **New client secret**.

Figure 14: Add Application Secret

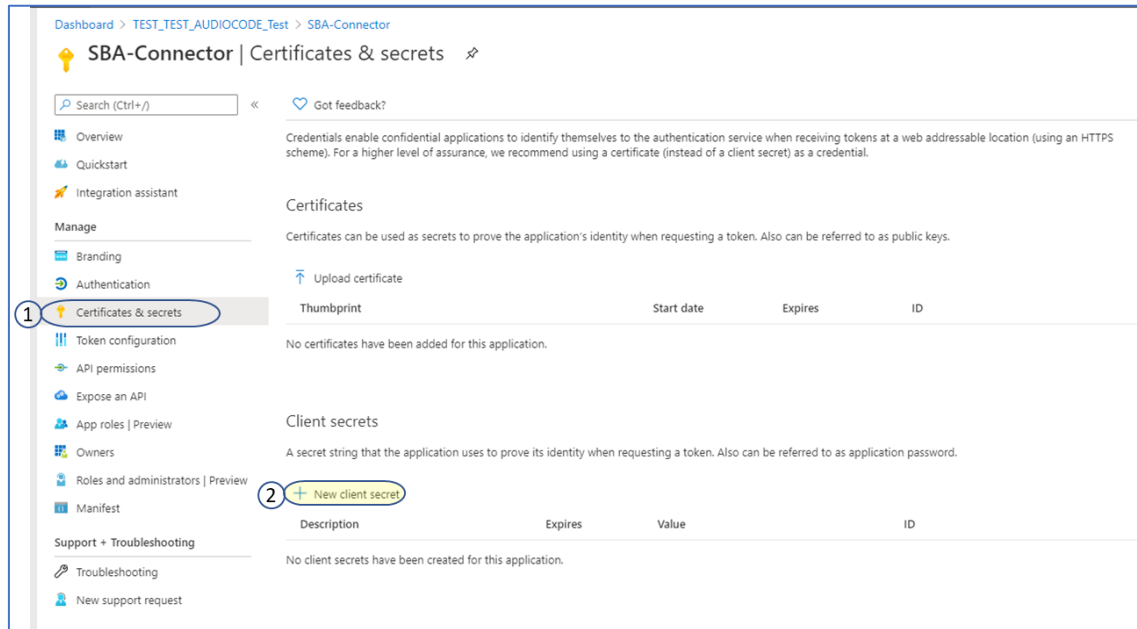
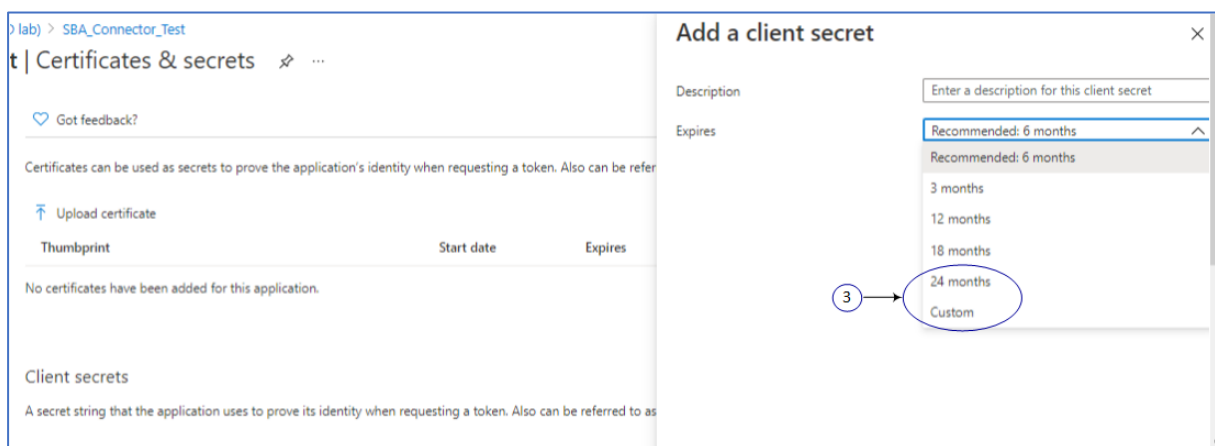


Figure 15: Add Application



3. Select either **24 months** or **Custom** years for expiration time and enter description.
4. Click **Add**.
5. **Copy** the new client secret value for the following steps.

Figure 16: Copy Client Secret Value

Dashboard > TEST_TEST_AUDIOCODE_Test > SBA-Connector

SBA-Connector | Certificates & secrets

Search (Ctrl+/) Got feedback?

Warning: Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets

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	ID
SBA	12/31/2299	[Redacted]	[Redacted]

5 Copy the new client secret value



Copy the new client secret value. You won't be able to retrieve it after you do another operation or leave this page. If you forget to copy it, you need to add a new secret and delete the old one if no DR-SBA devices use this secret.

5 Teams DR-SBA Setup

This chapter describes the Teams DR-SBA setup.



For the Virtual Appliance, the guest OS is Windows Server 2019 or 2022

5.1 Deploying DR-SBA Image with VMware vSphere Hypervisor (ESXi)

This section describes how to deploy the DR-SBA Image on the VMware vSphere hypervisor (ESXi) virtual appliance.



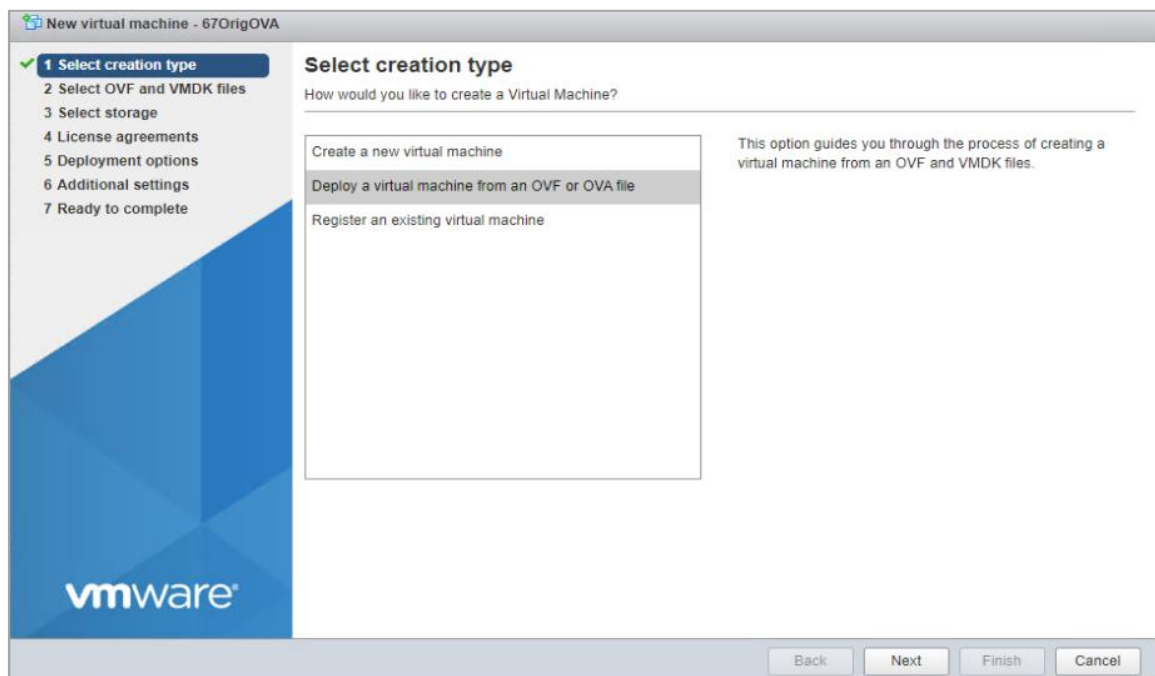
The Virtual Appliance DR-SBA runs as a **Windows Server 2019 or 2022** VM on ESXi.

To deploy DR-SBA image on VMware:

Prerequisite: Download the Windows Server 2019 or 2022 DR-SBA OVA

1. Download the OVA file containing the DR-SBA image to the virtual machine (see Section 2.3).

Figure 17: Select Creation Type



2. Select option **Deploy a virtual machine from OVF or OVA file** and then click **Next**.

Figure 18: Select Files

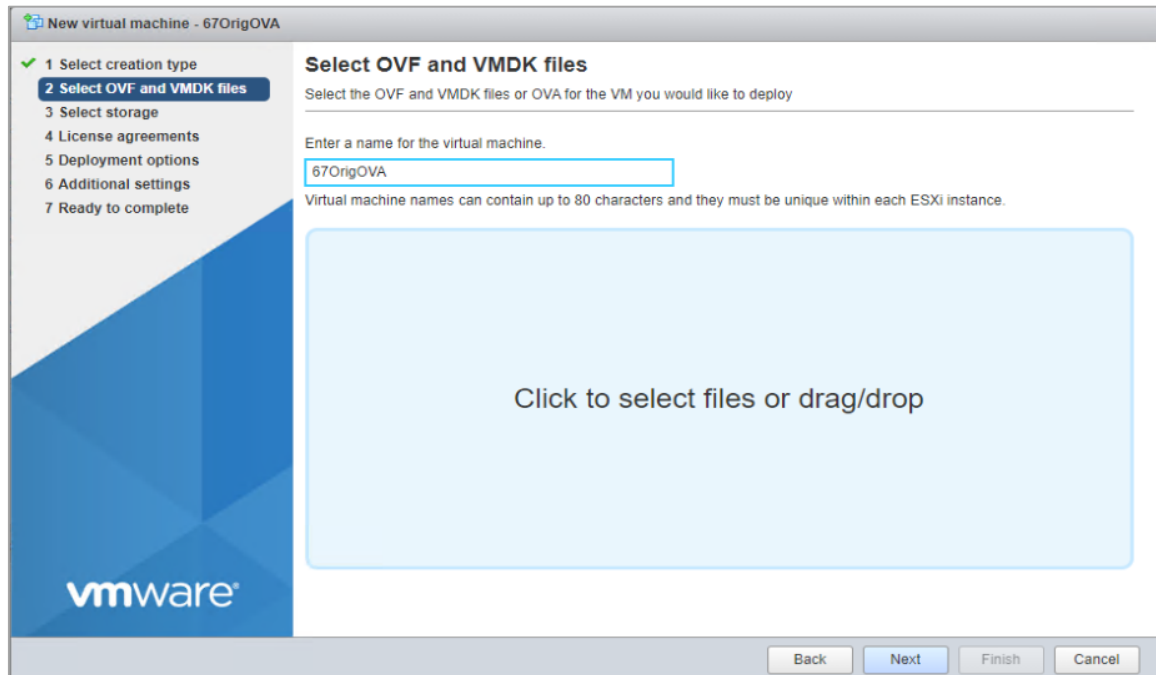
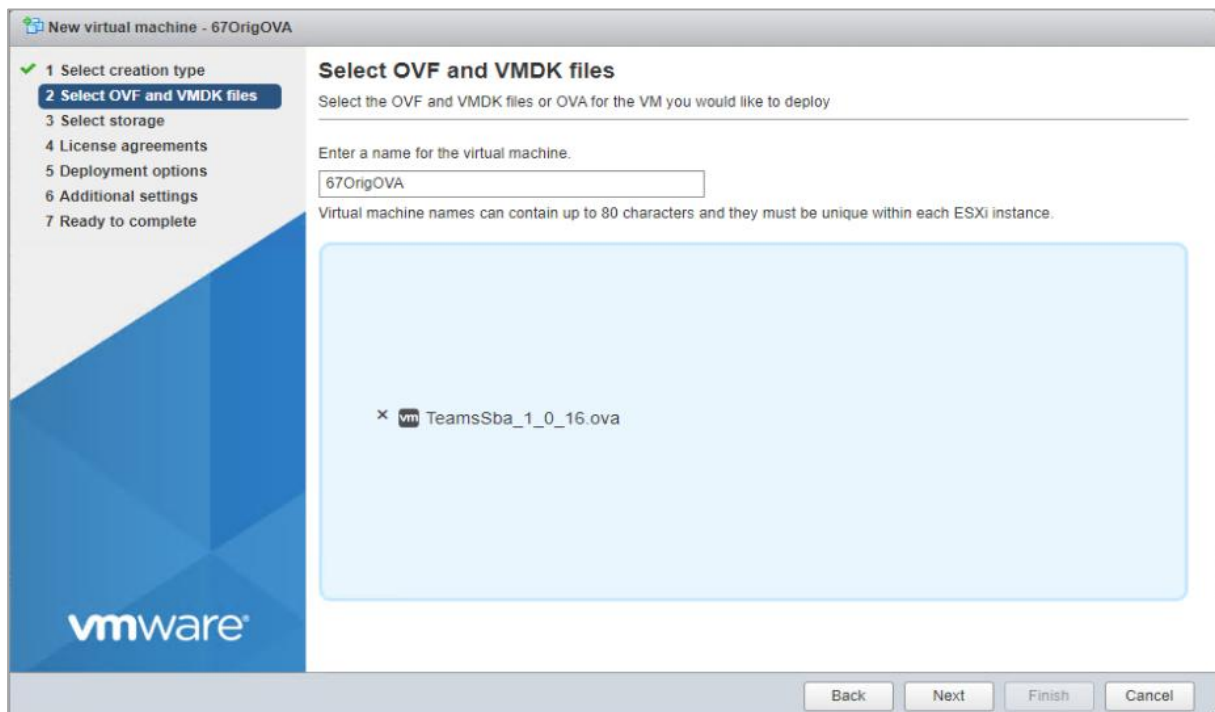
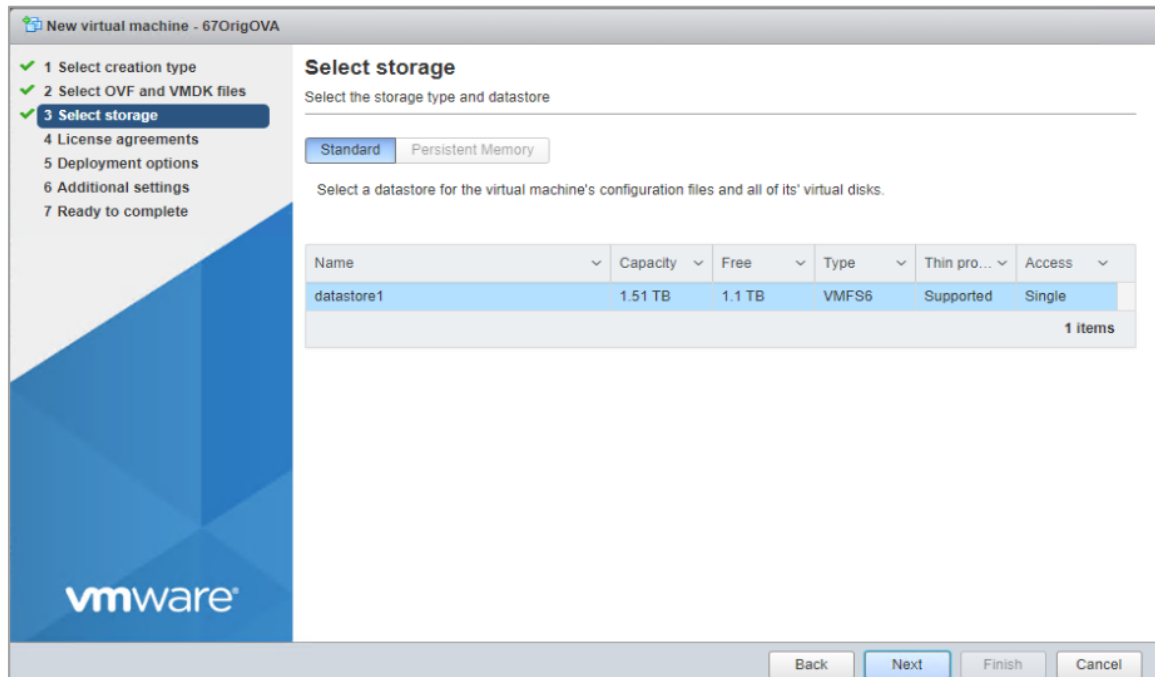


Figure 19: Select File



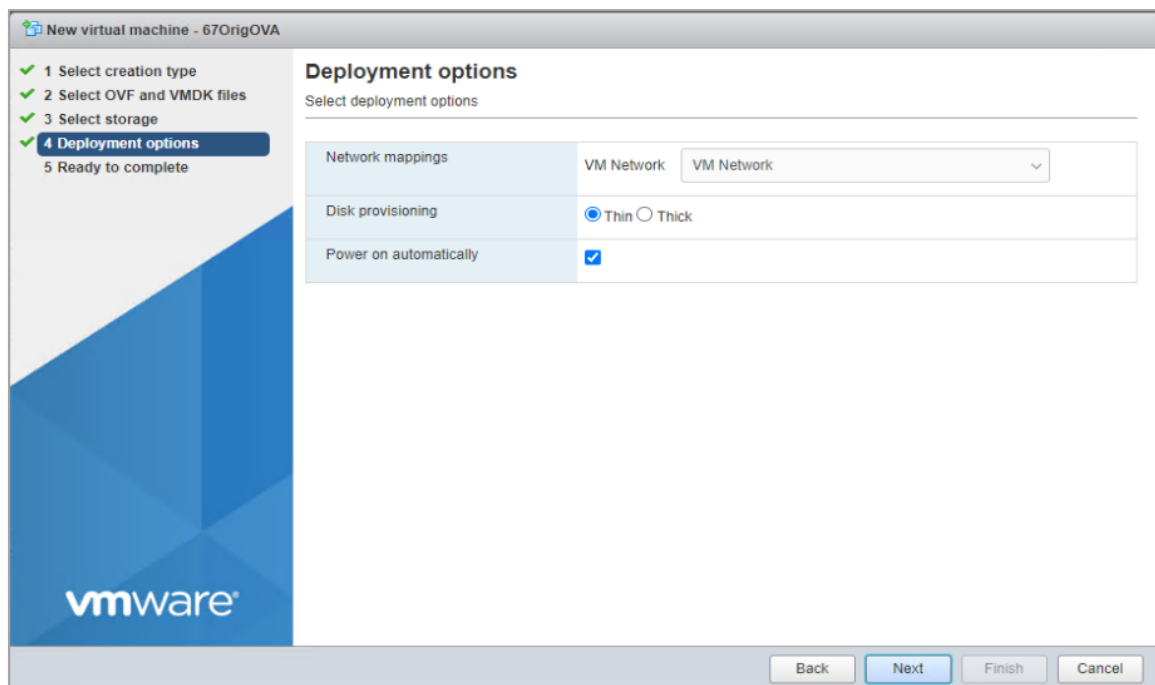
3. Enter the name of the Virtual machine to create, drag the file containing the installation package and then click **Next**.

Figure 20: Select Storage Type



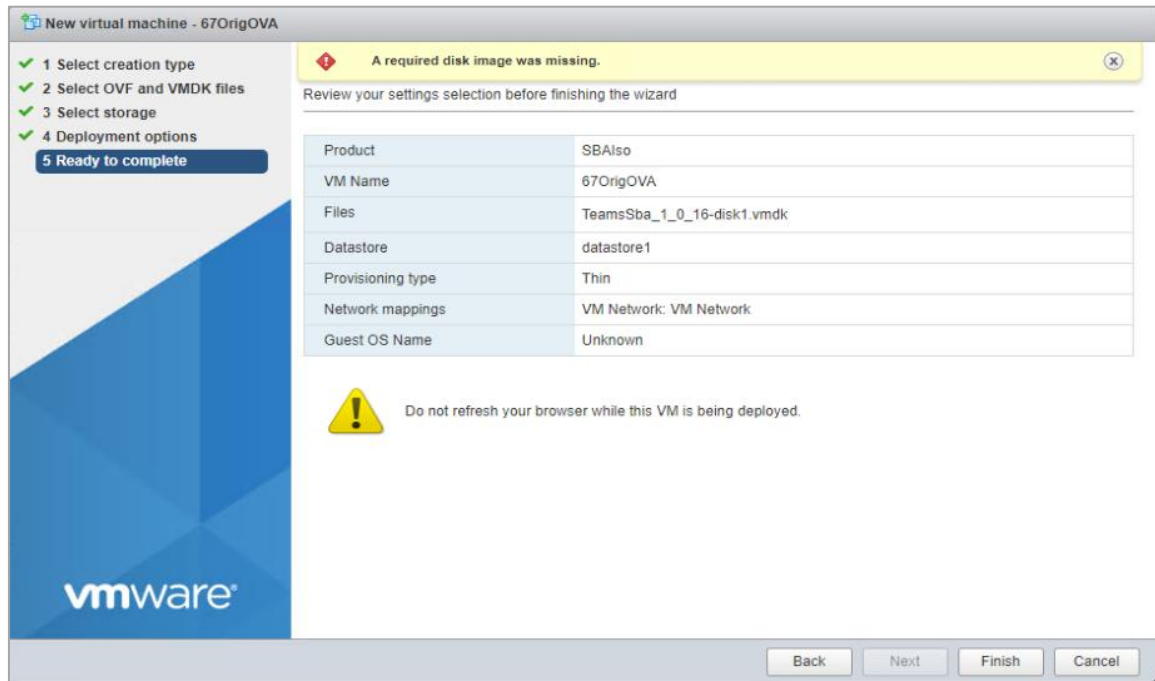
4. Select **Standard** datastore and then click **Next**.

Figure 21: Deployment Options



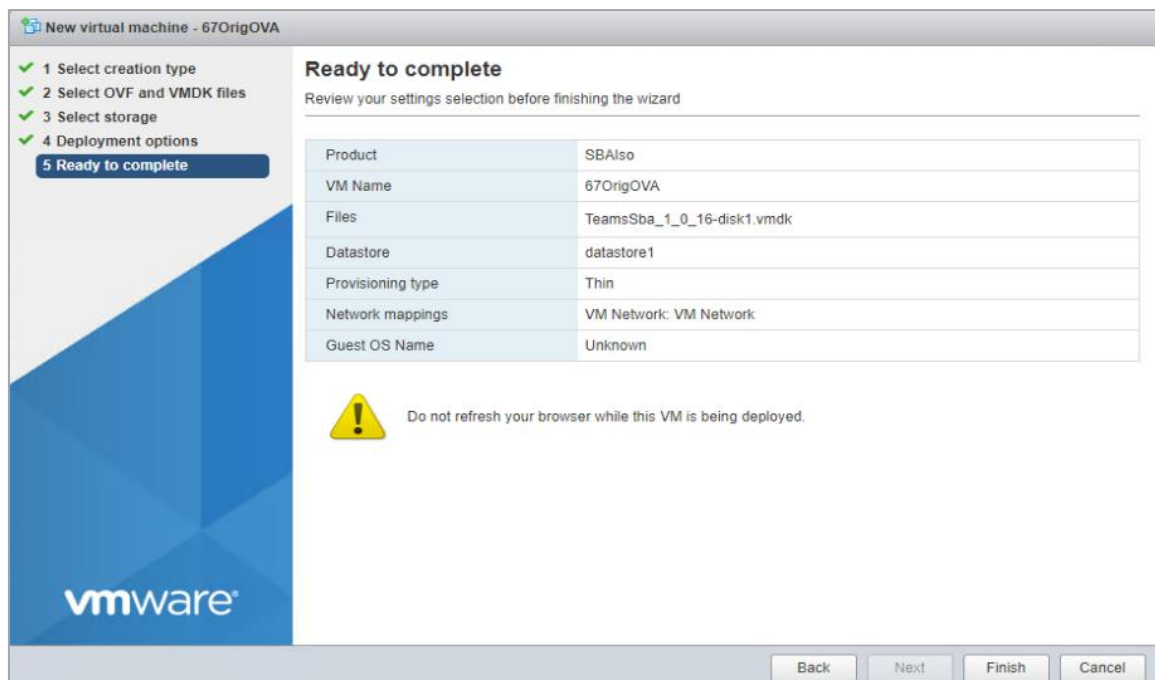
5. Configure the following options and then click **Next**:
 - From the Network mappings drop-down list, select **VM Network**.
 - For the Disk provisioning option, select **Thick**.
 - Select the Power on automatically checkbox.
 - The following screen appears during the deployment process.

Figure 22: Ready to complete



The error message displayed in the figure above can be ignored.

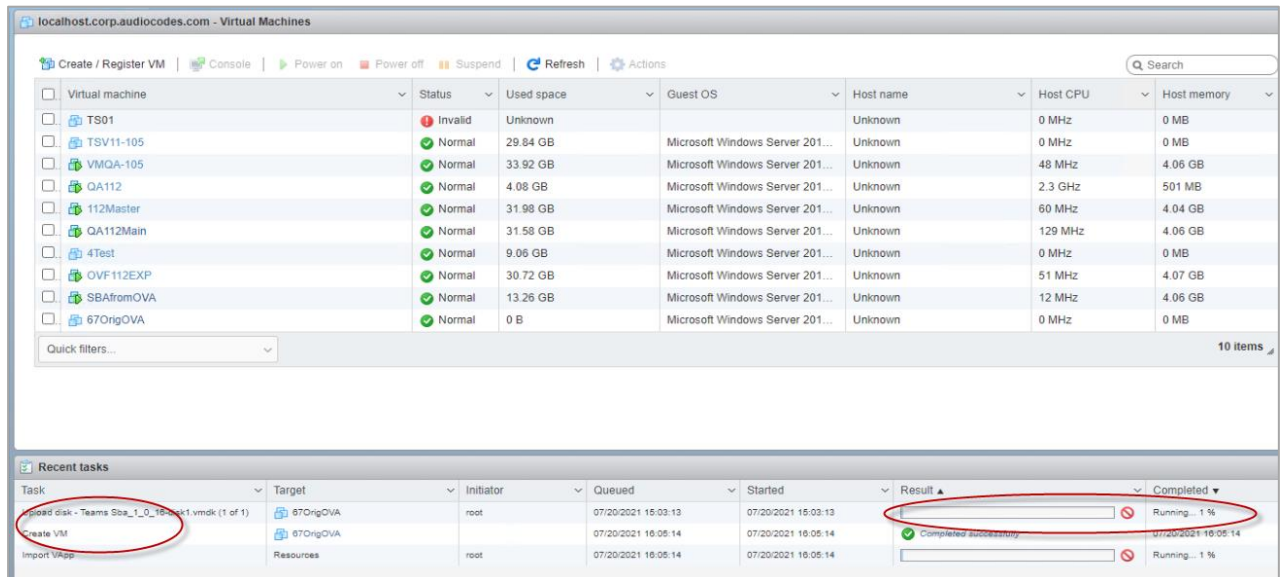
Figure 23: Review Settings



6. Review the settings and then click **Finish**.

The new virtual machine is created.

Figure 24: New Virtual Machine Added



The progress of the running task is displayed in the lower pane of the above screen. Once the virtual machine is created, it is added to the list in the top pane.

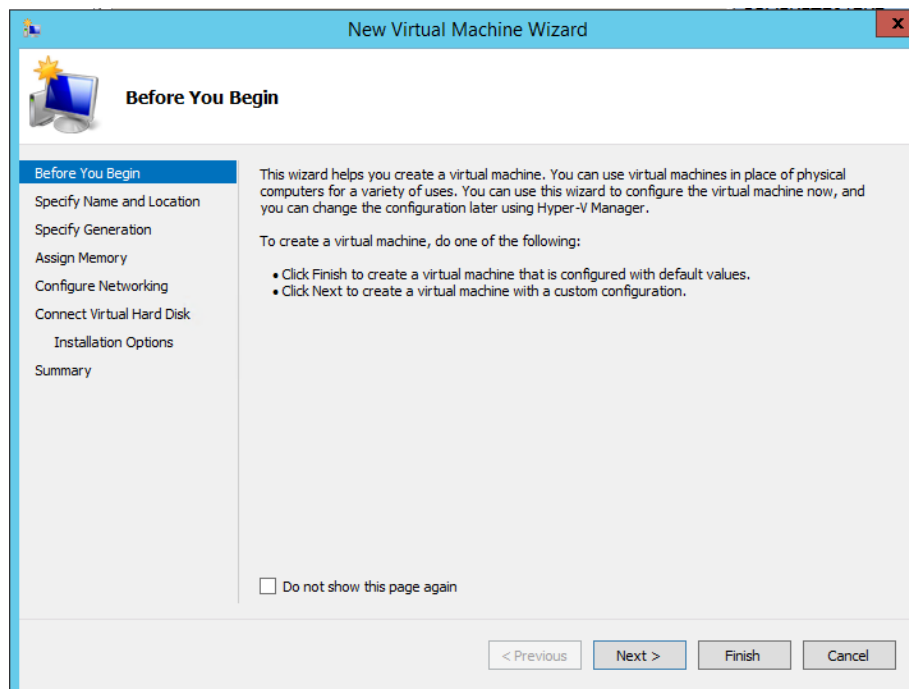
5.2 Deploying DR-SBA Image with Hyper-V Hypervisor

This section describes how to deploy the DR-SBA Image on the Hyper-V hypervisor virtual appliance.

To deploy the DR-SBA image with Hyper-V hypervisor:

1. Download the VHDX file containing the DR-SBA image to the virtual machine (see Section 2.3).
2. Open the Hyper-V management console and then click **Next**.

Figure 25: New Virtual Machine



3. Name the new virtual server.

Figure 26: Specify VM Name and Location

The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Specify Name and Location' step. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions: 'Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.' The 'Name' field is filled with 'Virtual Teams DR SBA VHDx'. Below, it says 'You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.' There is an unchecked checkbox 'Store the virtual machine in a different location'. The 'Location' field shows 'C:\ProgramData\Microsoft\Windows\Hyper-V\' with a 'Browse...' button. A warning icon and text state: 'If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.' At the bottom are buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

4. Select the **Generation 1** radio button and then click **Next**.

Figure 27: Specify Generation

The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Specify Generation' step. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation' (highlighted), 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions: 'Choose the generation of this virtual machine.' There are two radio buttons: 'Generation 1' (selected) and 'Generation 2'. Under 'Generation 1', it says 'This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.' Under 'Generation 2', it says 'This virtual machine generation provides support for features such as Secure Boot, SCSI boot, and PXE boot using a standard network adapter. Guest operating systems must be running at least Windows Server 2012 or 64-bit versions of Windows 8.' A warning icon and text state: 'Once a virtual machine has been created, you cannot change its generation.' At the bottom are buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

5. Assign memory (8G minimum).

Figure 28: Assign Memory

The screenshot shows the 'Assign Memory' step of the 'New Virtual Machine Wizard'. The wizard has a blue title bar and a sidebar on the left with the following steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation', 'Assign Memory' (highlighted), 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains the following text: 'Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 2560 MB. To improve performance, specify more than the minimum amount recommended for the operating system.' Below this, there is a 'Startup memory:' label followed by a text box containing '2048' and 'MB'. A checkbox labeled 'Use Dynamic Memory for this virtual machine.' is present and unchecked. An information icon (i) is followed by the text: 'When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

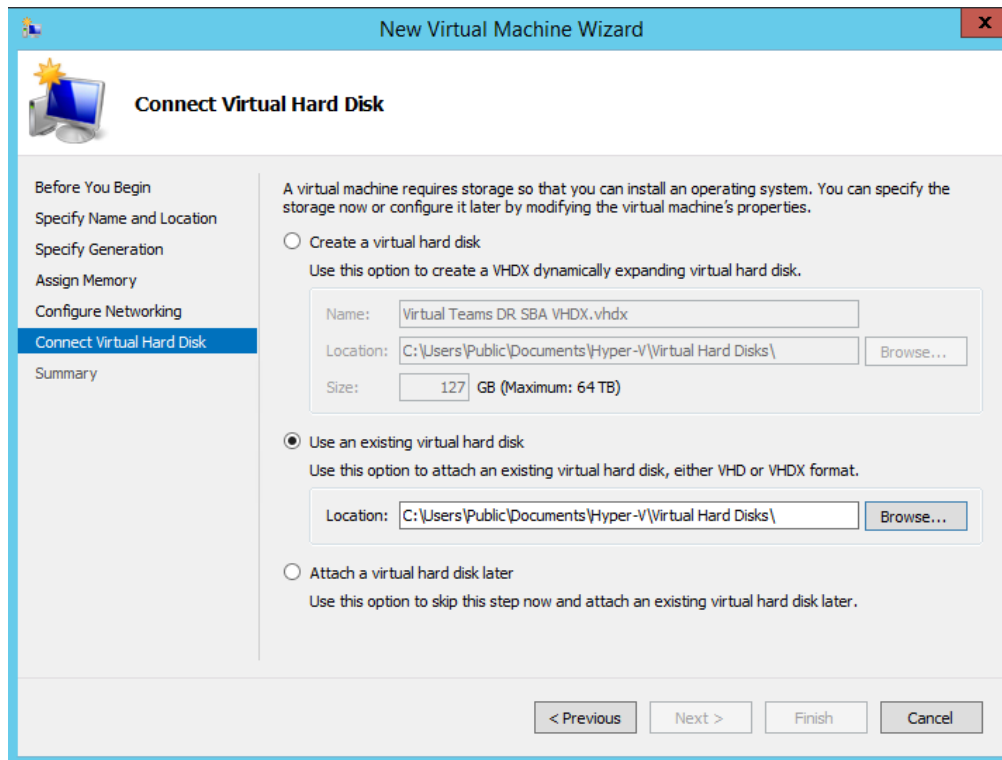
6. Configure the available network interface:

Figure 29: Configure Networking

The screenshot shows the 'Configure Networking' step of the 'New Virtual Machine Wizard'. The wizard has a blue title bar and a sidebar on the left with the following steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation', 'Assign Memory', 'Configure Networking' (highlighted), 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains the following text: 'Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.' Below this, there is a 'Connection:' label followed by a dropdown menu showing 'New Virtual Switch'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

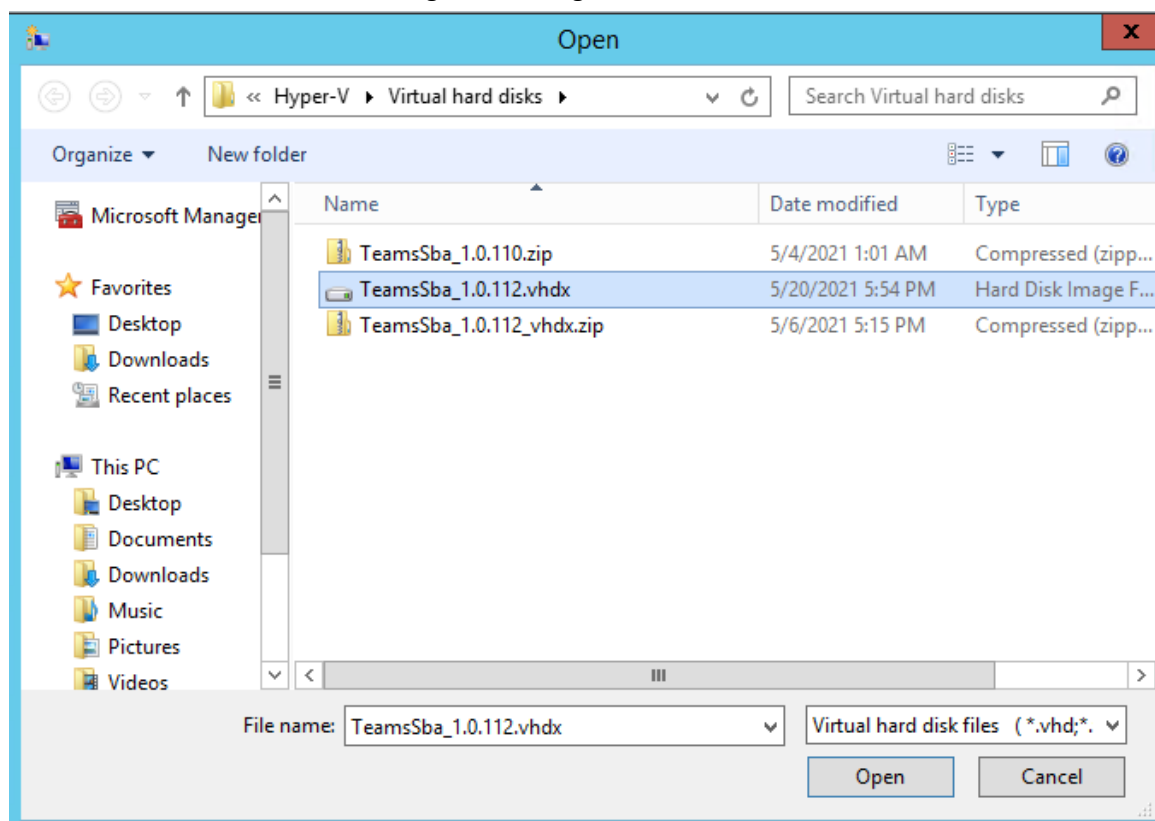
7. Chose to use an existing virtual hard disk and click **Browse**.

Figure 30: Connect Virtual Hard Disk



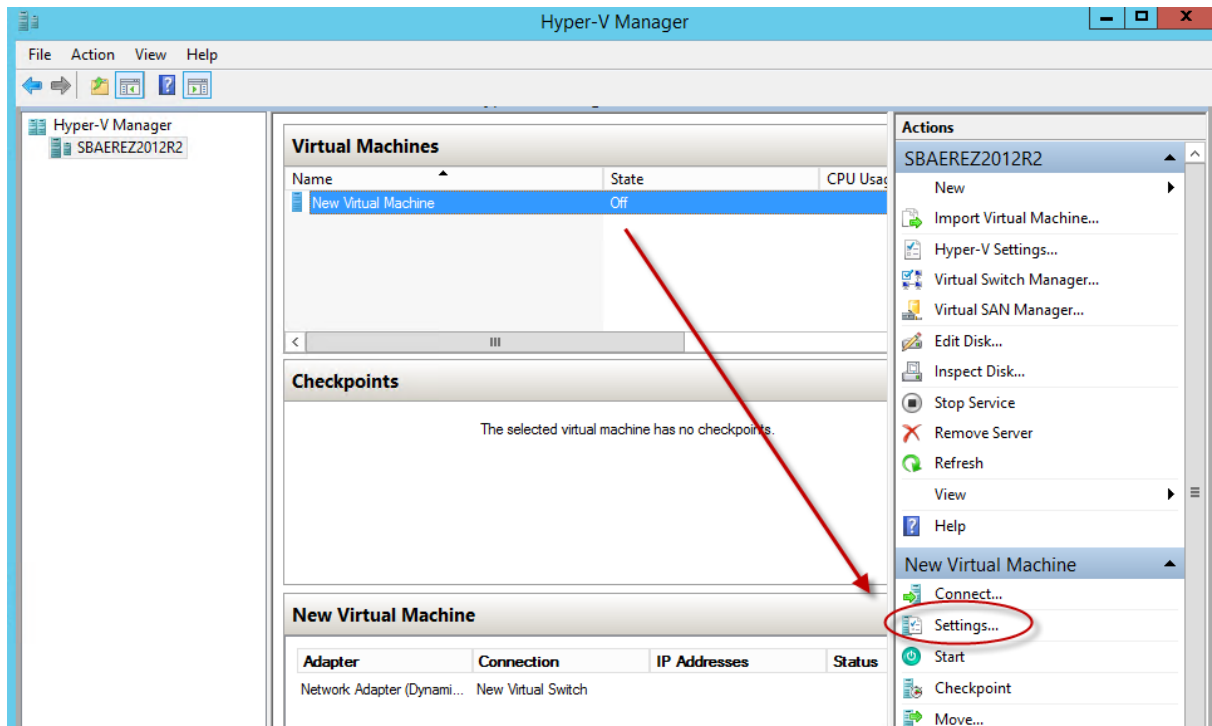
8. Navigate to the location of the vhd file you downloaded and copied to the hypervisor server.

Figure 31: Navigate to VHDX File



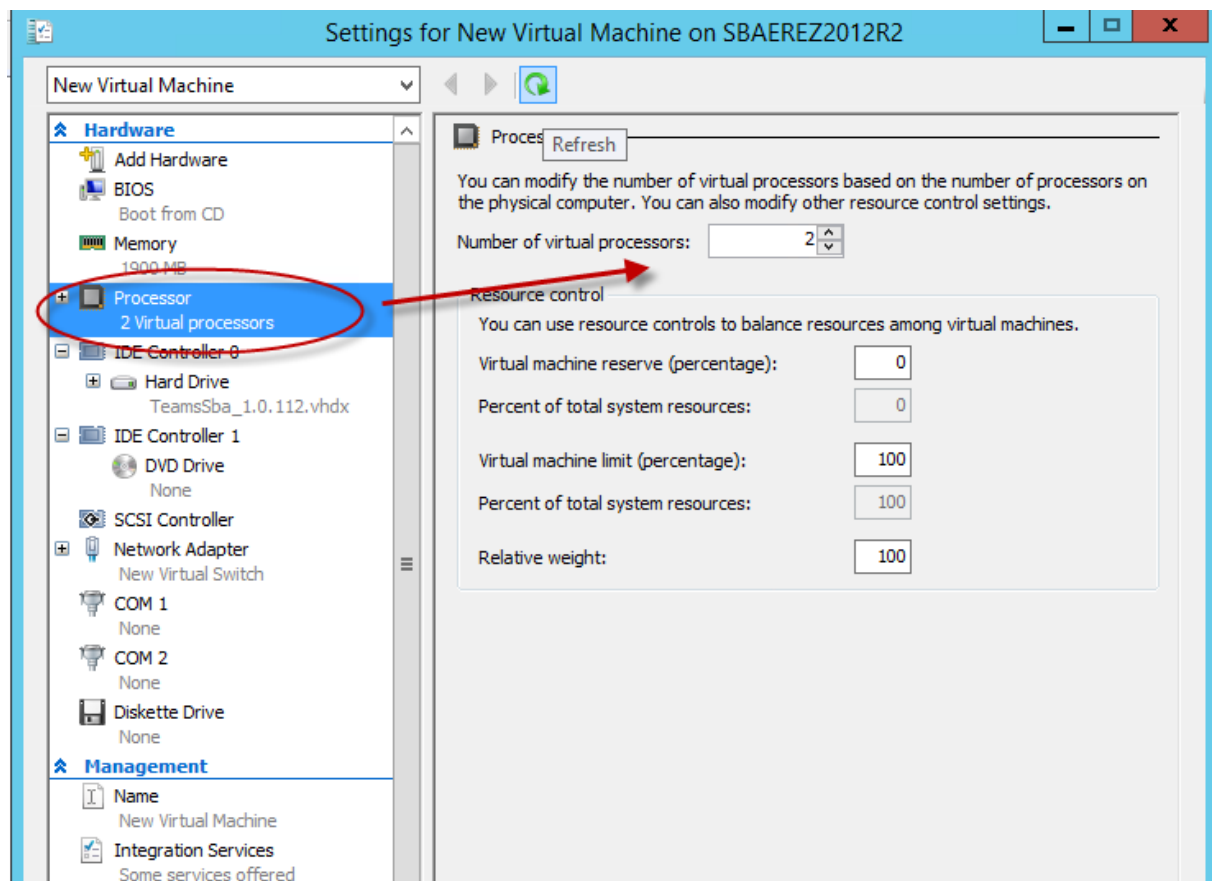
9. After the Hyper-V's new virtual server has been created, click **Settings**:

Figure 32: Settings



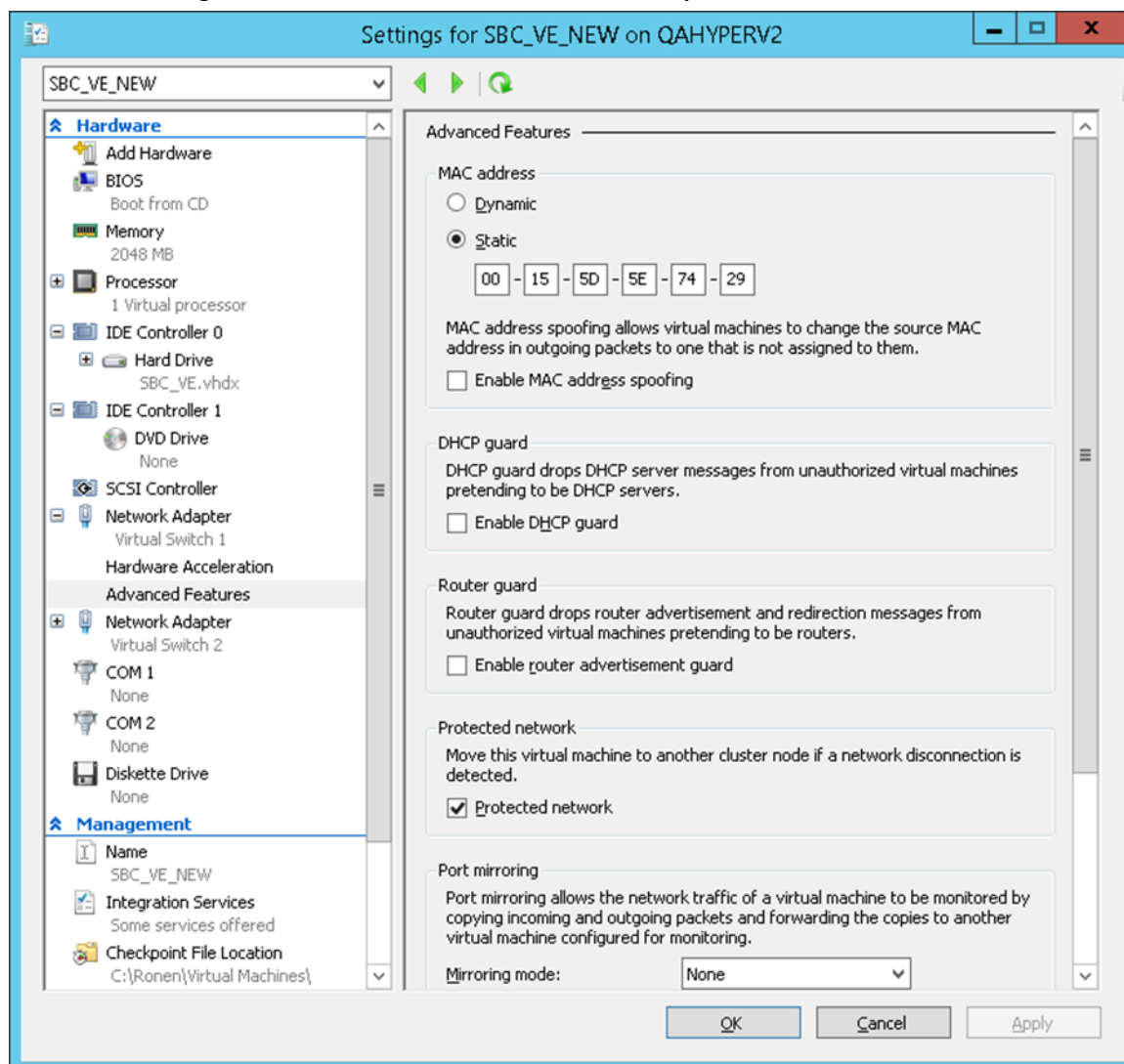
10. Click 'Processor' and set the number of processor cores (minimum 2):

Figure 33: Number of Virtual Processors



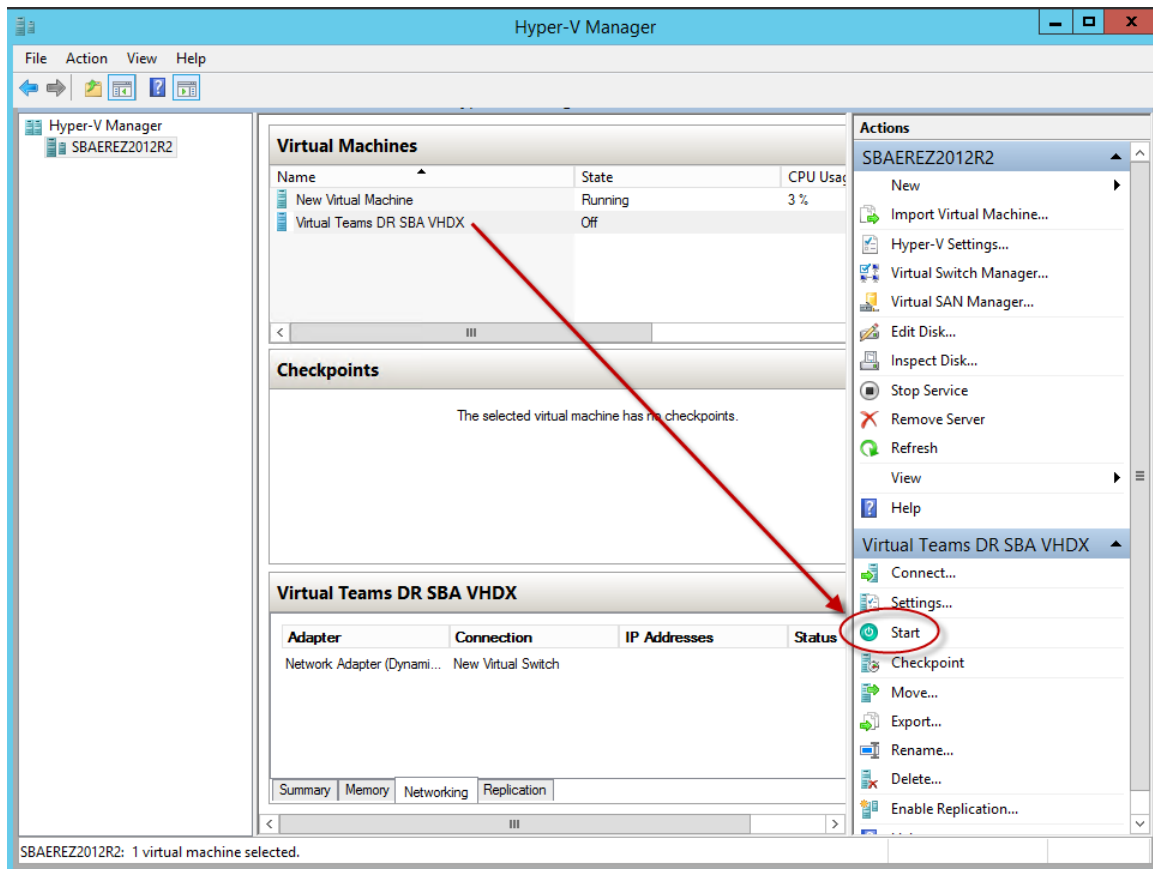
11. This paragraph describes how to change MAC Addresses from 'Dynamic' to 'Static'. By default, the MAC addresses of the SBC Virtual Machine are set dynamically by the hypervisor. Consequently, they might be changed under certain circumstances – for example, after moving the virtual machine between Hyper-V hosts. To prevent this, it's advisable to change the MAC Addressees from Dynamic to Static.
12. This paragraph shows how to change the MAC address to **Static** in Microsoft Hyper-V.
 - i. *Turn-off* the SBC virtual machine.
 - ii. Enter the **Settings** of the selected SBC virtual machine.
 - iii. For each Network Adapter, do the following:
 - a. Choose Advanced Features
 - b. Change the 'MAC address' option to **Static**.

Figure 5-34: Advanced Features - Network Adapter – Static MAC Address



13. When the new virtual machine is ready, click **Start** to start the server.

Figure 35: Start Virtual Machine



5.3 Authentication Method for the SBA Management Interface

The authentication method used by the SBA Management Interface depends on whether the SBA machine is joined to a domain.

Non-Domain-Joined SBA Machines

When the SBA is not joined to a domain, user credentials entered on the SBA web interface are validated against the local Windows accounts configured on the SBA server.

Domain-Joined SBA Machines

When the SBA is joined to a domain, the SBA web interface authenticates users against one of the following sources, depending on the format and context of the credentials entered (as occurs during standard Windows login):

- The customer's corporate Active Directory
- The local Windows accounts

This dual-mode authentication provides flexibility for environments with or without centralized identity management.

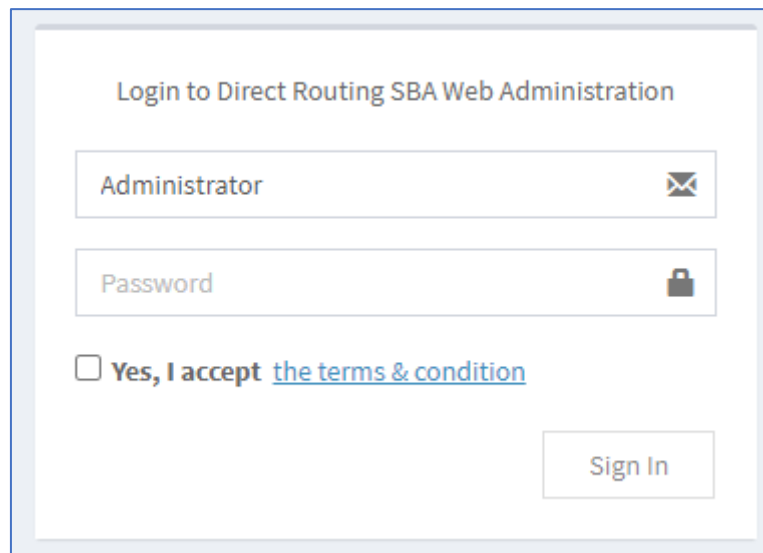
5.4 Logging into DR-SBA and Enabling DR-SBA License

This section describes the initial login to the DR-SBA Web browser and DR-SBA license activation.

To login to DR-SBA and enable license:

1. Login via web browser to the DR- SBA IP with the following credentials:
 - User: **Administrator**
 - Password: **Pass123**

Figure 36: Login



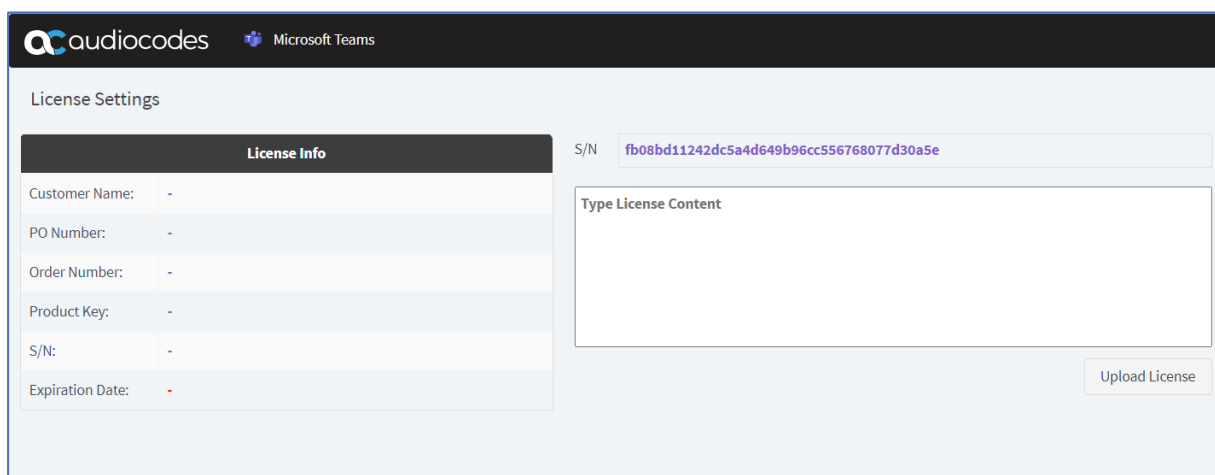
The login form is titled "Login to Direct Routing SBA Web Administration". It contains two input fields: "Administrator" with an eye icon and "Password" with a lock icon. Below these fields is a checkbox labeled "Yes, I accept" followed by a blue link "the terms & condition". A "Sign In" button is located at the bottom right of the form.



The above user and password are the DR-SBA Windows local Administrator default account.

The following screen is applicable only for the Virtual Edition:

Figure 37: License Settings



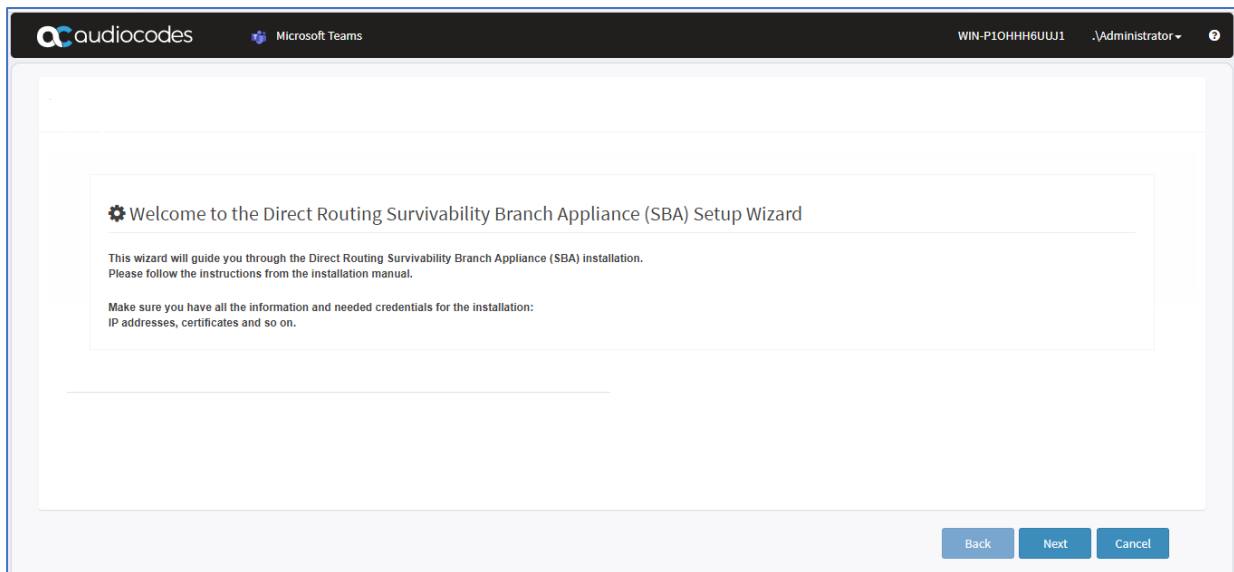
The "License Settings" screen features the Audiocodes and Microsoft Teams logos at the top. It includes a "License Info" table with fields for Customer Name, PO Number, Order Number, Product Key, S/N, and Expiration Date, all showing dashes. To the right, there is an "S/N" field containing the value "fb08bd11242dc5a4d649b96cc556768077d30a5e" and a "Type License Content" text area. An "Upload License" button is positioned at the bottom right.

License Info	
Customer Name:	-
PO Number:	-
Order Number:	-
Product Key:	-
S/N:	-
Expiration Date:	-

Upon initial login, you are prompted to enter the DR-SBA license. The license is mandatory to install; without the license you can't proceed to the next setup wizard page.

2. Copy the Serial Number (S/N) from the License Settings screen (see figure above). Proceed to Section 5.4.1 for Licensing activation.

3. Load the license and proceed to the Welcome page.
4. After login the Wizard opens. You can close the wizard by clicking cancel and returning to it from a key on the top bar.

Figure 38: Welcome Page

5. Click **Next** to continue.

5.4.1 Licensing the Product

Once you have successfully completed DR-SBA Virtual Teams virtual machine deployment, you need to obtain, activate and then install your purchased DR-SBA license key file.



- This license is only relevant for the DR-SBA Virtual Appliance.
- License activation is intended only for first-time software activation upon product purchase (or if your License Key is "lost", due to whatever reason).

To obtain and activate the License Key:

1. Open AudioCodes Web-based Software License Activation tool at <http://www.audiocodes.com/swactivation>:

Figure 39: Software License Activation Tool

The screenshot shows the 'Software License Activation' page of the AudioCodes website. The page has a dark blue header with the AudioCodes logo and a search icon. Below the header, there is a breadcrumb trail 'Home > Software License Activation'. The main heading is 'Software License Activation'. Below this, there is a text block stating: 'Please enter your Product Key received from AudioCodes and the fingerprint (e.g. Serial Number or Server Machine ID) that was generated as a result of your installation. For technical assistance, please contact AudioCodes support at support@audiocodes.com. *Supports CloudBond 365 version 7.2 and above.' The form contains three input fields: 'Product Key' with the value '8B0521934FF13DN8', 'Fingerprint' with a placeholder text 'For instructions on how to locate your product's fingerprint, please read the documentation relevant to your product', and 'Email' with a placeholder text. There is a green circular button with a plus sign next to the email field. At the bottom of the form, there is a checkbox labeled 'I'm not a robot' and a reCAPTCHA logo. A green button labeled 'Get in touch' is located at the bottom right of the page.

En

audiocodes

Home > Software License Activation

Software License Activation

Please enter your Product Key received from AudioCodes and the fingerprint (e.g. Serial Number or Server Machine ID) that was generated as a result of your installation.
For technical assistance, please contact AudioCodes support at support@audiocodes.com.
**Supports CloudBond 365 version 7.2 and above.*

Product Key *

8B0521934FF13DN8

Fingerprint *

For instructions on how to locate your product's fingerprint, please read the documentation relevant to your product

Email *

☐ I'm not a robot

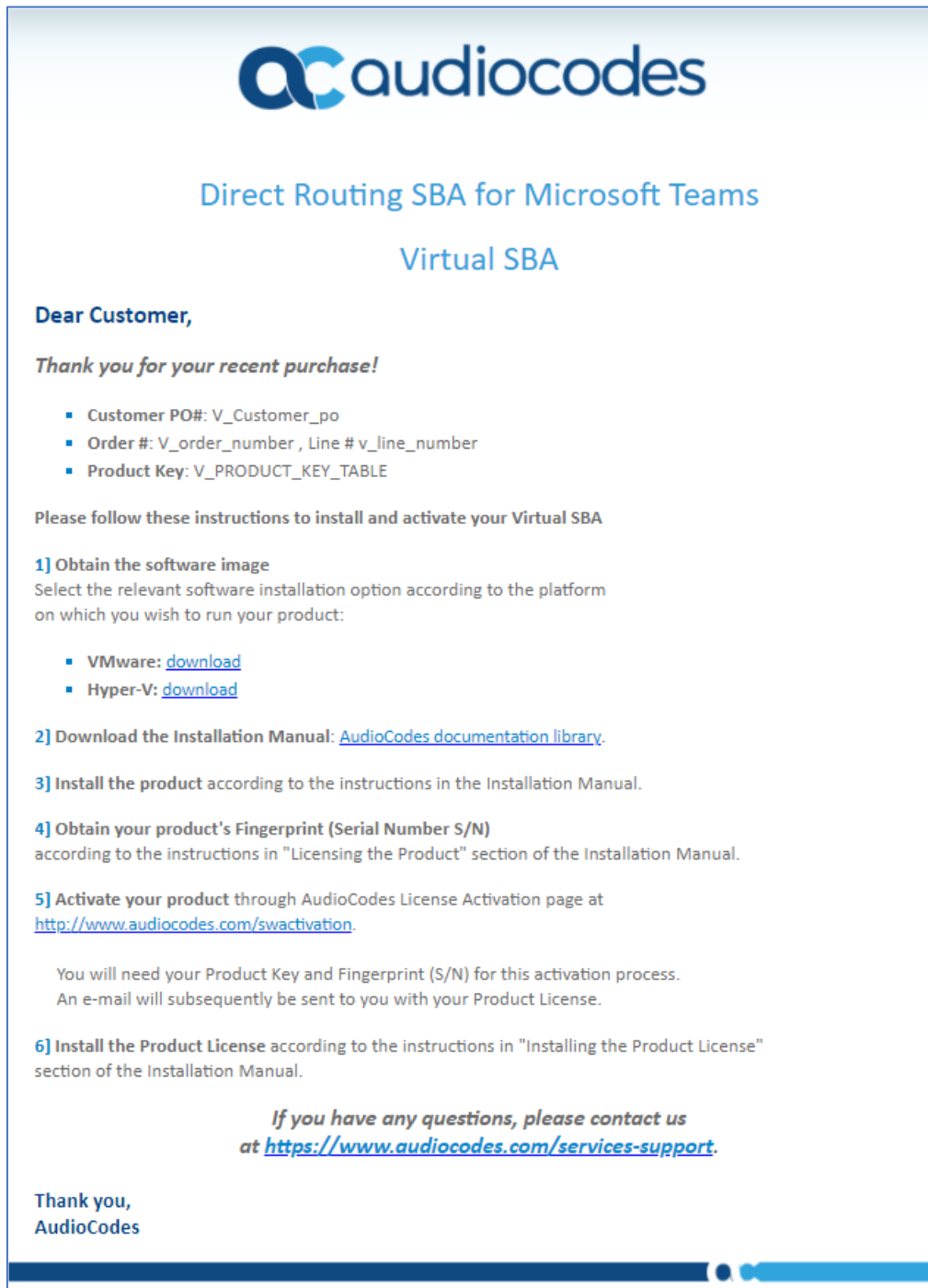
reCAPTCHA
Privacy · Terms

Get in touch

2. Enter the following information:

- **Product Key:** The Product Key identifies your specific DR-SBA purchase for the purpose of subsequent communication with AudioCodes (for example, for support and software upgrades). The Product Key is provided in the Order Confirmation e-mail sent to you by AudioCodes upon your purchase, as shown in the example below:

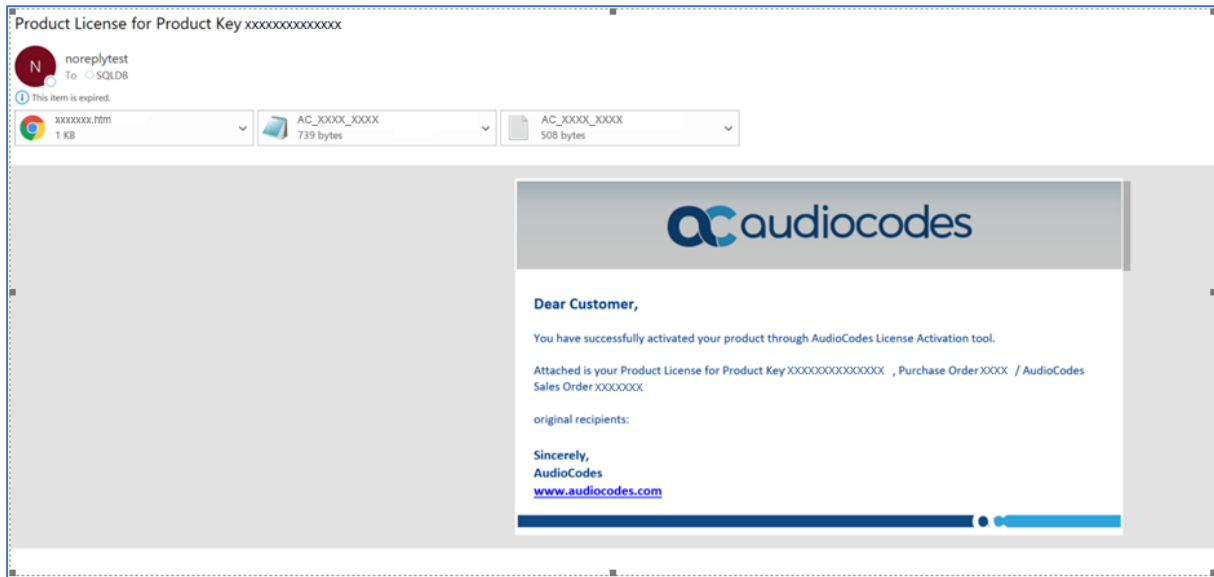
Figure 40: Product Key in Order Confirmation E-mail



- **Fingerprint:** The fingerprint is the DR-SBA's Serial Number (S/N) which can be extracted from the License Settings screen (see Section 5.3). This ID uniquely identifies the software installation.
- **Email:** Provide one or more e-mail addresses to where you want the License Key to be sent.

3. Click **Send** to submit your license activation request.
4. Once AudioCodes processes and completes your license activation, you will receive an e-mail notification with the License Key file attached. Open the file with any text-based program (such as Notepad) and make sure that the serial number ("**S/N**") in the License Key is correct and reflects the Serial Number of your DR-SBA displayed in the License Settings screen.

Figure 41: Email Confirmation with new License Key



Do not modify the contents of the DR-SBA License Key file.

5. Proceed to Step 1.3 in Section 5.3.

5.5 Network Setup

This section describes the Network Interface Setup.

To setup the network:

1. Disable the non-used NIC – Its recommended to have only one NIC enabled network card. (On the Virtual Edition, there is only one NIC by default).
2. Click **Next**.
3. Set the IP address as required for the interface that is used (or do it directly via RDP)
You can skip this step if the network has been setup correctly.

Figure 42: Network Interface Setup (OSN-Based Setup)

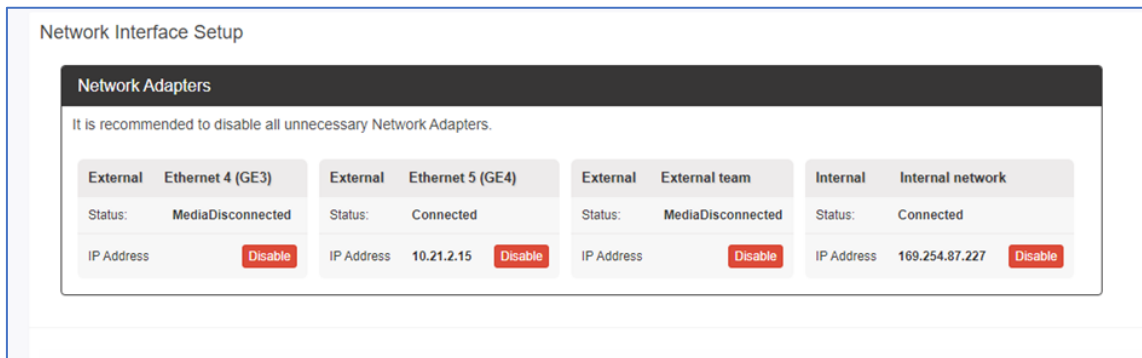


Figure 43: Network Interface Setup (Virtual Machine-Based Setup)

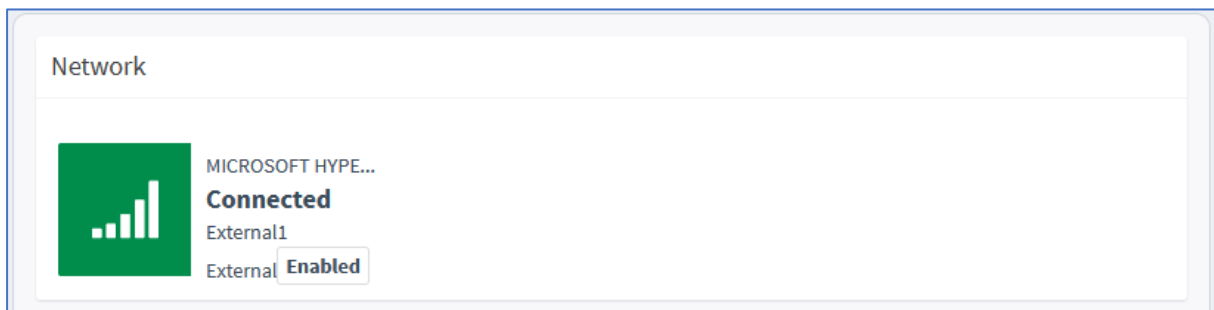


Figure 44: Direct Routing DR-SBA LAN Setup

Direct Routing SBA LAN Setup

Wizard will be automatically reconnected to external network interface card.

Select a Network Interface Card

GE1

Use the following IP address

IP Address

Subnet Mask

Default Gateway

Use the following DNS server address

Preferred DNS Server

Alternate DNS Server



After changing the Teams DR-SBA IP, you need to restart the Microsoft service. Restart the service also when you update the current IP address of the server. There is no need to restart the service while running the Setup through the initial setup wizard.

Whenever you change the IP address, you need to modify the same/new IP address in the 'SIP Listen IP' dropdown list, as described in Section 5.10.2 on page 42.

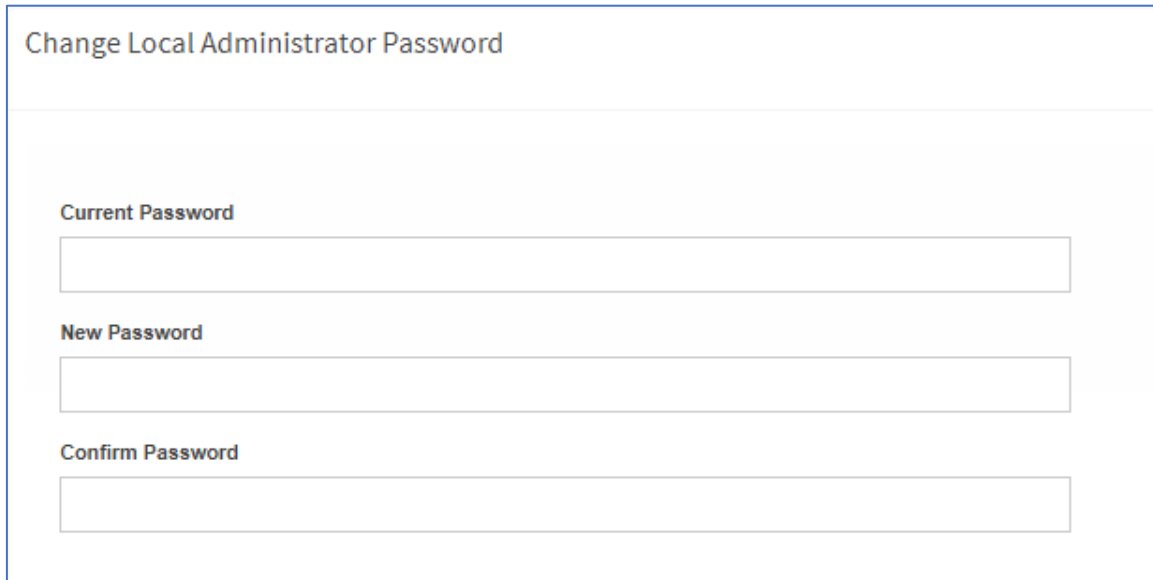
5.6 Change Local Administrator Password

The default password is **Pass123**, which is recommended that you change.



You can skip this step if you wish to retain the old password.

Figure 45: Change Local Admin Password



Change Local Administrator Password

Current Password

New Password

Confirm Password

5.7 Set Date and Time

1. Set the correct date/time/time zone. Make sure that you have access to NTP (by default, global NTP is used for workgroup: time.windows.com).



When the DR-SBA is in the workgroup, the NTP can be set via cmd when you RDP to the DR-SBA.

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\w32time\Parameters" -Name "NtpServer" -Value "ntp.server,0x8"
```

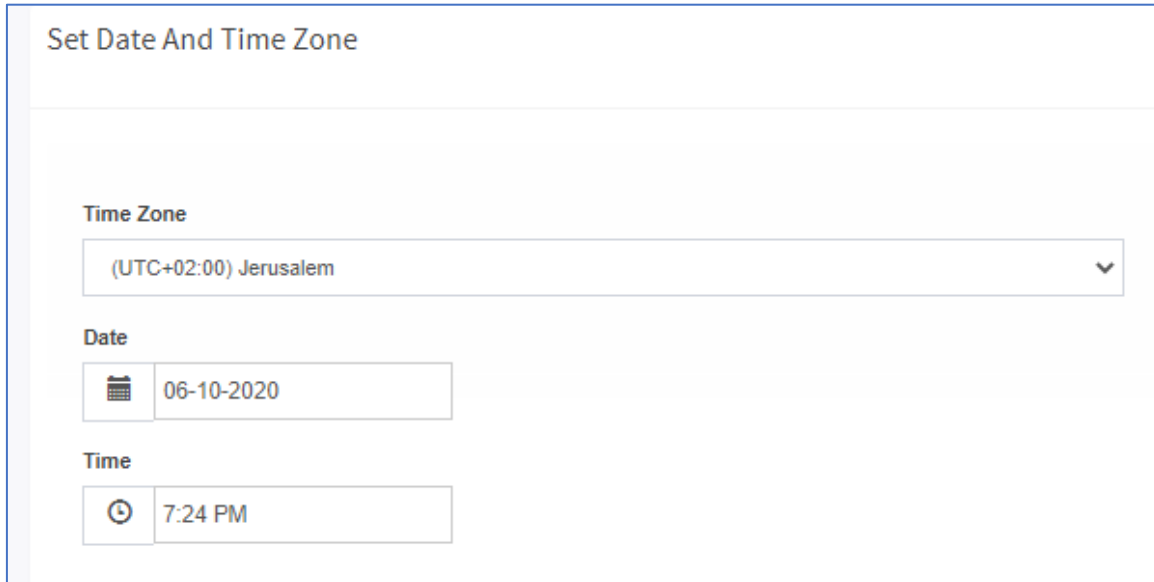
2. Restart # restart Windows Time service:

```
Restart-Service w32Tim
```



You can skip this step if the date/time are already set.

Figure 46: Set Date and Time Zone



Set Date And Time Zone

Time Zone

(UTC+02:00) Jerusalem

Date

06-10-2020

Time

7:24 PM

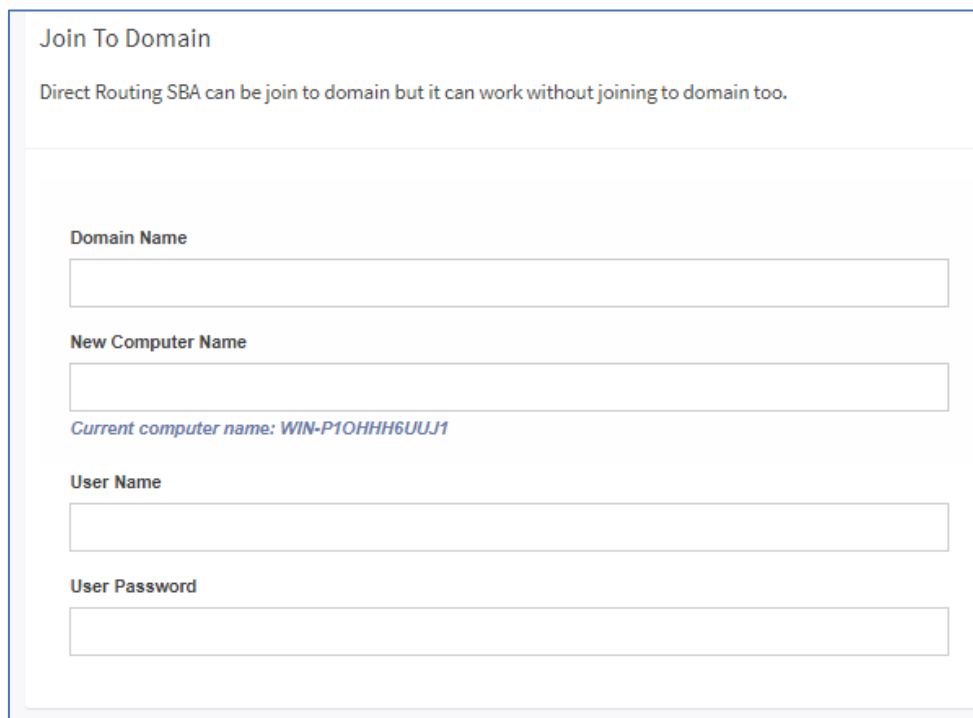
5.8 Join to Domain

You can join to the domain if its required. The Teams DR-SBA can run in Workgroup mode as well.



This step is optional.

Figure 47: Change Local Admin Password



Join To Domain

Direct Routing SBA can be join to domain but it can work without joining to domain too.

Domain Name

New Computer Name

Current computer name: WIN-P1OHHH6UUJ1

User Name

User Password

5.9 Log in to Teams

This section describes how to log in to Microsoft Teams.

To login to Microsoft Teams:

1. Enter Tenant (Teams) Admin/Password. You must use Teams Admin without MFA.
 - Customers can alternatively supply Tenant ID as Teams Admin credentials (select the 'Set DR-SBA without enter Teams Tenant Administrator' check box to enable this mode).
 - To obtain the Tenant ID, enter the following Online PowerShell command:

```
Get-CsTenant
```
2. If you enter tenant Admin/Password, click Login credentials (this may take some time). Once successfully logged in, a short message notification that you have logged in successfully is displayed and tenant information is displayed in "Last Login tenant information" section (see below) – click **Next**.

Figure 48: Login to Teams (User & Password)

Direct Routing SBA Tenant Credential

<input type="checkbox"/> Set DR SBA without enter Teams Tenant Administrator	<input type="text" value="Type tenant ID"/>	
Teams Administrator	<input type="text" value="Enter name"/>	<input type="button" value="Login"/>
Password	<input type="text" value="Enter password"/>	

Last login tenant information

Account	
Environment	

Figure 49: Login Direct Routing DR-SBA Tenant Credential (Set DR-SBA)

Direct Routing SBA Tenant Credential

Tenant Global Admin	<input type="text" value="Enter name"/>	<input type="button" value="Login"/>
Password	<input type="password" value="Enter password"/>	

Last login tenant information	
Account	<input type="text"/>
Environment	AzureCloud
Tenant Domain	<input type="text"/>

5.10 Add or Select Teams DR-SBA

Define the Teams DR-SBA and add it to Microsoft Teams. You can add the new Teams DR-SBA or use one that has already been defined on Teams directly via the PowerShell.

Don't select the same Teams DR-SBA that is already used on different active hardware. If you logged in without supplying the Teams admin username and password (see Section 5.9), you need to enter the FQDN manually without the option to add/select directly from the tenant.



Whether you add it through PowerShell or through the wizard, DR-SBA's FQDN should be written in lowercase.

5.10.1 Add DR-SBA via PowerShell

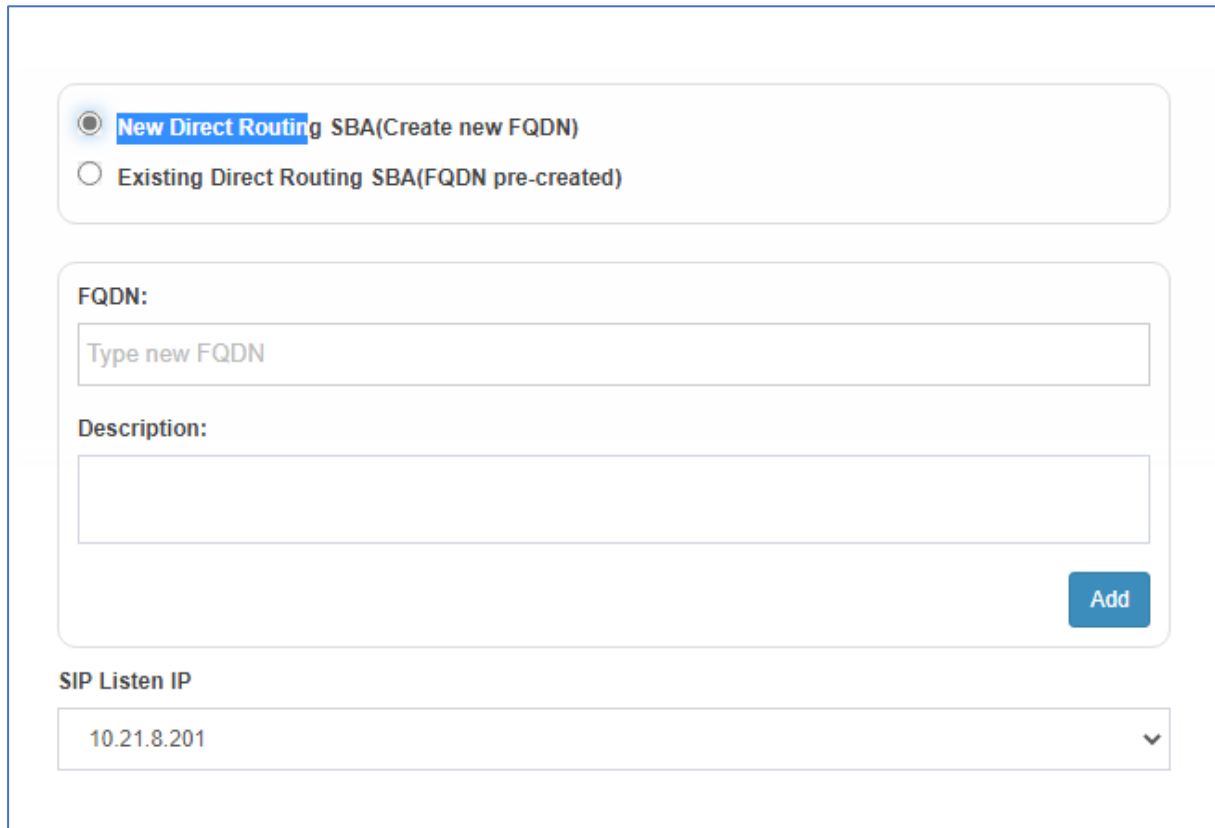
Add the DR-SBA via PowerShell directly, by entering the following command:

```
New-CsTeamsSurvivableBranchAppliance -Fqdn <sba FQDN> -Description "Description"
```

5.10.2 Add DR-SBA via Login to Tenant

1. If you are logged into a tenant without supplying the tenant's username and password, add the new DR-SBA FQDN:

Figure 50: Direct Routing DR-SBA Tenant Credentials



The screenshot shows a web form for adding a new Direct Routing SBA. At the top, there are two radio buttons: 'New Direct Routing SBA(Create new FQDN)' (which is selected) and 'Existing Direct Routing SBA(FQDN pre-created)'. Below this, there is a section for 'FQDN:' with a text input field containing the placeholder 'Type new FQDN'. Underneath is a 'Description:' section with a larger text area. To the right of the description field is a blue 'Add' button. At the bottom, there is a 'SIP Listen IP' section with a dropdown menu currently showing '10.21.8.201' and a downward arrow.

2. Enter the Teams DR-SBA FQDN and description (optional), and then click Add (this operation takes time due to the Teams connection).
3. From the 'SIP Listen IP' drop-down list, select on which IP address the DR-SBA listens for SIP transport.



Whenever you change the IP address, you need to modify the same/new IP address in the 'SIP Listen IP' dropdown list.

5.10.3 Select Existing Teams DR-SBA FQDN

If you wish to select the Teams DR-SBA FQDN that has already been defined for this DR-SBA:

1. Select the Existing Direct Routing SBA (FQDN pre-created) option.
2. Select the FQDN from the drop-down list and if you wish to update related data, for example, the SBA description, select the update key.
3. Proceed to step 6 below.

Figure 51: Existing Direct Routing DR-SBA

☐ New Direct Routing SBA(Create new FQDN)

☒ Existing Direct Routing SBA(FQDN pre-created)

FQDN:

sbaTeams.audctrunk.aceducation.info Delete

Description:

AUDC SBA IL| Update

SIP Listen IP

10.21.8.201

4. From the 'SIP Listen IP' drop-down list, select the IP address on which the DR-SBA listens for SIP transport.
5. When data has been updated, click **Next**.
6. If you selected to authenticate using the Tenant ID in Section (instead of logging with Tenant Username and password), enter the FQDN manually.

Figure 52: Enter FQDN

Create or Select Direct Routing SBA FQDN

FQDN:

sbaTeams164.audctrunk.aceducation.info

5.11 Teams DR-SBA Certificate

This section describes how to assign Teams DR-SBA certificates. Firstly, you must import a certificate, which can be done by importing a pfx file or by generating a CSR via the DR-SBA Web, have it signed and then imported.

5.11.1 Import PFX File

To import PFX file:

- Select **Import Certificate** and upload the PFX file (you must supply the private key password).

Figure 53: Import pfx file

5.11.2 Request CSR

To request CSR:

1. If you need to generate a CSR, you can click **Request CSR**.

Figure 54: DR-SBA Certificate

2. Fill the CSR fields.
3. If a CSR was generated, download the file by clicking on download key, sign the certificate and then import the signed certificate.

5.11.3 Assign Certificate

To assign certificate:

1. Click **Assign**, and then select the certificate you wish to use (DR-SBA looks for the certificate with CN = SBA FQDN). You should have one certificate with the same CN. If there is more than one certificate, delete those that are not relevant.



- The CA that is used must be trusted by the Teams clients and the SBC.
- If a Private CA is used, you need to verify that its CA is installed on the DR-SBA. Do this by importing a .p7b/.pfx certificate file with full certificate chain or directly via RDP.
- Certificate must include the SBA FQDN in the certificate CN and in the SAN.
- You can assign a Wildcard certificate.
- The DR-SBA creates a certificate for internal communication (localhost). Do not delete it. The certificate is unique to the system. Without it, the system will not work correctly.

2. Click **Assign** and select the certificate that you wish to use (the DR-SBA searches for the certificate according to the DR-SBA FQDN that was set in the previous step in this certificate) – you should have one certificate with the same common name (CN).



After changing the certificate, you need to reset the SBA Microsoft service.

There is no need to restart the service while running the Setup through the initial setup wizard. Restart the service only when you update the current server certificate.

5.12 Application ID and Application Secret

1. Enter the Application ID and application secret according to the App Registration that you defined on Azure AD.

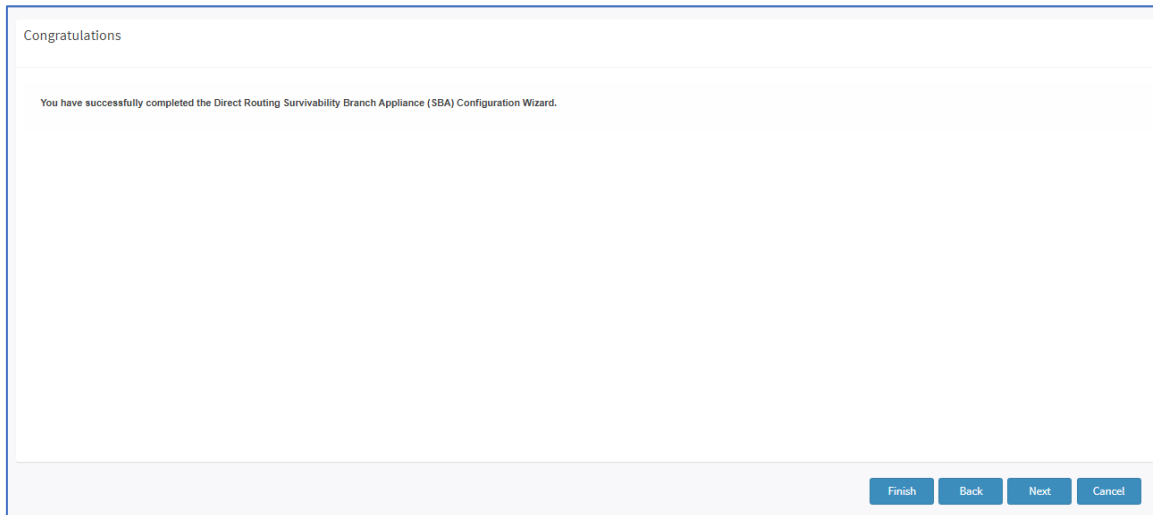
Figure 55: AD Application ID

The screenshot shows a web form titled "AD Application ID". It contains two input fields: "Application ID" and "Application Secret". The "Application ID" field has a placeholder text "Enter application ID" and the "Application Secret" field has a placeholder text "Enter Application secret".

AD Application ID	
Application ID	<input type="text" value="Enter application ID"/>
Application Secret	<input type="text" value="Enter Application secret"/>

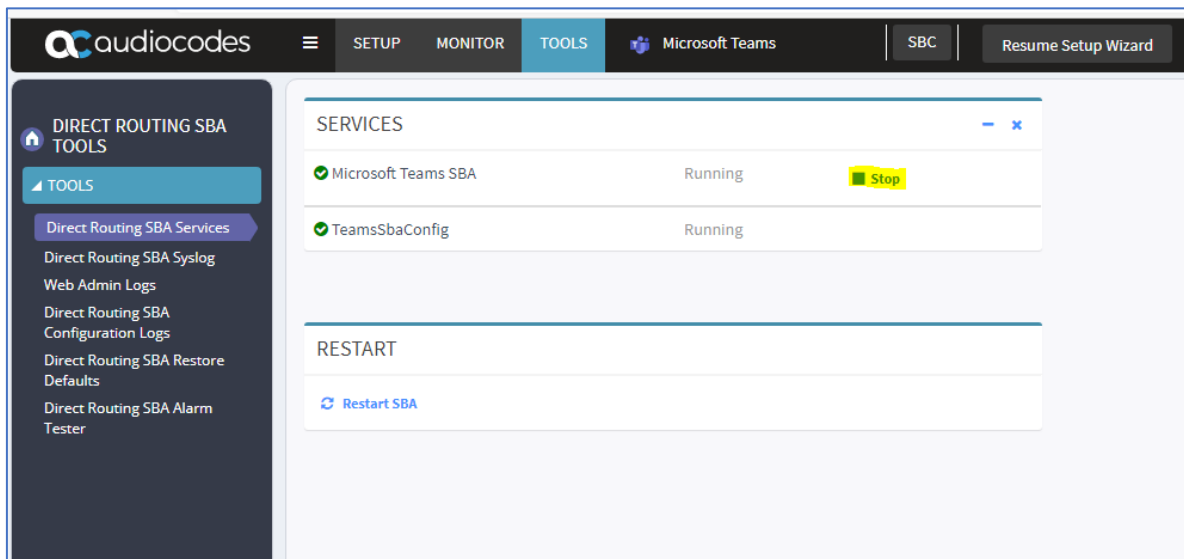
- Click **Next** to complete the setup of the DR-SBA.

Figure 56: DR-SBA is Ready



- Click **Finish** to close the Wizard.
- Due to a known issue, restart the "Microsoft Teams SBA service" after completing the wizard. This can be done from the Tools menu:

Figure 57: Microsoft Teams SBA service Restart



6 SBC Setup

Setup the SBC for Teams Direct Routing support with media bypass and validate that it works for incoming and outgoing calls. For configuration guidelines, refer to one of the following documents:

- **Enterprise Solution:** [Connecting AudioCodes' SBC to Microsoft Teams Direct Routing Enterprise Model](#)
- **Service Provider Solution:** [Connecting AudioCodes SBC to Microsoft Teams Direct Routing Hosting Model Configuration Note](#)

This chapter describes an example setup on how to configure the SBC setup to work with Teams DR-SBA. The setup can vary between customers and depends on the customer network topology. It represents common Enterprise topology. If you need to route calls via ARM or by using tagging, this requires a different setup, in which case, please contact AudioCodes Professional services for detailed guidelines.



The CA that is used to assign to the DR-SBA must be trusted by the Teams clients and the SBC. Add the Certificates on the SBC via the SBC Web interface.



Please continue to the next step only after you confirm that SBC is configured correctly and verify that Media bypass is enabled.

6.1 Add Proxy Set

This section describes how to add a Proxy Set for the DR-SBA.

Figure 58: Configuration Example Proxy Sets before the change

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method
1	SIPTrunk (arbitrary name)	SIPTrunk	Default	Using Options	-	-
2	Teams (arbitrary name)	Teams	Teams	Using Options	Enable	Random Weights

To add a Proxy Set:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** > **Proxy Sets**).
 - a. Click the **Add** button to create a Proxy Set for DR-SBA Teams Calls.
 - b. Use the same TLS context used by the Teams proxy – in this case the SBC uses the same certificate used on the Teams leg (the DR-SBA must trust the global CA that signed the SBC certificate).
 - c. From the 'Proxy Keep-Alive' drop-down list, select **Using OPTIONS** to discover whether a particular Mediation Server in the cluster is available and set Proxy Keep-Alive Time (secs) to 60 seconds.
 - d. Click **Apply** to apply your settings.

Figure 59: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC Ipv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method
1	SIPTrunk (arbitrary name)	SIPTrunk	Default	Using Options	-	-
2	Teams (arbitrary name)	Teams	Teams	Using Options	Enable	Random Weights
3	Teams (arbitrary name)	Teams	Teams	Using Options	Enable	-

6.1.1 Configure Proxy Addresses

This section shows how to configure a Proxy Address.

To configure a Proxy Address for DR-SBA Teams:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**), click the Proxy Set **SBA Teams**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 60: Configuring Proxy Address for Teams Direct Routing SBA Interface

The screenshot shows a configuration window titled 'GENERAL'. It contains five input fields:

- Index:** A text box containing the value '0'.
- Proxy Address:** A text box containing the value 'Teams SBAs FQDNs :5061'.
- Transport Type:** A dropdown menu with 'TLS' selected.
- Proxy Priority:** A text box containing the value '0'.
- Proxy Random Weight:** A text box containing the value '0'.

3. Configure the address of the Proxy Set according to the parameters described in the table below:

Figure 61: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	Teams DR-SBA FQDN:5061 (DR-SBA FQDN / port)	TLS	0	0

4. Click **Apply**.



The proxy set should connect to SIP interface that must listen on TLS 5061 and must be routable to DR-SBA.



If the DNS used by the SBC can't resolve the DR-SBA FQDN, add the DR-SBA FQDN to the SBC local DNS.

6.1.2 Add IP Group

This step describes how to configure an SBC IP Group to the DR-SBA. The IP Group represents an IP entity on the network with which the SBC communicates. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In the SBC topology, IP Groups must be configured for Teams DR-SBA.

To create an IP Group for Teams DR-SBA:

1. Open the IP Group table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Click **New** to create an IP Group of Type 'Server' for the Teams SBAs:
 - a. Configure the DR-SBA Proxy Set that you created in Section 6.16.1
 - b. Select the same IP Profile as used for Teams IP Group. If you create a new IP Profile pay attention and configure as set for Teams side with ICE Mode set to **Lite**.
 - c. Select Media Realm for the LAN side – media between the Teams clients and the SBC.
 - d. Configure the SBC FQDN for the SIP Group Name (Local Host Name). Use the same FQDN that is used for the SBC direct routing setup in Teams Tenant.
 - e. Enable **Proxy Keep-Alive using IP Group settings**.
 - f. Click **Apply** to apply your settings.

Figure 62: Configured IP Group for Teams SBA

Parameter	Value
Name	DR-SBA
Type	Server
Proxy Set	DR-SBA
IP Profile	Teams (same profile as used for Teams IP Group)
Media Realm	MRLan (Select Media Realm for the LAN side)
SIP Group Name	<FQDN name of the SBC in the enterprise tenant> Use the same FQDN that is used for the SBC direct routing setup in Teams Tenant
Local Host Name	<FQDN name of the SBC in the enterprise tenant> Use the same FQDN that is used for the SBC direct routing setup in Teams Tenant
Proxy Keep-Alive using IP Group settings	Enable
All other parameters can be left unchanged with their default values.	

6.2 Terminate SIP OPTIONS and Refer

Validate that the IP-to-IP Routing rules that were added for Microsoft Teams for SIP OPTIONS and REFER are valid for Teams DR-SBA as well or add the same routing for the Teams SBA IP Group.

6.3 Add IP-to-IP Routing from Teams DR-SBA to PSTN

Add IP-to-IP Routing from Teams DR-SBA to PSTN/SIP Trunk.



A separate configuration is required per SIP Trunk.

6.4 Add Forking for PSTN Calls to Teams and Teams DR-SBA

This step describes how to configure forking IP-to-IP call routing rules for incoming PSTN calls.

To configure forking IP-to-IP routing for Teams:

1. Open the IP-to-IP Routing page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Click **Edit** to modify rule for routing from PSTN to Teams:
 - a. Set Group Policy to **Forking**.
 - b. Click **Apply** to apply your settings.
3. Click **New** to create a new rule for routing from PSTN to Teams DR-SBA:
 - a. Set Group Policy to **Forking**.
 - b. Set Alternative Route Options to **Group Member Consider Inputs**.
 - c. Set destination IP Group as the DR-SBA IP Group
 - d. Set source IP Group as the PSTN IP Group
 - e. Click **Apply** to apply your settings.



A separate configuration is required per SIP Trunk.

Figure 63: IP-to-IP Call Routing Rules

Index		Source IP Group	Request Type	Call Trigger	ReRoute IP Group	Dest Type	Dest IP Group	Dest Address
0	Terminate OPTIONS	Any	OPTIONS			Dest Address		internal
1	Refer from Teams (arbitrary name)	Any		REFER	Teams	Request URI	Teams	
2	Refer from DR-SBA (arbitrary name)	Any		REFER	DR-SBA	Request URI	DR-SBA	
3	Teams to SIP Trunk (arbitrary name)	Teams				IP Group	SIPTrunk	
4	DR-SBA to SIP Trunk (arbitrary name)	DR-SBA				IP Group	SIPTrunk	
5	SIP Trunk to Teams (arbitrary name)	SIPTrunk				IP Group	Teams	
6	SIP Trunk to DR-SBA (arbitrary name)	SIPTrunk				IP Group	DR-SBA	



For Index 5 & 6, set Group Policy to **Forking**

7 Teams Branch Survivability Policy

The Teams Branch Policy contains one or more Teams DR-SBA devices. You need to create the policies via PowerShell command *New-CsTeamsSurvivableBranchAppliancePolicy* in Skype for Business Online PS. The parameters to the cmdlet are as follows:

- **Identity:** Defines the identity of the policy
- **BranchApplianceFqdns:** Defines the FQDN of the DR-SBA(s) in the site

For example:

```
new-CsTeamsSurvivableBranchAppliancePolicy -Identity Sba1Policy -  
BranchApplianceFqdns "sba1.contoso.com","sba2.contoso.com"  
Identity: Tag: Sba1Policy BranchApplianceFqdns :  
{sba1.contoso.com, sba2.contoso.com}
```

You can add or remove DR-SBA's from a policy by using the *Set-CsTeamsSurvivableApplianceBranchPolicy* as shown in the example below:

```
Set-CsTeamsSurvivableBranchAppliancePolicy -Identity Sba1Policy -  
BranchApplianceFqdns @{remove="sba1.contoso.com"}
```

8 Assigning Teams Branch Survivability Policy to Users

You assign the policy to individual users by using the “*Grant-CsTeamsSurvivableBranch*” cmdlet in Skype for Business Online PS. The parameters to the cmdlet are:

- **Identity:** Defines the identity of the user
- **PolicyName:** Defines the identity of the policy

For example:

```
Grant-CsTeamsSurvivableBranchAppliancePolicy -PolicyName  
Sba1Policy -Identity user1@contoso.com
```

You can remove a policy from a user by granting the \$Null policy:

```
Grant-CsTeamsSurvivableBranchAppliancePolicy -PolicyName $Null -  
Identity user1@contoso.com
```



- AudioCodes’ can offer User Management Pack 365 (UMP 365). UMP365 is a software application Web GUI that simplifies Microsoft 365 Users MACD and lifecycle management of Microsoft Teams, SharePoint and OneDrive policies with Microsoft Direct Routing capabilities. **UMP 365 supports Teams Branch Survivability Policy.**
- All DR SBA users should be licensed and must have an assigned phone number.

9 Firewall

The following tables describe the firewall rules that need to be configured on the enterprise firewall.

Table 8: Firewall Rules

Traffic	From	To	Source port	Destination port	Flow Direction
Teams Client ↔ DR-SBA					
TCP	Teams Client	DR-SBA	Any	4444	Bi-directional
TCP	Teams Client	DR-SBA	Any	3443	Bi-directional
TCP	Teams Client	DR-SBA	Any	8443	Bi-directional
DR-SBA ↔ Teams Client (Media) or SBC ↔ Teams Client (Media)					
SRTP	DR-SBA or SBC	Teams Client	UDP: 50000 or higher	UDP: configured on SBC	-
DR-SBA ↔ SBC					
TCP	DR-SBA	SBC	Any	5061 (or as configured on SBC)	-
TCP	SBC	DR-SBA	Any	5061	-
DR-SBA → NTP Server					
UDP	DR-SBA	NTP	UDP: Any (by default DR-SBA uses time.microsoft.com)	UDP: 123	-
DR-SBA (Appliance/Virtual Appliance) → Microsoft 365 (Teams tenant)					
HTTPS	DR-SBA	Azure IP Ranges and Service	Any	443	-
*ICMP	DR-SBA	www.microsoft.com	Any		-
**TCP	DR-SBA	sip.pstnhub.microsoft.com sip2.pstnhub.microsoft.com sip3.pstnhub.microsoft.com	Any	5061	
Admin Browser ↔ Teams DR-SBA Web					
HTTP	Admin Browser	Teams DR-SBA Web	Any	80	
HTTPS	Admin Browser	Teams DR-SBA Web	Any	443	
Management PC Station (e.g., RDP) → DR-SBA					
TCP	Computer	DR-SBA	Any	3389	Bi-directional

* For ICMP, see Known Issues on page 88. From version 1.1.008 no need for this rule on the firewall.

** This is needed from version 1.1.008 and above



Azure IP Ranges and Service Tags for the Public Cloud should be defined according to the guidelines described at [Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center](#).

Pending receipt of specific IP address ranges from Microsoft.



For Firewall rules between the SBC and Teams client, refer to the [Mediant SBC for Microsoft Teams Direct Routing documents](#).



HTTP or HTTPS proxy is not supported.

10 Using DR-SBA Management Interface

Once you have initially set up the DR-SBA through the DR-SBA Management Interface's DR-SBA Setup Wizard, as described in Chapter 5, you can use the DR-SBA Management Interface for full configuration, maintenance, and monitoring of the DR-SBA. In addition, if your DR-SBA device is also employing gateway functionality (i.e., PSTN Gateway and/or SBC), you can use the DR-SBA Management Interface for viewing basic monitoring of the gateway and for accessing the gateway's Web interface (single sign-on) for full gateway configuration.

The figure below shows the main areas of the DR-SBA Management Interface.

Figure 64: Main Areas of DR-SBA Management Interface

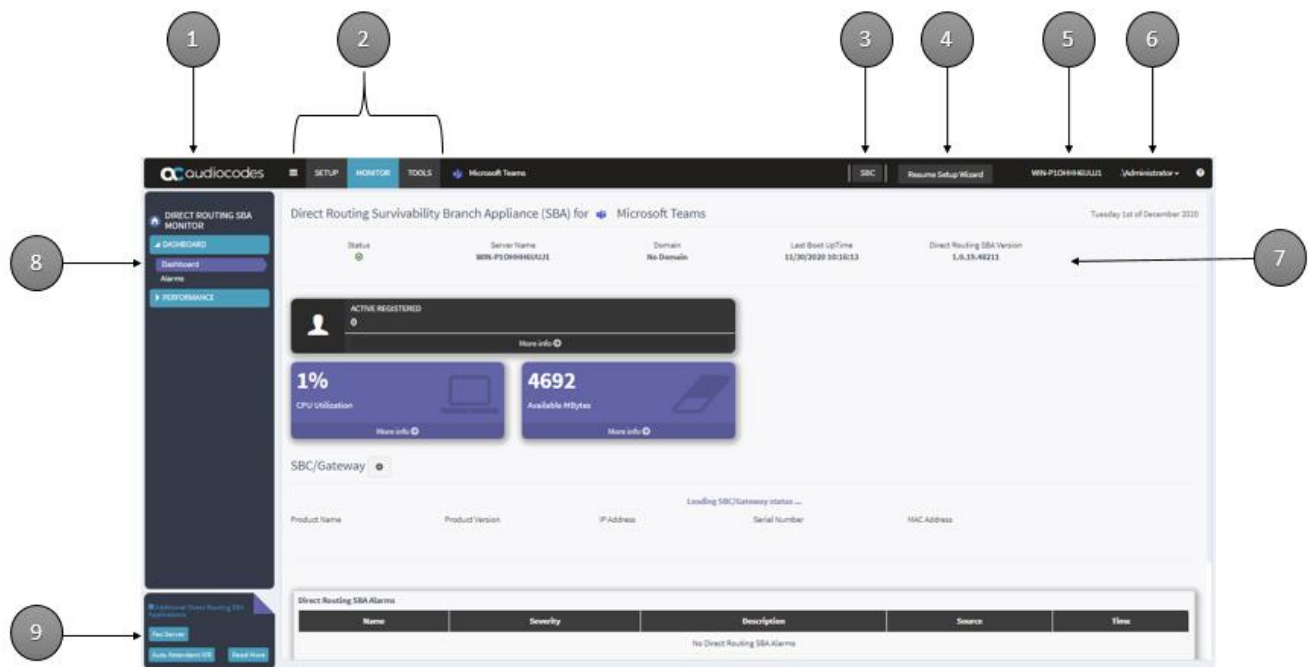


Table 9: Main Areas of DR-SBA Management Interface

Item #	Description
1	When clicked, displays the Dashboard.
2	Menu bar with menus (Setup, Monitor and Tools).
3	Switch to local SBC Web Interface (not applicable on Virtual Edition).
4	Resume Setup Wizard button. If you exit the DR-SBA Setup Wizard before its completion, you can later resume from the same wizard page, by clicking this button.
5	Displays the DR-SBA computer name (defined when joining the domain). If clicked, a pop-up appears displaying system information.
6	Displays the currently logged-in username. When clicked, a drop-down menu appears with the Logout command, which if clicked, logs you out of the DR-SBA Management interface.
7	Displays the details of the DR-SBA for Skype for Business and dashboard statistics.
9	Navigation pane containing folders and page items, which depend on the menu selected from the menu bar.
10	Opens AudioCodes website, displaying a page with additional DR-SBA applications (Fax Server).

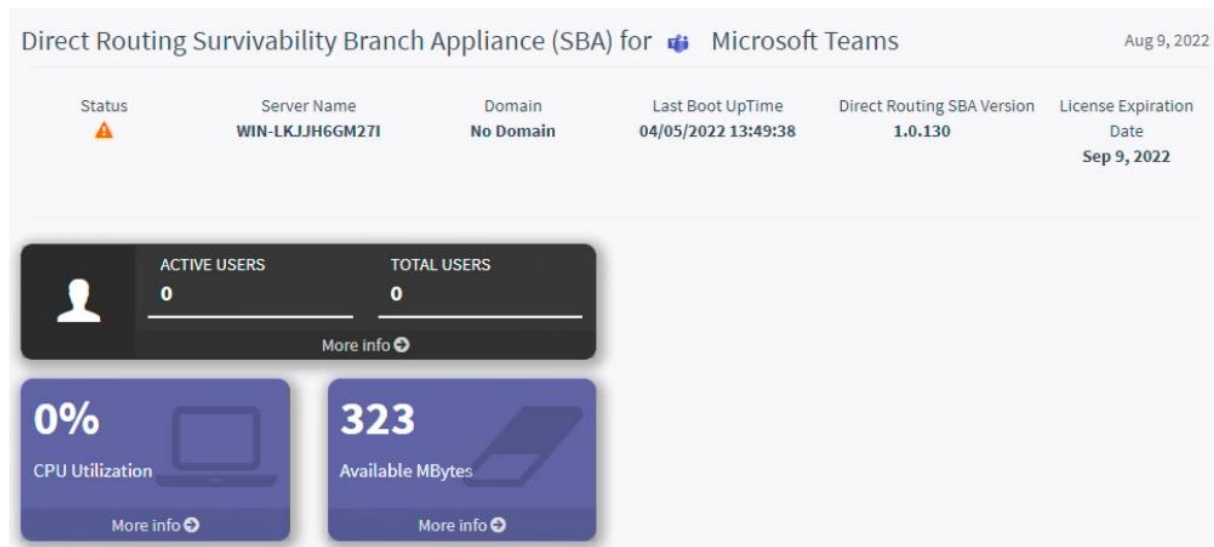
10.1 Viewing General DR-SBA Details on Dashboard

The following procedure describes how to view general DR-SBA details, which are displayed on the dashboard.

To view general DR-SBA details:

1. From the **Monitor** menu, select the **Dashboard** folder, and then click **Dashboard**:

Figure 65: Viewing Dashboard

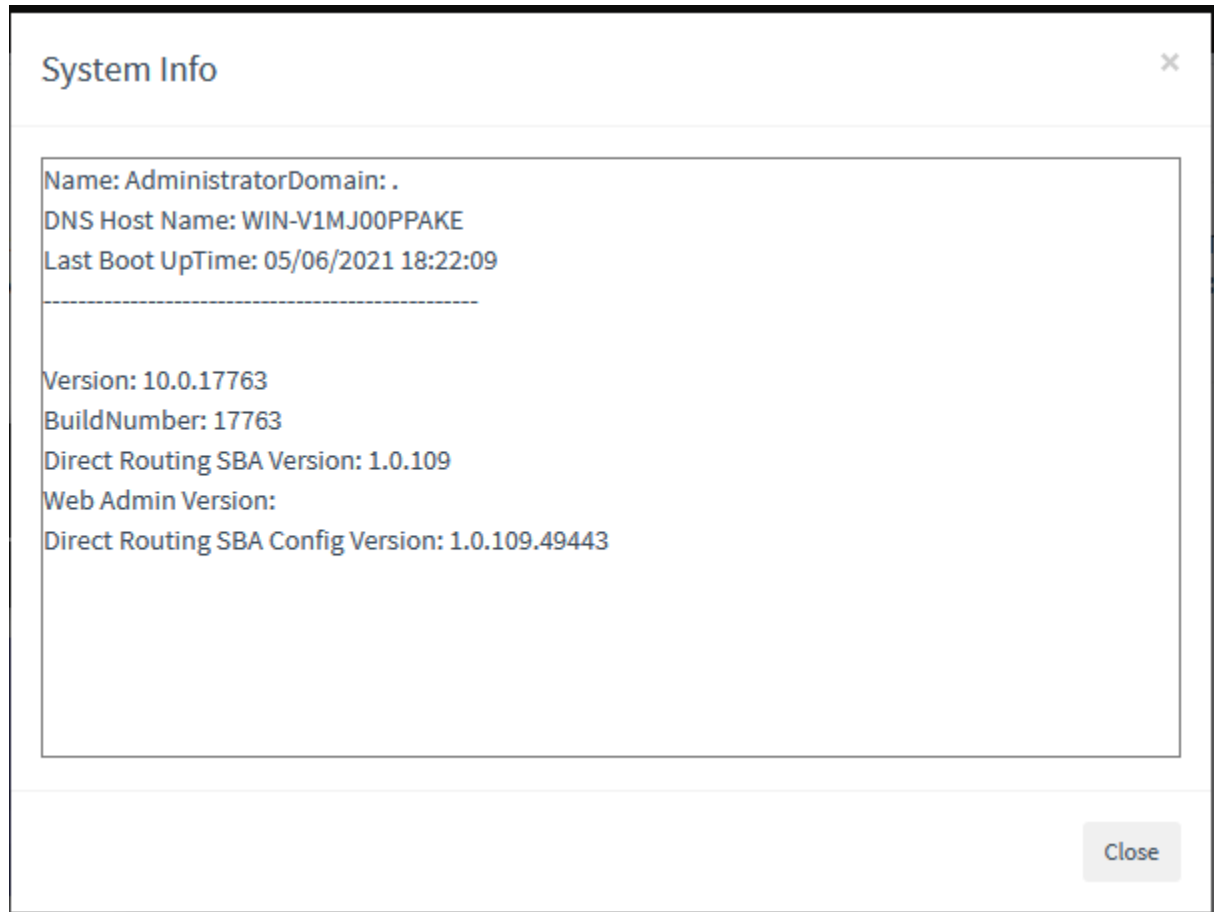


The following information is displayed:

- **Status:**
 - means that the DR-SBA is ready (can replicate data from Teams).
 - means that there is a problem. If you hover your mouse over the icon, a pop-up appears displaying detailed information of the problem.
- **Server Name:** Name of the DR-SBA server.
- **Domain:** Domain name to which the DR-SBA is joined.
- **Last Boot UpTime:** Date and time at which the DR-SBA server was last restarted.
- **Direct Routing SBA Version:** Version of the DR-SBA service. If you hover your mouse over the version, the OS and DR-SBA software components versions are displayed.
- **Active Users / Total Users:** Number of active and total users. This is displayed even when the internet is connected.
- **CPU Utilization:** CPU utilization of DR-SBA server.
- **Available Mbytes:** Free memory of DR-SBA server.

You can also view general DR-SBA details, by clicking the arrow next to the logged-in username, and then choosing **Info**:

Figure 66: System Info Window



The following information is displayed:

- **Name:** Username of the currently logged-in user
- **Domain:** Domain name to which the DR-SBA is joined
- **DNS Host Name:** Name of the DR-SBA
- **Last Boot Up Time:** Date and time at which the DR-SBA server was last restarted
- **On OSN appliances:**
 - **Version:** Version of the Windows Server 2019 operating system
 - **Build Number:** Build version of the Windows Server 2019 operating system
- **On Virtual Appliance:**
 - **Version:** Version of the Windows Server 2019 or 2022 operating system
 - **Build Number:** Build version of the Windows Server 2019 or 2022 operating system
- **SBA Version:** Software version of the DR-SBA
- **Web Admin Version:** Version number of the DR-SBA Management Interface
- **SBA Config Version:** Version of the Teams SBA Config service

10.2 DR-SBA Configuration

This section describes DR-SBA configuration operations that can be performed through the DR-SBA Management Interface (in addition to configuration through the DR-SBA Setup Wizard described in Chapter 5).

10.2.1 Viewing and Configuring Network Interfaces

The device includes the following network interface cards (NIC):

■ **OSN DR-SBA:**

- External Ethernet Ports:
 - If there are two or four external interfaces, NIC teaming is used between the first two.
 - ◆ **External Team:** By default, the NIC is enabled (192.168.0.20)
 - ◆ **GE 3:** By default, the NIC is Disable.
 - ◆ **GE 4:** By default, the NIC is Disable.
 - ◆ **GE 3 and GE 4 are available only for specific HW**
 - **Internal Ethernet Port:** By default, the NIC is enabled and enabled for DHCP

■ **Virtual DR-SBA:**

The virtual machine virtual network interface is listed

To view and configure network interfaces:

1. From the **Setup** menu, select the **Setup** folder, and then click **Network**:

Figure 67: Viewing Network Interfaces (OSN-Based DR-SBA)

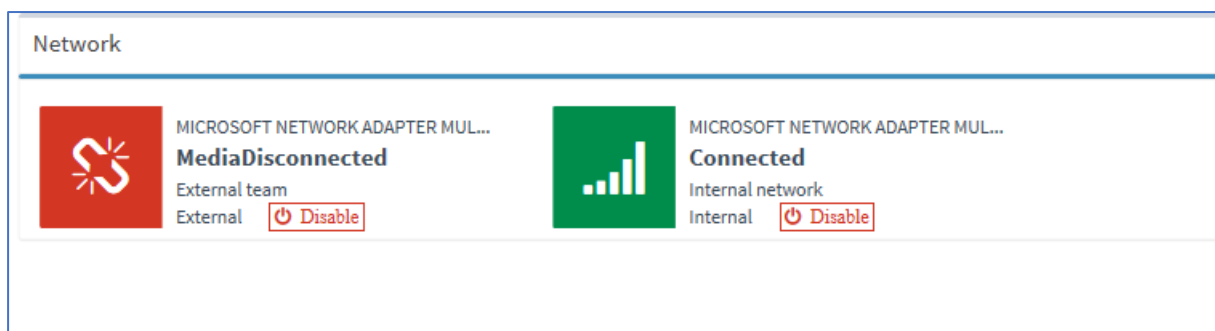
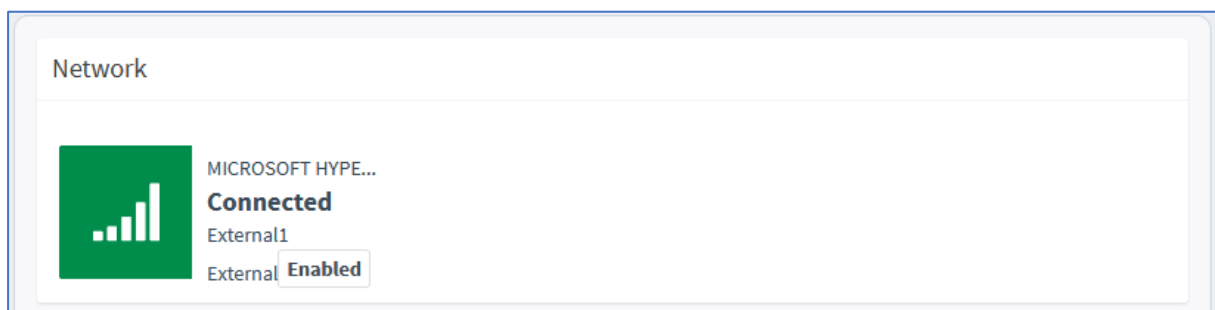


Figure 68: Viewing Network Interfaces (Virtual Appliance-Based DR-SBA)



2. To disable a network interface, click **Disable**; to enable a network interface, click **Enable**.
3. To configure a network interface, click the required network icon; the following appears:

Figure 69: Configuring a Network Interface (e.g., External NIC Team)

The screenshot shows a configuration window titled "Network IP address and DNS address". It contains several input fields and dropdown menus for network settings. At the bottom right, there are "Submit" and "Cancel" buttons.

Network IP address and DNS address

Network Interface Card

DHCP Or IP

Obtain an IP address automatically

IP Address

Enter IP address

IP Mask

Enter subnet mask address

Default Gateway

Enter default gateway address

DNS Address

Obtain DNS server address automatically

Preferred DNS server

Enter preferred IP address

Alternate DNS server

Enter alternate IP address

Submit Cancel

Network configuration is explained in detail in the DR-SBA Wizard section (see Section 5.55.5).



When the DR-SBA IP has changed, navigate to **Configuring Teams Online > Teams SBA FQDN** tab and set the new IP to be used by the DR-SBA services. After this change, restart the Microsoft SBA Service.

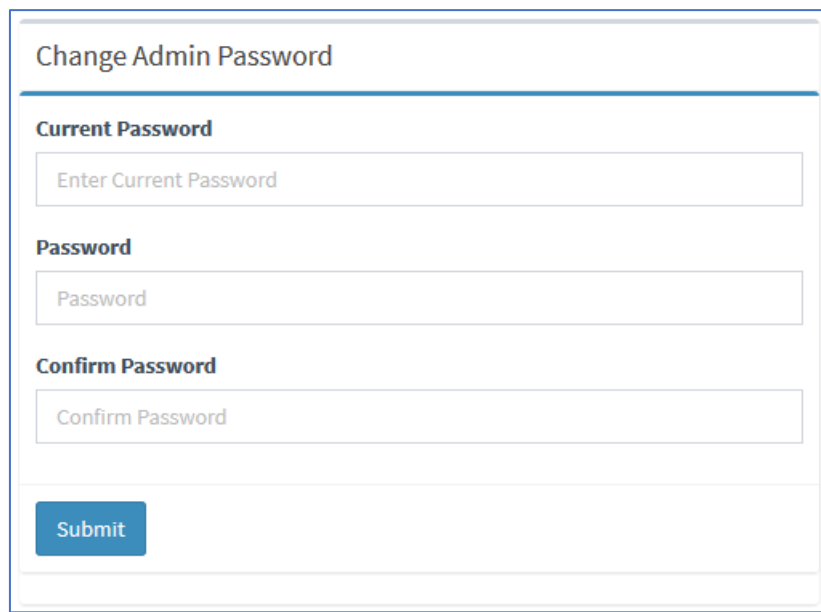
10.2.2 Changing Login Password

The following procedure describes how to change the login password of the administrator who is currently logged into the DR-SBA Management Interface.

To change the login password:

1. From the **Setup** menu, select the **Setup** folder, and then click **Change Admin Password**; the following appears:

Figure 70: Changing Login Password



The screenshot shows a web form titled "Change Admin Password". It contains three text input fields stacked vertically. The first field is labeled "Current Password" and has the placeholder text "Enter Current Password". The second field is labeled "Password" and has the placeholder text "Password". The third field is labeled "Confirm Password" and has the placeholder text "Confirm Password". Below these fields is a blue button labeled "Submit".

2. In the 'Current Password' field, enter the current password.
3. In the 'New Password' field, enter the new password.
4. In the 'Confirm Password' field, enter the new password again.
5. Click **Submit**.

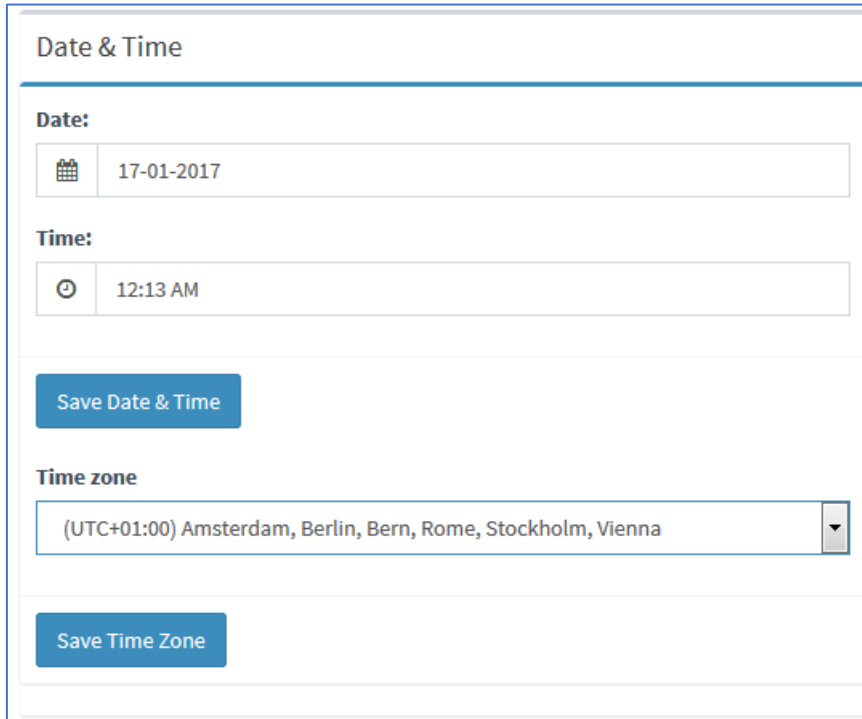
10.2.3 Configuring Date and Time

The following procedure describes how to configure the DR-SBA server's date and time.

To configure the date and time:

1. From the **Setup** menu, select the **Setup** folder, and then click **Date & Time**; the following appears:

Figure 71: Configuring Date and Time



2. Click the 'Date' field, and then select the date using the pop-up calendar.
3. Click the 'Time' field, and then select the time using the pop-up time box.
4. Click **Save Date & Time**.
5. From the 'Time Zone' drop-down list, select the UTC time zone in which the DR-SBA is located, and then click **Save Time Zone**; the date in the 'Date' field is automatically adjusted according to the selected time zone.

10.2.4 Configuring SNMP

The following procedure describes how to configure SNMP-based communication between DR-SBA and AudioCodes One Voice Operations Center (OVOC).

To configure SNMP:

1. From the Setup menu, select the Setup folder, and then click **SNMP**.

Figure 72: Configuring SNMP

The screenshot shows the 'OVOC Setting' configuration page. It contains four main panels:

- OVOC Connection:** Fields for IP Address (10.21.8.37), Trap Port (162), and Keep Alive Port (1161).
- OVOC Public Cloud:** A checkbox labeled 'Use public OVOC'.
- System Info Settings:** Fields for System Name (SBA3434) and Location (string).
- Access Settings:** A field for Login URL (http://169.254.22.94/tenantui).
- SNMP:** Radio buttons for SNMP v2 (selected) and SNMP v3. Below them are fields for Community Read (public) and Community Write (private).

A 'Save' button is located at the bottom right of the page.

2. In the 'IP Address' field, type the OVOC address (FQDN or IP address).



For 'Public OVOC', the 'IP Address' field is grayed out.

3. In the 'Trap Port' field, type the SNMP port number (default=162) for sending traps.
4. In the 'Keep Alive Port' field, type the SNMP port number (default=1161) for sending keep-alive messages.
5. Under **System Info Settings**, in the 'System Name' and 'Location' fields, type the system name and physical location, respectively.
6. In the 'Login URL' field, type the URL of the DR-SBA Web interface. OVOC uses this URL to access the DR-SBA Web.
7. Under **SNMP**, do the following:
 - a. Select the **SNMP v2** or **SNMP v3** option.
 - b. Enter the SNMP authentication fields according to the protocol you selected.
8. Click **Save**.

10.2.4.1 OVOC in Public Cloud

When OVOC is deployed in the cloud, DR-SBA can connect to OVOC through a WebSocket tunnel using port 443 (instead of opening incoming SNMP transport on the firewall from OVOC to DR-SBA).

This Public OVOC mode allows the OVOC administrator to access DR-SBA's Web Admin or access DR-SBA by remote desktop, using this WebSocket tunnel. For more information on WebSocket tunneling with OVOC, refer to the [OVOC User's Manual](#).

To enable Public OVOC mode:

1. From the Setup menu, select the Setup folder, and then click **SNMP**.
2. Select the 'Use public OVOC' check box:

Figure 73: Enabling Public OVOC Mode

3. In the 'OVOC Public IP' field, type the public address (FQDN or IP address) of OVOC.
4. In the 'OVOC Public User' field, type the username.
5. In the 'OVOC Public Password' field, type the password.
6. Click **Save**.

10.2.5 Configuring Certificates

The following dialog is used to configure the DR-SBA certificate.

To configure certificates:

1. From the **Setup** menu, select the **Setup** folder, and then click **Direct Routing SBA Certificate**.

Figure 74: Configuring Certificates

Certificate	Friendly Name	Expiration Date	Assigned
*.audctrunk.aceducation.info		05/04/2022 17:24:51	✓

Certificate configuration is explained in detail in the DR-SBA Wizard section in Chapter 5.

2. After the certificate has been changed, restart Microsoft SBA Service to load the new certificate.

10.2.6 Access List

The following procedure describes how to configure which IP addresses are allowed to access the DR-SBA Web and RDP. This setup limits access to the DR-SBA part only and not to the SBC/Gateway part (for the SBC/Gateway access list, use the SBC/Gateway Web interface).



Pay attention to which IP address/subnet you specify. You can accidentally block access to the DR-SBA. If this occurs, use the screen and keyboard to connect to the DR-SBA locally and open the Web interface locally to fix the access list.

To configure the Access List:

1. From the **Setup** menu, select the **Setup** folder, and then click **Access List**.

Figure 75: Access List

Access List

Select the Web and RDP access list:

Any – Web and RDP can be access from any IP.

Authorized IP/Subnet – Web and RDP can be access from the list of IP/Subnet that you define.

Adding IP/Subnet can be done in one of the following formats:

Single IP4 address (e.g. "192.168.0.17")

Single IP4 subnet by subnet mask (e.g. "192.168.0.17/255.255.255.0")

Single IP4 subnet by network bits (e.g. "192.168.0.17/24")

☒ **Any**

☐ **Authorized IP/Subnet**

Save

2. By default, any IP address can access the Web and RDP (**Any** option).
3. To allow DR-SBA management from a specific IP/Subnet, select the **Authorized IP/Subnet** option; the following appears:

Figure 76: Access List: Authorized IP/Subnet

Access List

Select the Web and RDP access list:

Any – Web and RDP can be access from any IP.

Authorized IP/Subnet – Web and RDP can be access from the list of IP/Subnet that you define.

Adding IP/Subnet can be done in one of the following formats:

Single IP4 address (e.g. "192.168.0.17")

Single IP4 subnet by subnet mask (e.g. "192.168.0.17/255.255.255.0")

Single IP4 subnet by network bits (e.g. "192.168.0.17/24")

☐ Any

☒ **Authorized IP/Subnet**

Add

Save

4. You can add an IP address/subnet in one of the following formats:
 - Single IPv4 address (e.g., "192.168.0.17")
 - Single IPv4 subnet by subnet mask (e.g., "192.168.0.17/255.255.255.0")
 - Single IPv4 subnet by network bits (e.g., "192.168.0.17/24")
5. Click **Add**.
6. Click **Save** to save your changes.

10.2.7 Configuring Teams Online

The following dialog is used to configure the DR-SBA FQDN, SIP listen IP and Azure Application ID/Secret.

To configure Tenant ID, SBA FQDN or SBA Application ID/Secret:

1. Select the Setup folder, and then click **Teams Online**.

Figure 77: Configuring Teams Online

Last login tenant information	
Account	ron@cce.sceducation.info
Environment	AzureCloud
Tenant Domain	audiocodesipprnd.onmicrosoft.com

2. For detailed information on Teams Online configuration,, see the DR-SBA Wizard section (see Section 5.9, Log in to Teams).

10.2.8 Configuring Voice Application

The **Voice Application** menu allows you to configure the DR-SBA Voice Application. This allows you to configure where to redirect Teams Call queue or Auto attendant calls upon survivable mode:

- Redirect an incoming PSTN call to a Call queue or Auto attendant number, to a local agent.
- Redirect an incoming PSTN call to a Call queue or Auto attendant number, to an alternative Call queue or Auto attendant number.

The Tenant admin can configure on-prem agent (Teams users in the format username@company.domain) or user's number, or external PSTN numbers for each Call queue or Auto attendant number.

Incoming calls to a Call queue or Auto attendant number via the PSTN or VoIP (from outside or within the SBA site) are redirected to a predefined phone number or Teams user, based on the settings defined by the Tenant Admin. If this Teams user doesn't answer, the call is forwarded to a fallback number or a user.

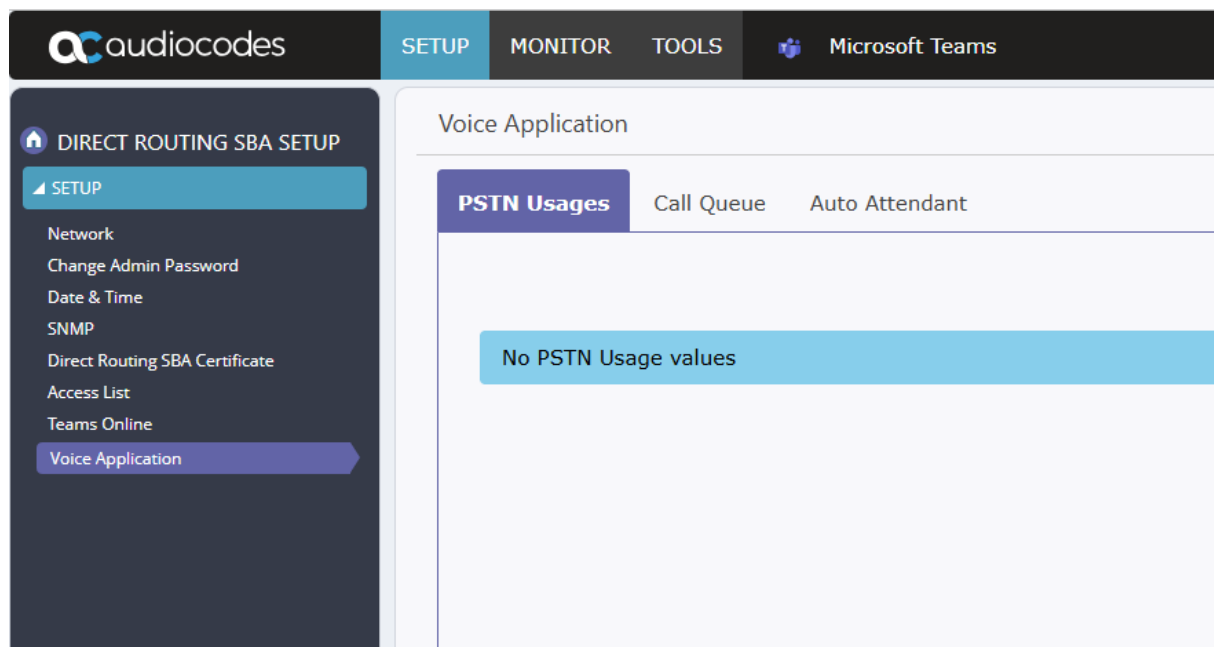


Simultaneous ringing is not supported. DR-SBA supports 1:1 mapping only – one agent per Call queue or Auto attendant number.

To configure voice application:

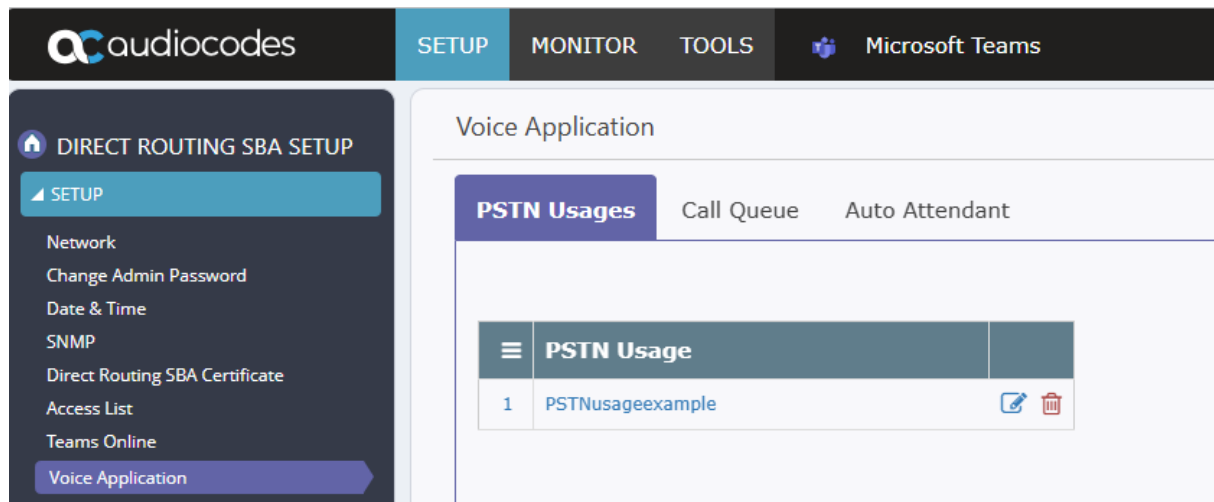
1. From the **Setup** menu, expand the **Setup** folder, and then click **Voice Application**:

Figure 78: Configuring Voice Application



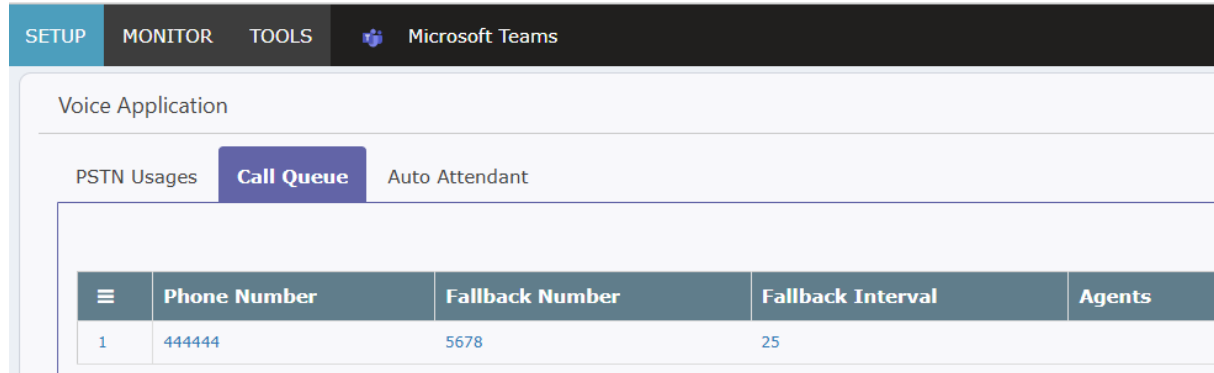
2. The **PSTN Usages** tab is for PSTN-to-PSTN calls, where a redirect of an incoming PSTN call to a Call queue or Auto attendant number is redirected back to the PSTN:
 - a. Click **Add New**.
 - b. Click **Save**.

Figure 79: Configuring PSTN Usages



3. To configure Call queue:
 - a. Select the **Call Queue** tab.
 - b. Click **Add New**.
 - c. Click **Save**.

Figure 80: Configuring Call Queue



4. To configure Auto attendant:
 - a. Select the **Auto Attendant** tab.
 - b. Click **Add New**:

Figure 81: Configuring Auto Attendant

- b. Add an agent or simply add a fallback number. The fallback number can also be a Teams user phone number connected to DR-SBA.
 - ◆ **Agent:** This can be a phone number associated with a user or an external PSTN number, or a username of a local Teams user.
 - ◆ **FallbackCloudNumber:** (Optional) This can be a Calling Plan, Operator Connect number, or an external PSTN number. If the configured agent is unavailable (busy, rejects the call, or doesn't answer within the **FallbackInterval** duration – see below), the call is forwarded to this number.
 - ◆ **FallbackInterval:** (Optional) Defines the duration (in seconds) before the call is forwarded to the **FallbackCloudNumber** (see above). The value must be between 16 and 30 seconds. If you don't configure this parameter or configure it to a value outside of the range, it defaults to 25 seconds. For optimal performance, it's recommended to configure the parameter between 17 to 25 seconds.



For the Voice Application, DR-SBA requires that you configure at least an **agent** or a **FallbackCloudNumber**, or both. If you configure only a **FallbackCloudNumber**, forwarding is done immediately, regardless of the **FallbackInterval** value.

- c. Click **Apply**, and then click **Save**.



When simulating survivability mode, you must also simulate no internet for the SBA server and not only for the Teams client, to allow the voice application to function.

10.3 SBC/Gateway-Related Operations

If you are also using your device for SBC/Gateway functionality (i.e., PSTN Gateway and/ or SBC), you can use the DR-SBA Management Interface for various Gateway-related operations, as described in this section.



To enable communication between the DR-SBA Management Interface and the Gateway's Web interface, ensure Internal VLAN is enabled (OSNInternalVLAN=1).

10.3.1 Viewing SBC/Gateway Information

The following subsections describe how to view various information relating to the SBC/Gateway.



10.3.1.1 Viewing SBC/Gateway Details

The following procedure describes how to view details about the SBC/Gateway.

To view gateway details:

1. From the **Monitor** menu, select the **Dashboard** folder, and then click **Dashboard**.
2. Scroll down the page to the SBC/Gateway section:

Figure 82: Viewing SBC/Gateway Details

SBC/Gateway   10.21.66.67				
Product Name	Product Version	IP Address	Serial Number	MAC Address
Mediant 800B	7.10A.036.018	10.21.41.89	8952484	00908f889aa4


The following information is displayed:

- **Product Name:** Name of the SBC/Gateway model
- **Product Version:** Software version currently running on the SBC/Gateway
- **IP Address:** IP address of the SBC/Gateway's OAMP interface
- **Serial Number:** Serial number of the SBC/Gateway's CPU
- **MAC Address:** MAC address of the SBC/Gateway

10.3.2 Accessing the SBC/Gateway's Web Interface

If required, you can access the SBC/Gateway's Web interface from the DR-SBA Management Interface. The Web interface allows you to fully configure SBC/Gateway functionality.

To access SBC/Gateway's Web interface:

1. From the **Monitor** menu, select the **Dashboard** folder, and then click **Dashboard**.
2. You can modify the SBC/Gateway IP address manually and only once, during initial setup.
3. Scroll down the page to the SBC/Gateway section, and then click ; the Web interface opens.
4. Type the SBC/Gateway IP address, and then click **Save**:

SBC/Gateway Web Admin IP ×

Save Close

For more information on using the SBC/Gateway's Web interface, refer to the SBC/Gateway's *User's Manual*.

10.4 Performance Monitoring

The DR-SBA Management Interface allows you to monitor the DR-SBA.

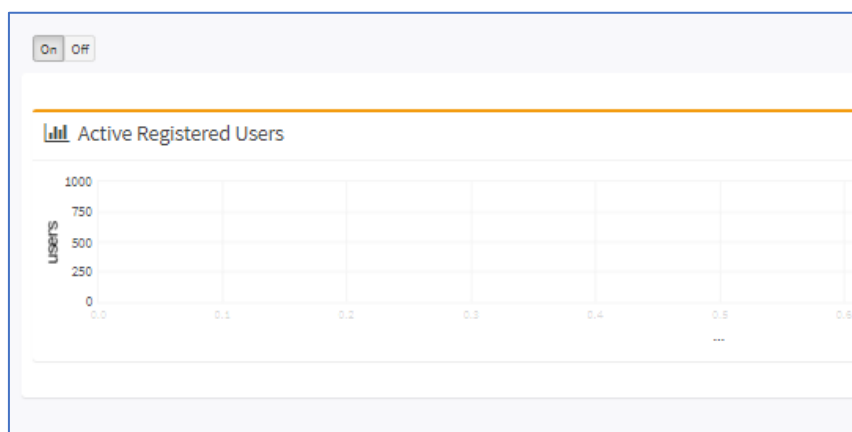
10.4.1 Viewing Registered Users Statistics

The following procedure describes how to view active registered user statistics, which includes users and endpoints.

To view registered user statistics:

1. From the **Dashboard** menu, select the **More Info** link on **Active Registered** counter.
2. Click **On** to enable statistics or **Off** to disable.

Figure 83: Viewing Active Registered Users



10.4.2 Viewing General DR-SBA Server Statistics

The following procedure describes how to view general statistics of the DR-SBA server.

To view DR-SBA server statistics:

1. From the **Monitor** menu, select the **Performance** folder, and then click **Key Health Indicators**.
2. Click **On** to enable statistics or **Off** to disable.

Figure 84: Viewing DR-SBA Server Statistics

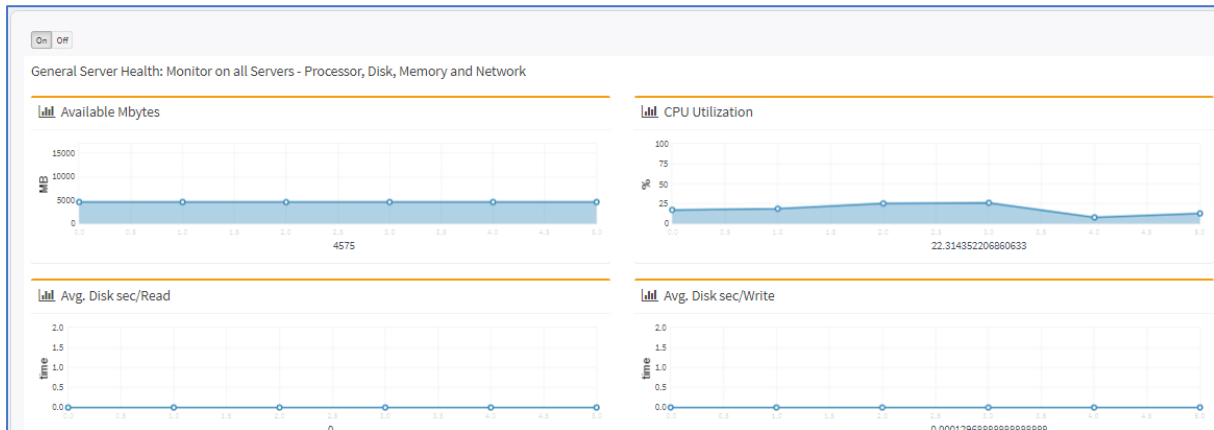


Table 10: DR-SBA Server Statistics

Graph	Description
General Server Health	
Available Bytes	Available physical memory (in MBytes) for running processes
CPU Utilization	Current utilization of CPU (in %)
Avg. Disk Sec/Read	Average time of disk-read latency
Avg. Disk Sec/Write	Average time of disk-write latency

10.5 Maintenance

This section describes various maintenance operations.

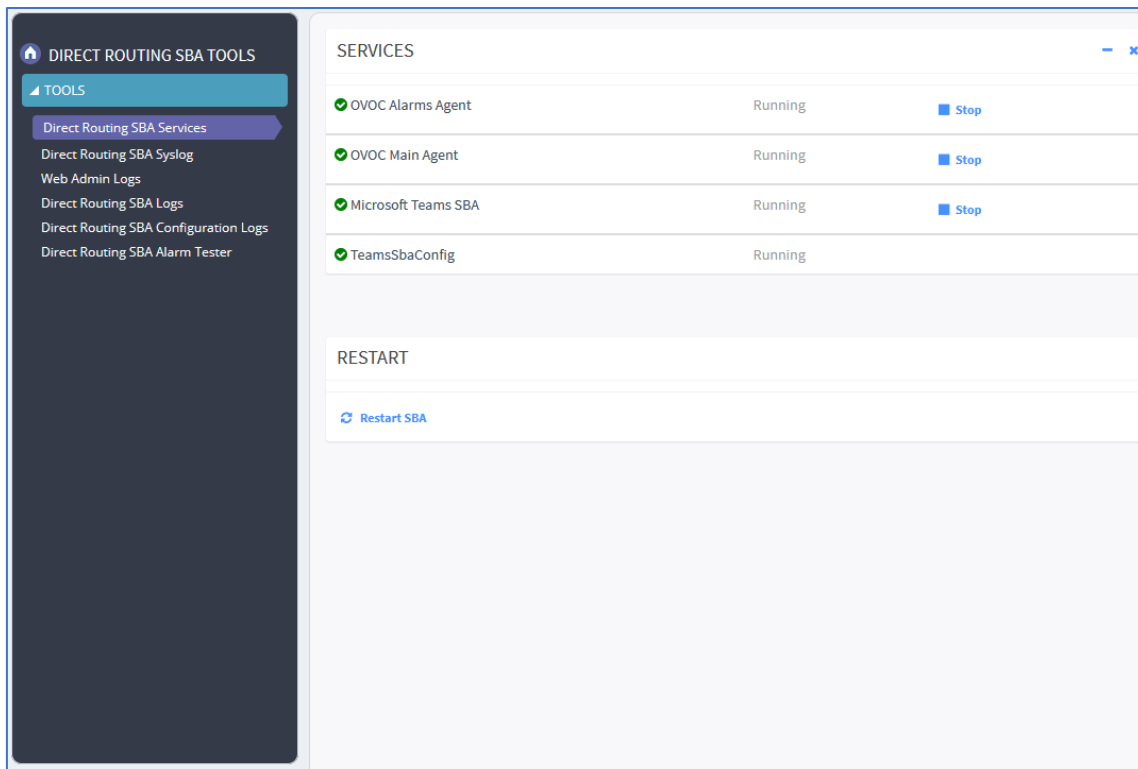
10.5.1 Stopping and Starting DR-SBA Services

The following procedure describes how to stop and start DR-SBA services.

To stop and start DR-SBA services:

1. From the **Tools** menu, click **Direct Routing SBA Services**; the following screen appears:

Figure 85: Stopping and Starting DR-SBA Services



2. Do one of the following:
 - To stop a service, click the corresponding **Stop** button; the service displays the "Stopped" status message.
 - To start a service, click the corresponding **Start** button; the service displays the "Running" status message.

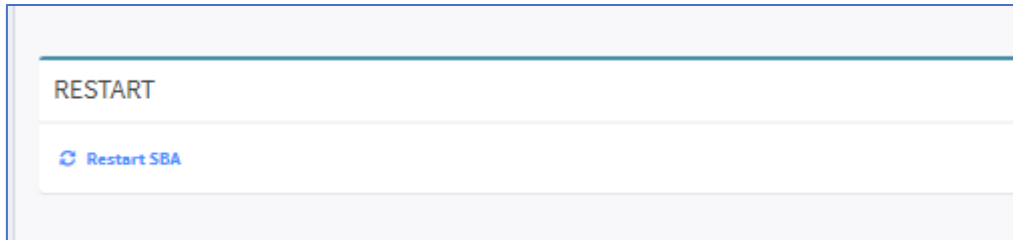
10.5.2 Restarting DR-SBA Server

The following procedure describes how to restart the DR-SBA.

To restart the DR-SBA:

1. From the **Tools** menu, click **SBA Services**; the following screen appears:

Figure 86: Restarting DR-SBA



2. Click **Restart SBA**.

10.5.3 Configuring Syslog

The following procedure describes how to enable the DR-SBA to send DR-SBA configuration logs (see [SBA Configuration Logs](#) on page 79) to a Syslog server (for diagnostics).

To configure Syslog:

1. From the **Tools** menu, click **Direct Routing SBA Syslog**; the following screen appears:

Figure 87: Configuring Syslog

The screenshot shows the 'Syslog Settings' configuration page. On the left is a dark sidebar with the title 'DIRECT ROUTING SBA TOOLS' and a 'TOOLS' menu. Under 'TOOLS', several options are listed: 'Direct Routing SBA Services', 'Direct Routing SBA Syslog' (which is highlighted with a blue arrow), 'Web Admin Logs', 'Direct Routing SBA Logs', 'Direct Routing SBA Configuration Logs', and 'Direct Routing SBA Alarm Tester'. The main content area is titled 'Syslog Settings' and contains an 'Enable' checkbox (currently unchecked), a 'Server' text field with the value '127.0.0.1', a 'Port' text field with the value '514', and a blue 'Submit' button at the bottom.

2. Select the **Enable** check box.
3. In the 'Server' field, enter the Syslog server's IP address.
4. In the 'Port' field, enter the Syslog server's port.
5. Click **Submit**.

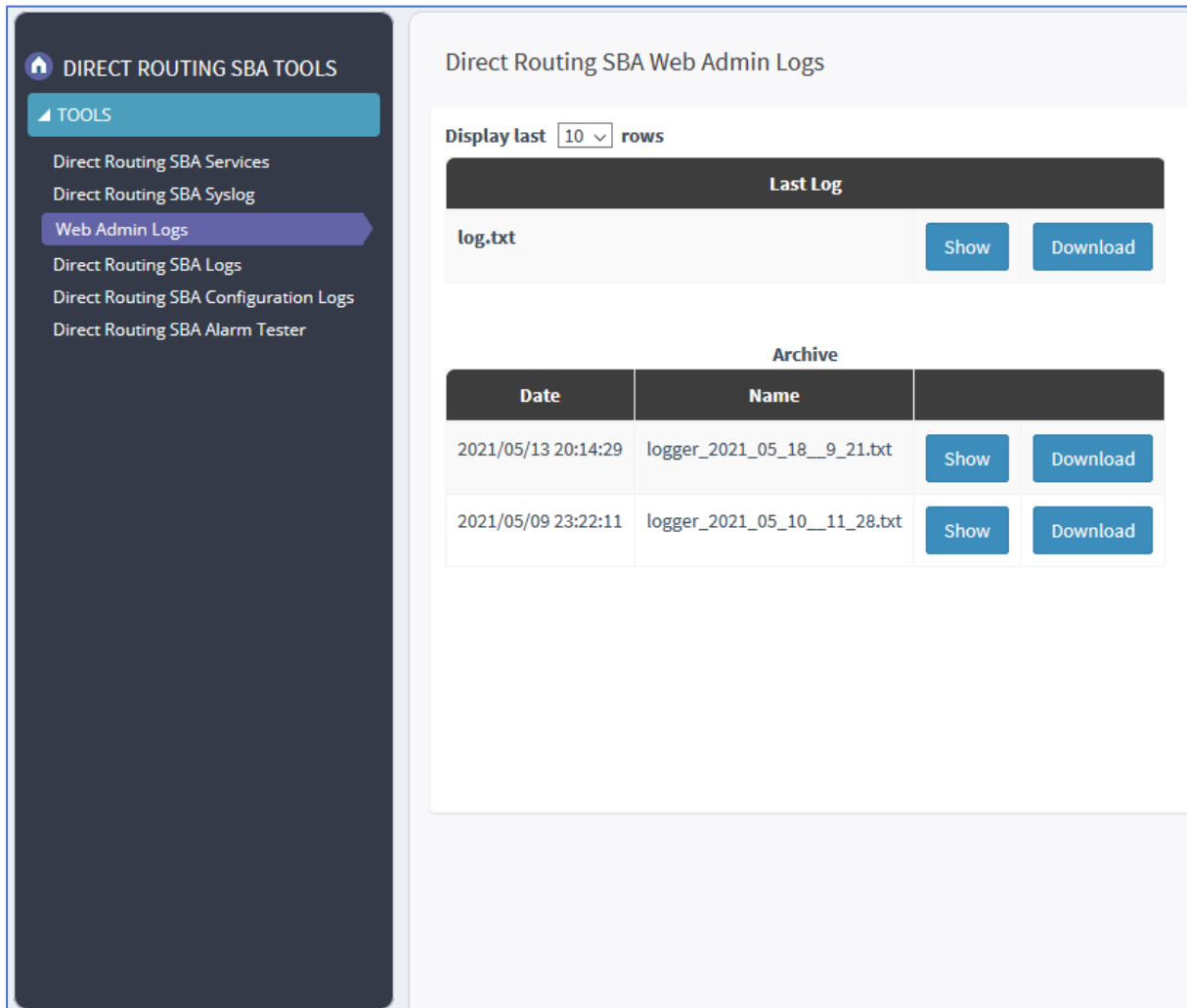
10.5.4 Viewing Logged DR-SBA Management Interface Activities

The following procedure describes how to view logged activities performed in the DR-SBA Management interface such as logging in and out of the GUI.

To view logged activities:

1. From the **Tools** menu, click **Web Admin Logs**; the following screen appears:

Figure 88: Viewing Logged DR-SBA Management Activities



Direct Routing SBA Web Admin Logs

Display last rows

Last Log	
log.txt	Show Download

Archive	
Date	Name
2021/05/13 20:14:29	logger_2021_05_18__9_21.txt
2021/05/09 23:22:11	logger_2021_05_10__11_28.txt

2. From the 'Display last' drop-down list, select the number of row records to display.
3. Click **Show** to view the contents of the logged file or **Download** to save the logged file to your PC.

10.5.5 Viewing Logged Teams DR-SBA Activities

The following procedure describes how to view Microsoft service logs for logged DR-SBA operations.

To view Microsoft Service Logs:

1. From the **Tools** menu, click **Direct Routing SBA Logs**; the following screen appears:

Figure 89: Viewing Microsoft DR-SBA Operations

The screenshot shows the 'Direct Routing SBA Tools' sidebar on the left with the 'Direct Routing SBA Logs' option selected. The main content area is titled 'Direct Routing SBA Logs' and includes a 'Display last 10 rows' dropdown. Below this, there is a 'Last Log' section showing 'SBA.log' with 'Show' and 'Download' buttons. An 'Archive' table lists several log files with their dates and names, each with 'Show' and 'Download' buttons.

Archive			
Date	Name	Show	Download
2021/05/18 11:59:12	SBA_2021_05_18_11_59_12.log	Show	Download
2021/05/18 10:59:58	SBA_2021_05_18_10_59_58.log	Show	Download
2021/05/18 09:59:55	SBA_2021_05_18_09_59_55.log	Show	Download
2021/05/18 08:59:51	SBA_2021_05_18_08_59_51.log	Show	Download
2021/05/18 07:59:46	SBA_2021_05_18_07_59_46.log	Show	Download

10.5.6 Viewing Logged Teams DR-SBA Configuration Activities

This option displays logged AudioCodes DR-SBA configuration operations.

To view logged DR-SBA configuration:

1. From the **Tools** menu, click **Direct Routing SBA Configuration Logs**; the following screen appears:

Figure 90: Viewing Logged SBA Configuration Operations

Direct Routing SBA Configuration Logs

Display last rows

Last Log	
teams-sba-config-log.txt	Show Download

Archive	
Date	Name
2021/05/17 22:59:08	202105172359-teams-sba-config-log.txt
2021/05/16 22:59:01	202105162359-teams-sba-config-log.txt
2021/05/15 22:58:53	202105152358-teams-sba-config-log.txt
2021/05/14 22:58:41	202105142358-teams-sba-config-log.txt
2021/05/13 22:58:35	202105132358-teams-sba-config-log.txt

2. From the 'Display last' drop-down list, select the number of rows to display.
3. Click **Show** to view the contents of the logged file or click **Download** to save the logged file to your PC.

10.5.7 Generating DR-SBA Test Alarms

This option generates tests alarms and sends them to OVOC.

To generate test alarms:

1. From the **Tools** menu, click **Direct Routing SBA Alarm Tester**; the following screen appears:

Figure 91: Direct Routing DR-SBA Alarm Tester

The screenshot shows the Audiocodes management interface. The top navigation bar includes the Audiocodes logo, a menu icon, and tabs for SETUP, MONITOR, and TOOLS (which is active). A Microsoft Teams icon is also present. On the left, a sidebar titled 'DIRECT ROUTING SBA TOOLS' contains a 'TOOLS' section with several options, including 'Direct Routing SBA Alarm Tester' which is highlighted. The main content area is titled 'Send Test Alarm To The OVOC' and contains four form fields: 'Name' (a dropdown menu with 'Direct Routing SBA Services Status Alarm' selected), 'Severity Name' (a dropdown menu with 'Warning' selected), 'Source' (a text input field), and 'Description' (a text input field). At the bottom of the form is a blue button with a bell icon and the text 'Test'.

2. From the Name drop-down list, select the desired alarm to generate.
3. From the Severity Name drop-down list, select the desired severity.
4. In the Source field, enter the alarm source (free text field). For example, for the DR-SBA Services Status alarm, enter "RtcSrv/ RTCMEDSRV/ REPLIC/ RTCCLSAGT". For details regarding the Alarm Source formats, refer to the "SBA Alarms" section in the [OVOC Alarms Guide](#).
5. In the description field, enter the alarm description of the alarm (best to use the "Alarm Text" field; refer to the "SBA Alarms" section in the OVOC Alarms Guide).
6. Click the **Test** button; the alarm is generated and sent to OVOC.

10.5.8 Restoring DR-SBA to Factory Defaults Remotely



This option does not appear for the Virtual Appliance. If the DR-SBA hosts a virtual machine, restoring the DR-SBA to factory defaults deletes the virtual machine. Therefore, if you need the virtual machine, before restoring the DR-SBA to factory defaults, make a backup of the virtual machine through Hyper-V and keep the backup on an external storage device (as the C drive will be formatted).

You can restore the DR-SBA to factory defaults, by using the DR-SBA Management Interface to remotely soft-burn the image of the DR-SBA. This is instead of using the USB. This uses the image from the D:\ partition. By default, the same DR-SBA image is used; the image that was used to burn the DR-SBA on the previous burn. If you want to burn a different DR-SBA image, then replace the existing .wim file, located on the D:\ partition.

When updating an existing DR-SBA with the new DR-SBA Management Interface, the upgrade file does not include the remote burn package. Therefore, you need to download the burn package separately and install it on the DR-SBA through RDP. If the remote burn package is not installed on the DR-SBA, the DR-SBA Management Interface displays a message with the download link.



- Remote soft-burn of the DR-SBA image restores only the DR-SBA OSN to factory defaults (not the SBC-Gateway).
- If the DR-SBA hosts a virtual machine, restoring the DR-SBA to factory defaults deletes the virtual machine. Therefore, if you need the virtual machine, before restoring the DR-SBA to factory defaults, make a backup of the virtual machine through Hyper-V and keep the backup on an external storage device (as the C drive will be formatted).

Figure 92: Restoring DR-SBA to Factory Defaults

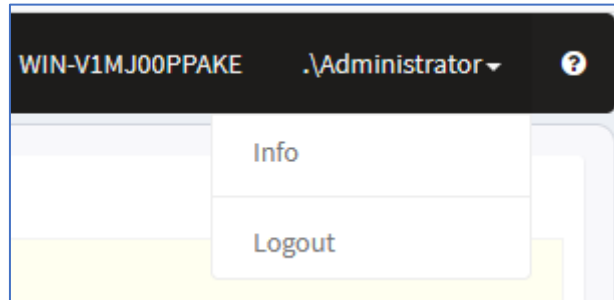
The screenshot shows the Audiocodes DR-SBA Management Interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TOOLS'. The left sidebar lists 'SBA TOOLS' with options like 'SBA Software Upgrade', 'SBA Services', 'SBA Syslog', 'Web Admin Logs', 'SBA Configuration Logs', 'SBA Restore Defaults' (highlighted), and 'SBA Alarm Tester'. The main content area is titled 'SBA Restore To Factory Defaults'. It contains a red warning box stating: 'This option burn the SBA machine with the image that located at D:\. You may select a static IP address which be set to the new image or DHCP option. Once you submit the option, the current SBA machine will no longer functioning. The burn process can take about an hour and the machine is inaccessible during that period. Once the image burn is completed, the new SBA machine is restarted with the selected network settings. You shell run the setup to configure the new image.' Below this, there is a section 'Select SBA IP address to restore' with two radio buttons: 'Static' (selected) and 'DHCP'. The 'Static' option has a text input field showing '10.21.29.120'. At the bottom, there is a red 'Restore' button with a lightning bolt icon.

10.6 Logging Out

The following procedure describes how to log out the DR-SBA Management Interface.

To log out DR-SBA Management Interface:

1. Click the arrow adjacent to the logged-in username:



2. Choose **Logout**.

11 Configuring Token Expiration Grace Period

You can configure the token expiration grace, which provides up to 7 days grace period after the 24-hour Teams client-token expires. During this period, you can operate in survivability mode.



- This feature is available from Version 1.1.017.
- Currently, configuration is done through the DR-SBA configuration file (not through the DR-SBA Web interface).

To configure token expiration grace:

1. Make a backup of the **sbasettings.json** file (C:\Program Files\Microsoft\Microsoft SBA\sbasettings.json).
2. Open the **sbasettings.json** file.
3. Add the **voiceApps** section after the **logger** section (keep existing section intact).
4. Configure Call queue or Auto attendant numbers with their respective fallback numbers or users.
5. Restart the **Microsoft Teams SBA** service.

Below is a configuration example in the **sbasettings.json** file. The parameters related to token expiration grace are displayed in bold:

```
{
  "SbaBasic": {
    "ServerCertificateCommonName": sbalab-xxx.com ",
    "ClientCertificateThumbprints": ["xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"],
    "LocalSipIPAddress": "0.0.0.0"
  },
  "Sba": {
    "Identity": " sbalab-xxx.com ",
    "TenantId": "xxxxxxxx-xxxx-yyyy-yyyy-xxxxxxxxxxxx",
    "Logger": {
      "Directory": "",
      "Level": "Trace",
      "MaxArchiveDays": 30
    },
    "VoiceApps": {
      {
      },
    },
    "ConnectivityCheckIntervalSeconds": 10,
    "ExpiredTokenAcceptancePeriodHours": 72,
    "AcceptExpiredTokenAfterMinutes": 20,
    "DeclareOutageAfterSeconds": 30
  },
  "SbaSecured": {
  }
}
```



- The **ExpiredTokenAcceptancePeriodHours** parameter is optional. It's valid value is an integer in hours, ranging from 0 to 168. If you don't configure the parameter, the default value of 72 hours is used. Configuring a value of 0 or less disables the acceptance of expired tokens, and any request with an expired token will be rejected.
- The remaining parameters -- **ConnectivityCheckIntervalSeconds**, **AcceptExpiredTokenAfterMinutes** and **DeclareOutageAfterSeconds** – are related to the expired token acceptance functionality. However, it's strongly recommended to use their default values (i.e., not configure them).

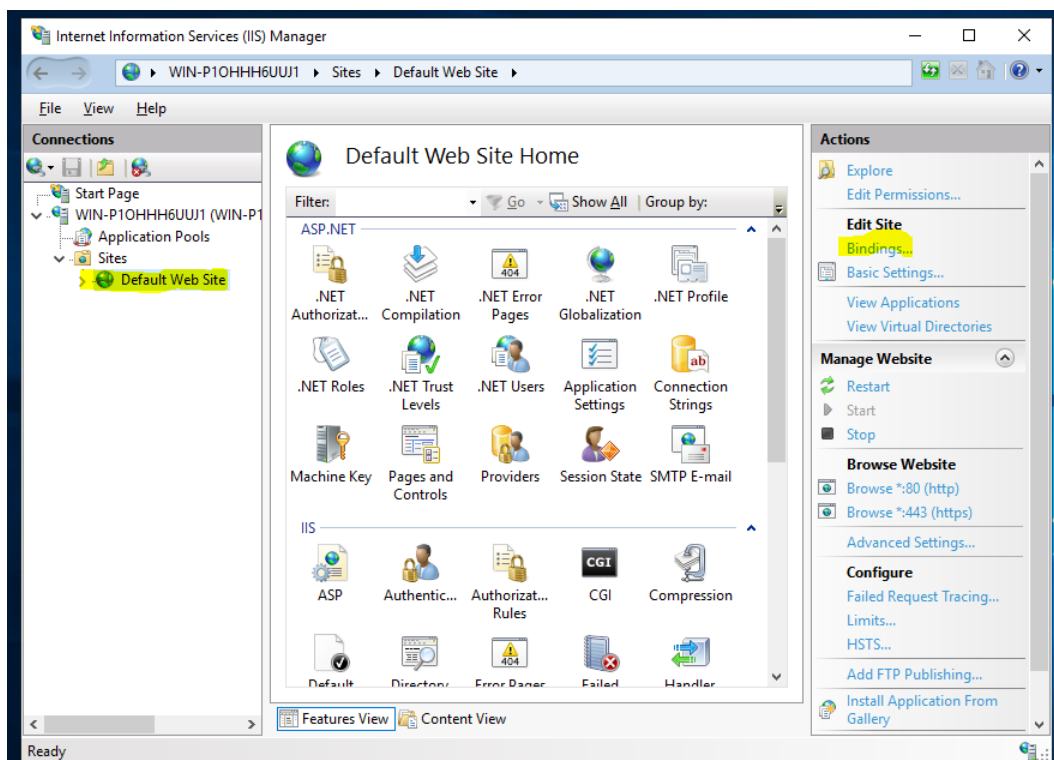
12 Configure DR-SBA Web to Work with HTTPS

This section describes how to configure the DR-SBA Web interface to work over HTTPS.

To configure HTTPS for DR-SBA Web interface:

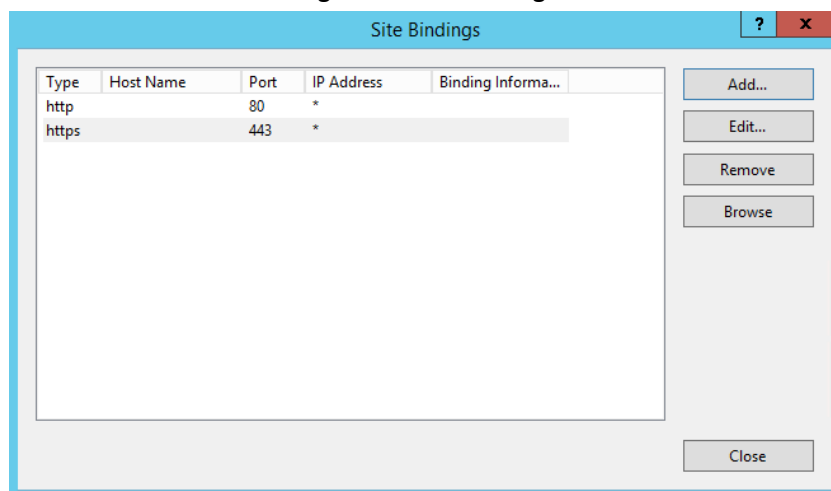
1. For configuring the DR-SBA Web interface to work over HTTPS, a certificate is required. – You can use same certificate you selected for the DR-SBA (with the DR-SBA FQDN CN) or install a different certificate for the DR-SBA Web.
2. Open Microsoft Internet Information Services (IIS).
3. Open the "Default Web Site" site and then click **Bindings**:

Figure 93: Default Web Site



The following site appears:

Figure 94: Site Bindings



4. If you don't have a binding line for HTTPS, click **Add**. If you have the HTTPS line, click **Edit**; the following screen appears:

Figure 95: Edit Site Bindings

Edit Site Binding

Type: **https** IP address: **All Unassigned** Port: **443**

Host name:

☐ Require Server Name Indication

☐ Disable HTTP/2

☐ Disable OCSP Stapling

SSL certificate:

localhost
Not selected
WMSVC-SHA2
localhost
*.audctrunk.aceducation.info

Select... View...

OK Cancel

5. From the 'Type' drop-down list, select **https**.
6. From the 'SSL certificate' drop-down list, select the certificate created by the DR-SBA setup (or use the certificate that you added for the Web interface).
7. For the certificate created by the DR-SBA, use the DR-SBA FQDN as the Subject Name (When you access the DR-SBA's Web interface using this Web certificate, you need to enter the DR-SBA's FQDN as the URL –requiring local DNS resolving).
8. By default, binding to port 80 is available. If you want to enable access only through HTTPS (and therefore block HTTP), you need to delete the HTTP binding. Before doing this, check that HTTPS is functioning correctly.

13 Running an Anti-Virus Software

To ensure that the antivirus scanner does not interfere with the operation of DR-SBA, you must exclude specific processes and directories. The following processes and directories should be excluded:

- Directories (need to exclude subfolders too):
 - C:\Program Files\AudioCodes
 - C:\Program Files\Microsoft\Microsoft SBA
 - C:\AudioCodes
 - C:\PHP\log
- DR-SBA processes:
 - C:\Program Files\AudioCodes\TeamsSbaConfig\TeamsSbaConfig.exe
 - C:\Program Files\AudioCodes\SbaRecovery\SbaRecovery.exe
 - C:\Program Files\AudioCodes\MainAgent\MainAgent.exe
 - C:\Program Files\AudioCodes\AlarmsAgent\AlarmsAgent.App.exe
 - C:\Program Files\Microsoft\Microsoft SBA\Sba\Microsoft.Teams.SBA.exe
- IIS processes:
 - %systemroot%\system32\inetsrv\w3wp.exe
 - %systemroot%\SysWOW64\inetsrv\w3wp.exe

14 Known Issues

- To view the list of updated known issues published by Microsoft, click [here](#).
- When the Teams DR-SBA IP address is changed and the SIP listen IP address is updated, the MSFT service needs to be restarted.
- When recovering from USB and the goRecover command fails, try to run goRecover again without rebooting.
- The Microsoft API returns a "503 Error" when there is no certificate that matches the DR-SBA FQDN. When the basic API returns a "serverCertificateCommonName" that does not exist on the server certificate list, the call to the general API returns a "503 Error".
- As a workaround, open "sbasettings.json" under C:\Program Files\Microsoft\Microsoft SBA, and then change the "ServerCertificateCommonName" parameter to "ServerCertificateCommonName": "localhost". You can then save the file and reset the Microsoft SBA service.
- A TLS connectivity check to sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com is required as part of the firewall requirements. If this check is denied by the firewall, the DR-SBA doesn't function. A log is recorded every 30 seconds in the sba.log file, showing "TcpClient did not manage to establish connection. No connectivity with sip.pstnhub.microsoft.com".
- If you install the SBA server and then change the name of the computer on which the SBA is installed, an alarm is raised (even though it doesn't affect functionality). To resolve this issue and clear this alarm, see Section 15.10, Clearing Alarm Due to Computer Name Change.
- DR-SBA doesn't support numbers with extensions. For example, if the outbound routing is destined to '+xxxxxxxxxx;ext=1000', it's routed without using the extension.

15 DR-SBA Troubleshooting

This section describes DR-SBA troubleshooting issues.

15.1 Validate Tenant is Enabled for DR-SBA

Enter the following command to validate if new PowerShell commands are available:

```
Get-Command *TeamsSurvivableBranchAppliance*
```

15.2 Ensure User is Enabled for DR-SBA

You can use the following process to ensure that the Teams user has been enabled for DR-SBA support:

1. Restart the Microsoft Teams client.
2. Immediately after restart, download the MSTEams Diagnostics Log (see here for instructions on how to collect them).
3. Open the file with a name like MSTEams Diagnostics Log 12_9_2019__10_58_11_AM.txt and search for the string enableSurvivability. It should display a value of true like in the example below:
 - "enableSurvivability": true,
 - If it displays false validate that user was granted DR-SBA policy.

15.3 Verify which DR-SBA the Client Retrieves Based on Policy

Search the diagnostics log collected above for lines similar to below:

```
2020-09-22T01:04:37.595Z Inf SurvivabilityService:  
[setAvailableAppliances] setting appliances to  
[{"fqdn":"sba1.contoso.dk"}]
```

If you do not view lines similar to the above, this means that the user has not been granted the correct policy or that the policy does not contain the expected DR-SBA.

15.4 Verify if Client can Send Keep-Alive Messages to DR-SBA

Search the diagnostics log collected above for lines similar to below:

```
2020-09-22T01:04:37.595Z Inf SurvivabilityService:  
[setupApplianceLivenessChecks] 1 appliances have been pinged  
[appliances=[{"fqdn":"sba1.contoso.dk","lastCheck":1600736677529,"  
isUp":true}]]  
2020-09-22T01:04:37.582Z Inf SurvivabilityService:  
[setupApplianceLivenessChecks] appliance reached successfully  
[status=200]
```

If you don't see lines similar to above, this means that Keep-alive messages that are sent from the Teams client reach the DR-SBA.

If you see lines similar to below, this means that the Keep-alive messages that are sent from the Teams client do not reach the DR-SBA. Check firewall settings on the SBC, name resolution and general network connectivity issues between the Teams client and the DR-SBA.

```
2020-09-22T01:04:37.595Z Inf SurvivabilityService:  
[setupApplianceLivenessChecks] 1 appliances have been pinged  
[appliances=[{"fqdn":"sba1.contoso.dk","lastCheck":1600736677529,"  
isUp":false}]]
```

15.5 DR-SBA to SBC SIP OPTIONS Not Responding

If you don't see any response from DR-SBA to SBC SIP OPTIONS, make sure that the SBC was added to Teams.

15.6 Collect Required Information to Report an Issue

To create a log for troubleshooting, set the trace level of MSFT service's log file to 'Trace':

1. Browse to **C:\Program Files\Microsoft\Microsoft SBA** and edit the **sbasettings.json** file.
2. Change the trace level from '**Info**' to '**Trace**'
3. Restart the MSFT service.
4. Wait 4-5 minutes before you make the test call.
5. Make the test call.
6. Collect the logs.
7. Revert the log level back to '**Info**' and restart the MSFT service again.

To collect the information for AudioCodes technical support regarding the troubleshooting of issues, Provide the following information:

- Detailed description of the scenario.
- Date & Time in UTC time zone for when the issue happened.
- Traces files from Microsoft Teams immediately after you reproduced the issue.
- SBC traces corresponding to the client-side traces.
- For obtaining the necessary trace information from the Microsoft Teams client: Microsoft Teams debug logs, click [here](#).

15.7 One-Way Voice

Check that the ICE Mode is set to **Lite** d for the DR-SBA profile IP Profile on the SBC configuration.

15.8 LMO (Local Media Optimization) not Working

The DR-SBA SBC should be connected on the outbound leg to the main site SBC (the Proxy Set that is paired as the Microsoft Teams Direct Routing interface) and not paired with the Teams SIP HUB.

15.9 Validating Active Users

Connect through RDP and use the following link localhost:8081/api/v1/diagnostics/users to get a list of activated users (with valuable information, e.g., “Last Active Time” and “Token Expiry Time”):

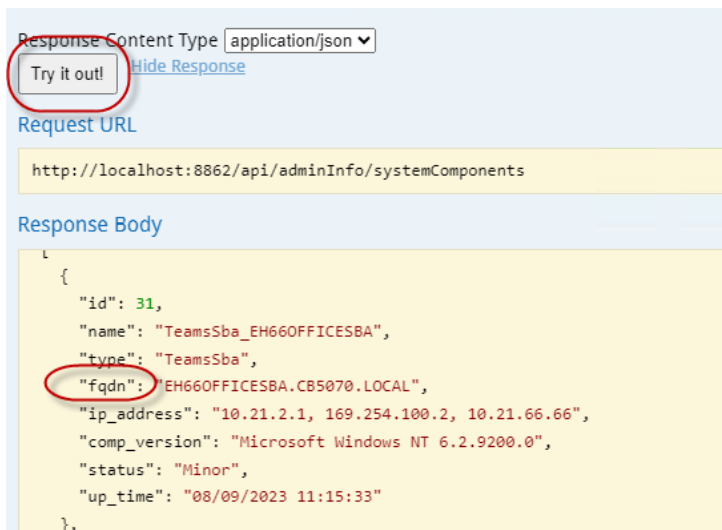
```
[{"userId":"110051a8-67b8-4f41-9803-1fbf49ed7fda","sipUri":"sip:sps2121@cce.aceducation.info","lastActiveTime":"2023-07-31T15:32:54.7590087","lastSyncTime":"2023-07-20T20:03:26.9582457","tokenExpiresAt":"2023-08-01T05:44:58"}, {"userId":"36198c46-8c34-462b-8489-fc4df5ed71c5","sipUri":"sip:sps2119@cce.aceducation.info","lastActiveTime":"2023-07-31T15:32:25.0898998","lastSyncTime":"2023-07-20T20:03:26.9582457","tokenExpiresAt":"2023-07-31T17:56:51"}]
```

15.10 Clearing Alarm Due to Computer Name Change

If you deploy the SBA server and then change the name of the computer on which the SBA is installed, the alarm *acGaManEnvUnreachableAlarm* is raised (even though it doesn't affect SBA functionality).

To resolve this issue and clear this alarm, you need to delete the old computer name:

1. Open Swagger:
 - a. Perform a remote desktop to the SBA.
 - b. Open Chrome or Edge, and then go to http://localhost:8862/swagger/ui/index#!/AppSystemInfoSettings/AppSystemInfoSettings_GetSystemComponents.
2. Navigate to *GET /api/admininfo/systemComponents*.
3. Click **Try it out!**; the output looks something like this:



4. Copy the FQDN to your clipboard (verify that it's the old computer name).
5. Scroll down to the **DELETE** button for */api/admininfo/systemComponents/{fqdn}*, and then click the button.

6. Paste the FQDN from your clipboard into the 'Value' field for the **fqdn** parameter:

DELETE /api/adminInfo/systemComponent/{fqdn}

Response Class (Status 200)

Model | Model Schema

{ }

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
fqdn	<input type="text" value="(required)"/>		path	string

Try it out!

7. Click **Try it out!**.
8. Verify that a 200 OK response is sent.
9. Scroll back up to *GET /api/admininfo/systemComponents* and verify that the old FQDN no longer exists.

16 Q&A

This section provides answers to frequently asked questions.

16.1 Multiple DR-SBAs per Site

You can deploy multiple DR-SBAs at a site and add Microsoft Teams clients to the policy associated with the DR-SBAs.

DR-SBAs provide flexible deployment options for SBCs:

- **One-to-Many:** A single DR-SBA can work with multiple SBCs.
- **Many-to-Many:** Multiple DR-SBAs can work with multiple SBCs.
- **Many-to-One:** Multiple DR-SBAs can work with a single SBC.

Every SBC must send SIP OPTIONS keep-alive messages to all the DR-SBAs.

Call forking must be done for all DR-SBAs.

Teams clients send keep-alive messages to all DR-SBAs in the policy. For survivability, if the internet goes down, the Teams clients choose one of the DR-SBAs (using round-robin).

16.2 Different Management and Media Interfaces

DR-SBA can have different network interfaces for management and media.

To have separate interfaces, you can use two NICs:

- One NIC for external communication with the internet (i.e., interfacing with Microsoft Teams).
- One NIC for internal communication (i.e., DR-SBA <-> SBC, and Teams clients -> DR-SBA).

When configuring (in the wizard) the DR-SBA, in the 'SIP Listen IP' field, you need to select the IP address that is used for the DR-SBA <-> SBC, and Teams clients connection (see Add DR-SBA via Login to Tenant).

17 Re-image DR-SBA from USB

This Appendix describes the process, how to create a bootable USB dongle, loaded with the DR-SBA for Teams image.



This section is only relevant for OSN-based devices (Mediant 800C and Mediant 1000B DR-SBAs) and is not relevant for the Virtual Appliance DR-SBA.

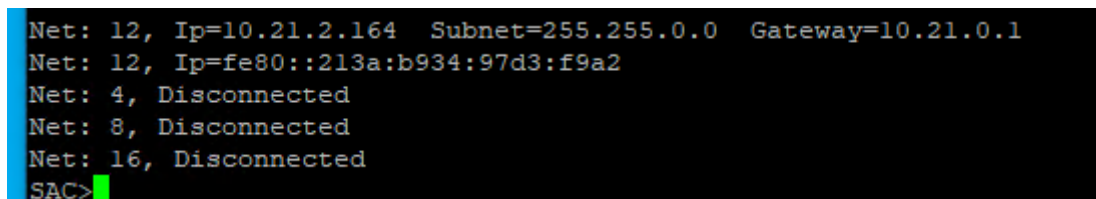
17.1 Burn DR-SBA via USB

1. Plug the USB into the USB port on the rear panel.
2. Connect the console port (Mediant 800C and Mediant 1000B) or HDMI port (Mediant 1000B) to your monitor (screen).
3. For COM Console connection: on your PC/Laptop, find the COM port via the Device manager and use PuTTY, for example, to open a console (115200, n8).
4. Reset the power.
5. Boot from the USB. Most of the hardware boots from the USB automatically if a USB is detected. If this is not the case, access BIOS and select to boot from the USB, or access the Boot menu and select to boot from USB.
6. Proceed to one of the following procedures:
 - COM Console (see below)
 - KVM/VGA Systems (see Section 17.3)

17.2 COM Console

1. After booting from USB, the SAC console appears; wait to see the following message: "EVENT: The CMD command is now available."
2. Type the following:
`cmd`
3. Type the following:
`ch -sn Cmd0001 (Cmd0001 the channel that is open for you see the exact number on the screen)`
4. To burn the SSD, type the following:
`goRecovery.exe`
when prompted, click 'Yes' to approve and continue
When completed, a text message is displayed to remove the USB and reset; remove the USB, enter 'exit' and when the SAC console appears, type 'restart'.
The system boots twice due to the sysprep.
5. After the second boot, connect the OSN (rear panel of the Mediant device) to the network.
6. Type "i" and then the IP address that was retrieved from the DHCP should be displayed.

Figure 96: Display the IP Address



```
Net: 12, Ip=10.21.2.164 Subnet=255.255.0.0 Gateway=10.21.0.1
Net: 12, Ip=fe80::213a:b934:97d3:f9a2
Net: 4, Disconnected
Net: 8, Disconnected
Net: 16, Disconnected
SAC>
```

If a static IP address needs to be set, use the following command:

```
i <#> <ip> <subnet> <gateway>
```

<#> is the interface number – the example above interface number 12 is connected and can be set.

For example: i 12 10.21.2.164 255.255.0.0 10.21.0.1

17.3 KVM/VGA Systems

After booting from USB, the cmd screen is displayed.

1. Type **goRecovery.exe** to burn the SSD.
2. When complete, a text message is displayed to remove the USB and reset. Remove the USB, enter exit, and then validate that the system restarts.

The system boots twice due to the sysprep.

After the second boot, you can connect to Windows, set the IP address manually or see which IP address was received from DHCP.

17.4 Teams DR-SBA Update Procedure

To upgrade AudioCodes Teams DR-SBA:

1. Download the new GUI version from https://downloads-audiocodes.s3.amazonaws.com/Download/AC_Teams_SBA_upgrade.html.
2. Stop the Microsoft Teams SBA service.
3. Backup the DR-SBA settings by copy the sbasettings.json under C:\Program Files\Microsoft\Microsoft SBA.
4. Open the **Add Or Remove Programs** menu, and uninstall service **Microsoft Survivable Branch Appliance**.
5. Validate if Microsoft Skype for Business Online PowerShell exists in the **Add Or Remove Programs** menu. If it exists, uninstall Microsoft Skype for Business Online.
6. Upgrade Microsoft Teams PowerShell:
 - a. Start PowerShell.
 - b. At the prompt, type the following:

```
Install-Module -Name MicrosoftTeams -force
```
 - c. At the prompt, to check if an earlier version is installed, type the following:

```
Get-InstalledModule -Name MicrosoftTeams -AllVersions
```If an earlier version exists, uninstall it:

```
Uninstall-Module -name MicrosoftTeams -RequiredVersion  
<earlier PowerShell version>
```
7. Run the upgrade files that you downloaded.
8. Copy sbasettings.json back to C:\Program Files\Microsoft\Microsoft SBA.
9. Restart the server.

17.5 Recovery USB Update (for OSN-based devices)

The recovery USB can be upgraded as follows:

1. Download the new WIM file from https://downloads-audiocodes.s3.amazonaws.com/Download/AC_Teams_SBA_Wim.html
2. Copy the downloaded file to the root of the USB. (If there is no free memory, delete the old WIM file.)
3. In the USB recoveryUtil.ini file, change the WIM file name to the same name as the downloaded file.



If you don't have the original USB dongle and need to prepare one, see Creating a Bootable USB Dongle.

18 Survivability PSTN Calling using Cellular Backup

This section describes the required configuration to support DR-SBA backup connectivity through a cellular network for survivability. This occurs when there is no internet and connectivity with Teams cloud.

In normal operation (when there is connectivity), outgoing calls don't traverse the DR-SBA. Instead, the Teams client directly contacts the Teams cloud through the main router.

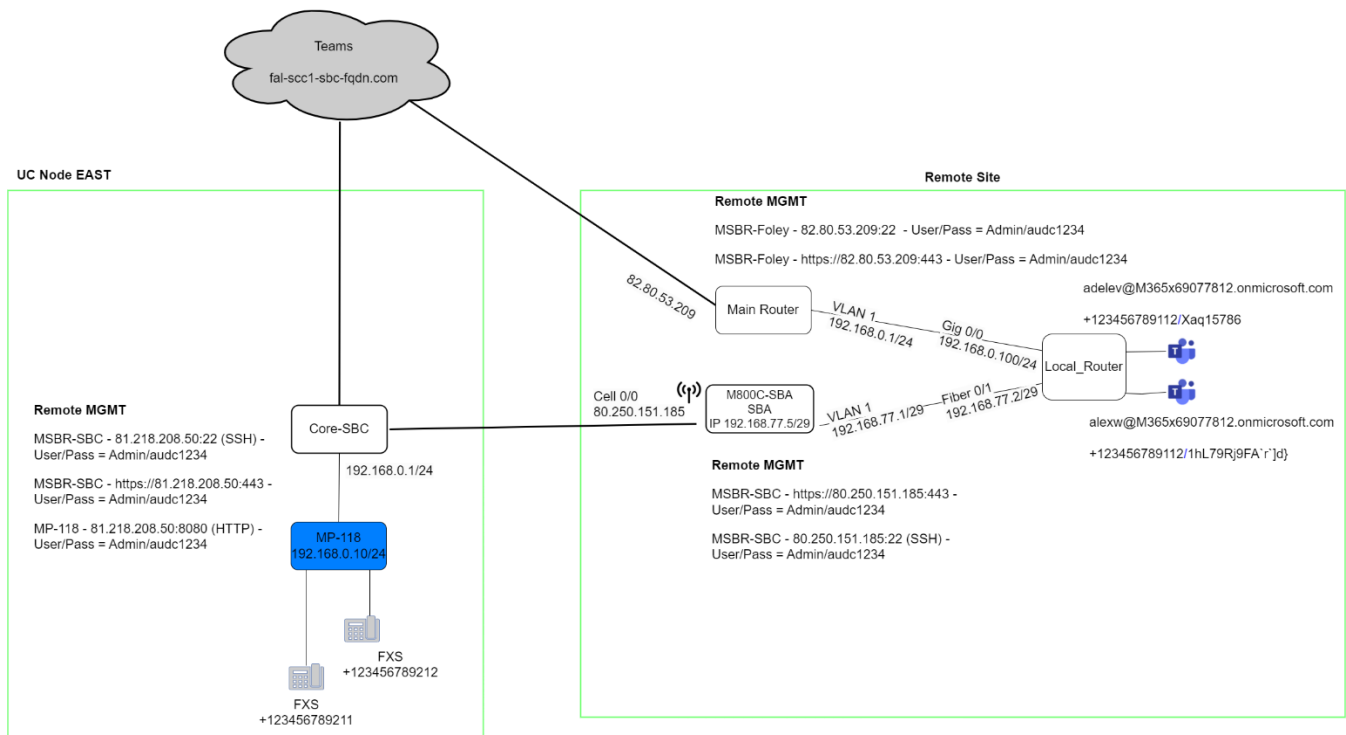
In survivability mode, the Teams client has no connectivity to the Teams cloud. The Teams client sends the traffic to the DR-SBA, which forwards the traffic to the PSTN using a unique backup channel on its cellular interface.



PSTN calling survivability over a cellular network is a special application that is applicable only to the Mediant 800C DR-SBA model that provides an internal 3G/4G cellular modem (CPN# **M800C-4S-LA-SBA-TMS**).

This feature is explained using the configuration example setup illustrated below.

Figure 97: Example Setup for PSTN Calling based on Cellular Backup



In this example setup, DR-SBA needs to be configured with the following interfaces:

- **interface osn:** Layer-2 connection between SBC and DR-SBA
- **interface VLAN 1:** Communication between SBC and DR-SBA
- **interface Cellular 0/0:** WAN cellular interface (backup interface)



- Configure DR-SBA according to this manual.
- The cellular interface must have a static IP address.
- DR-SBA must support ICE.
- The IP-to-IP Routing rule must operate in sequential mode and not forking ('Group Policy' parameter in the IP-to-IP Routing table).
- The IP host is sba-br3424.audiocodesaas.com [DR-SBA IP address] 120.

Configuration is as follows:

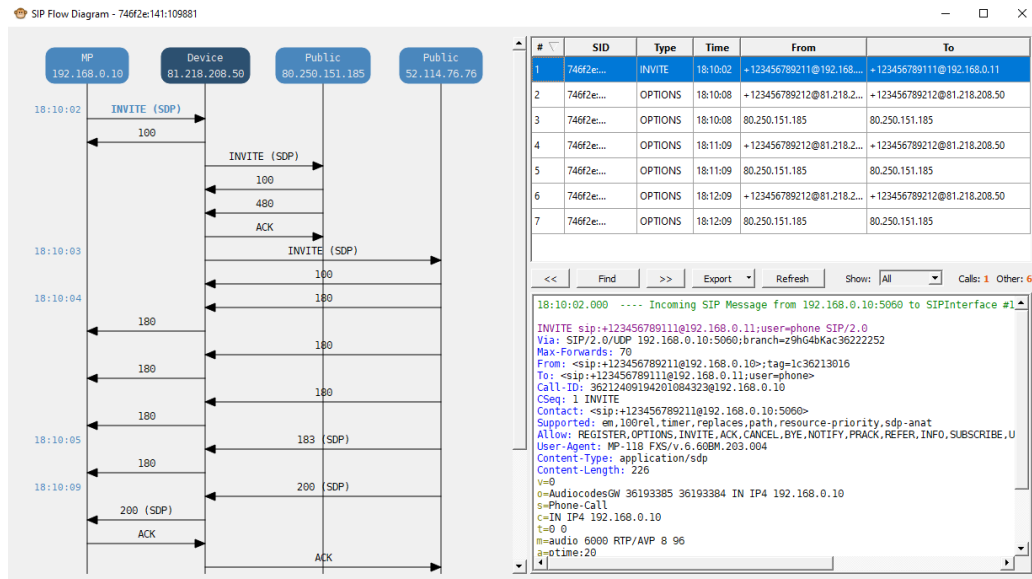
```
configure data
interface VLAN 1
ip address 192.168.77.1 255.255.255.248
mtu auto
desc "LAN switch VLAN 1"
no ipv6 enable
no service dhcp
ip dns server static
no napt
no firewall enable
no link-state monitor
no shutdown
exit
interface Cellular 0/0
desc "WAN Cellular"
mode dhcp
ip address auto
firewall enable
napt
mtu dhcp
profile
apn statreal
user user
obscured-pass 8oKSh4aBmIqd
exit
no ipv6 enable
no shutdown
ip dns server auto
exit
interface osn
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan add 1
no shutdown
exit
ip host sba-br3424.audiocodesaas.com 192.168.77.5 120
ip route 0.0.0.0 0.0.0.0 Cellular 0/0 1
ip route 192.168.20.0 255.255.255.0 192.168.77.2 VLAN 1 1
exit
```

Based on this example setup, the call flow for normal operation and survivability mode is as follows:

- **Normal Operation:** Call traverses the main router.

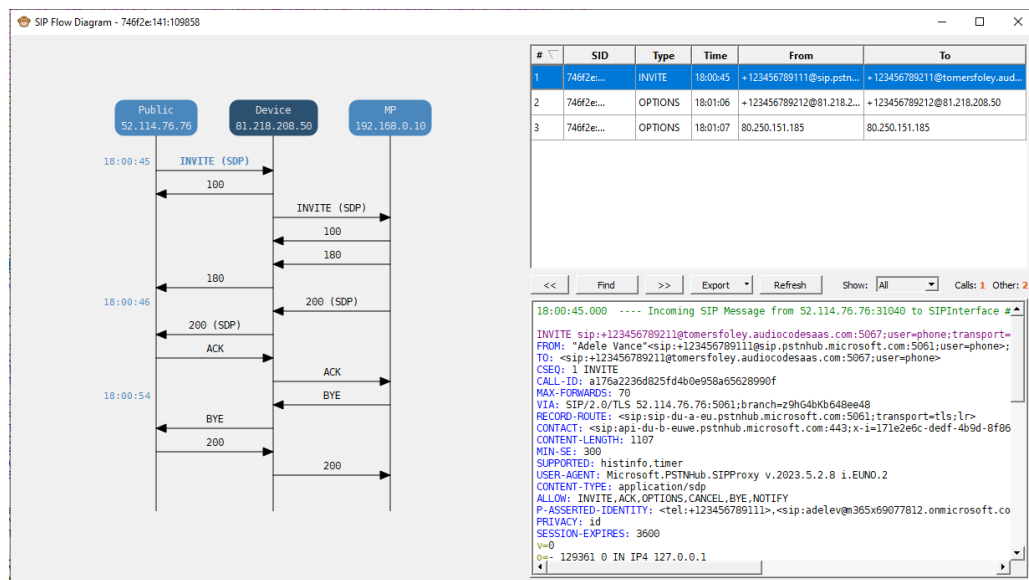
- **Incoming call:** PSTN > Core SBC > Teams Cloud > Main Router > Teams client (DR-SBA rejects the call with a SIP 480 as not in survivability mode)

Figure 98: Normal Operation – Incoming Call Flow



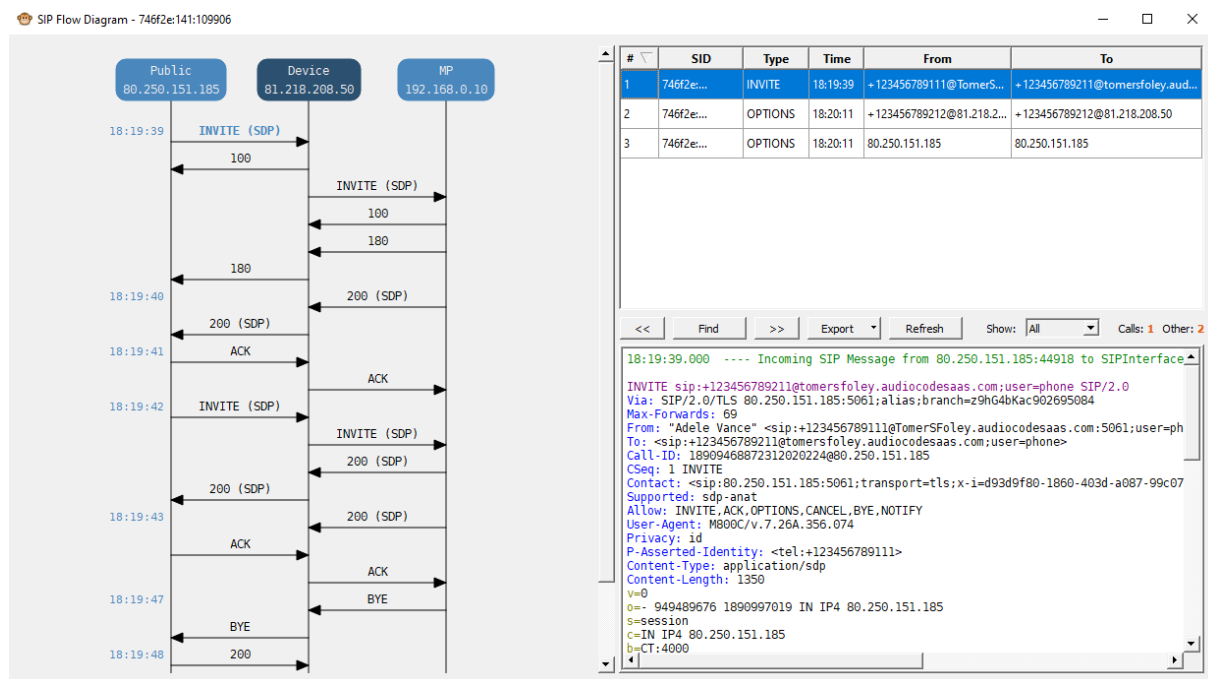
- **Outgoing call:** Teams client > Main Router > Teams Cloud > Core SBC > PSTN

Figure 99: Normal Operation – Outgoing Call Flow



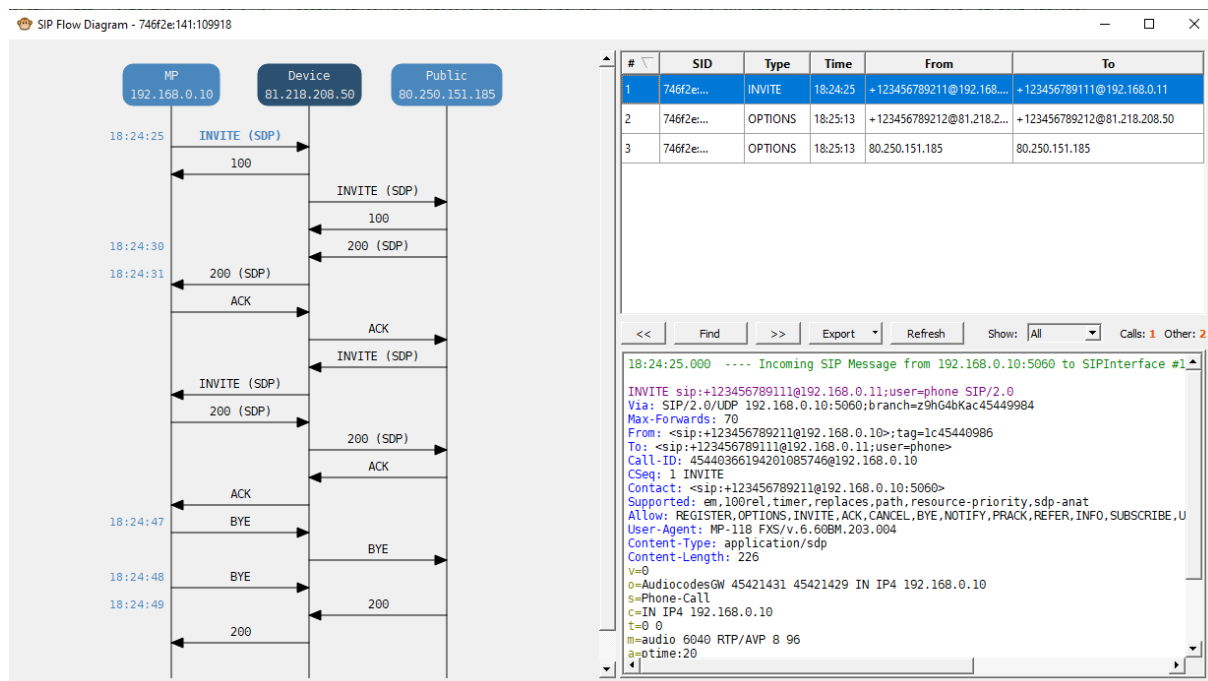
- **Survivability Mode:** Teams cloud and Main Router are not reachable.
- **Outgoing call:** Teams client > DR-SBA > Core SBC > PSTN

Figure 100: Survivability Mode – Outgoing Call Flow



- **Incoming call:** PSTN > Core SBC > DR-SBA > Teams client

Figure 101: Survivability Mode – Incoming Call Flow



19 Creating a Bootable USB Dongle

This section describes how to create a bootable USB dongle for DR-SBA.

To create a bootable USB dongle:

1. Prepare a new USB dongle that has a 32 GB storage size.
2. Start a PowerShell or Command Prompt session.
3. Enter diskpart:
`Commandline: diskpart`
4. List disks:
`Commandline: list disk`
5. Choose the USB Drive Number (where 0 is the number of the USB Drive):
`Commandline: select disk 1`
6. Clean the disk:
`Commandline: clean`
7. Create a primary partition on the disk:
`Commandline: create partition primary`
8. Format the partition to NTFS:
`Commandline: format fs=ntfs quick label="ACSSetup"`
9. Make the flash drive bootable:
`Commandline: active`
10. Assign a drive letter:
`Commandline: assign`
11. Exit diskpart:
`Commandline: exit`
12. Download the USB content from [https://downloads-audiocodes.s3.eu-central-1.amazonaws.com/SBA/TEAMS/Entire+USB+\(zip\)/DRSBA_1.1.001.zip](https://downloads-audiocodes.s3.eu-central-1.amazonaws.com/SBA/TEAMS/Entire+USB+(zip)/DRSBA_1.1.001.zip)
13. Unzip and copy all the files to the root directory of the newly created USB drive.
14. Continue according to Section Re-image DR-SBA from USB.

International Headquarters

Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com>

©2025 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: **LTRT-33498**

