
Ribbon SBC Core SWe R10.1 Interop with Microsoft Survivable Branch Appliance : Interoperability Guide

Table of Contents

- Interoperable Vendors
- Copyright
- Document Overview
 - About Ribbon SBC Core
 - About Virtual Survivable Branch Appliance (vSBA)
- Non-Goals
- Audience
- Prerequisites
- Product and Device Details
- Network Topology Diagram
 - Deployment Topology
 - Interoperability Test Lab Topology
- Document Workflow
- Section A: SBC Core Configuration
 - Network and Connectivity
 - Static Routes
 - Static route towards SBA
 - Configure SBC for MS Teams
 - Configure ERE for MS Teams
 - SBC Core SBA Leg Generic Configuration
 - Crypto Suite Profile
 - Codec Entry
 - RTCP for Media
 - SIP Domain
 - Path Check Profile
 - SIP Message Manipulation (SMM)
 - Microsoft SBA Leg Configuration
 - IP Interface Group
 - Zone
 - SIP Signaling Port
 - IP Peer
 - SIP Trunk Group
 - Routing Label
 - Call Routing
 - Configure PSX for MS Teams
 - IP Peer
 - Sip Domain
 - SIP Trunk Group
 - Routing Label
 - Standard Route
- Section B: Microsoft SBA Configuration
 - Prerequisites
 - Installation
 - Configuration
 - Name Resolution
 - Certificates
 - Importing a vSBA Certificate
 - X.509 Signed Certificate
 - Import PKCS12 Certificate and Key
 - Exporting a vSBA Certificate
 - Managing Trusted CA Certificate
 - Importing a Trusted CA Certificate
- Supplementary Services and Features Coverage
- Caveats
- Support
- References
- Conclusion

Interoperable Vendors



Copyright

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

The trademarks, logos, service marks, trade names, and trade dress (“look and feel”) on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

Document Overview

This document outlines the configuration best practices for the Ribbon solution covering the Ribbon SBC Core SWe when deployed with Microsoft Teams vSBA (virtual Survivable Branch Appliance).

About Ribbon SBC Core

A Session Border Controller (SBC) is a network element deployed to protect SIP-based Voice over Internet Protocol (VoIP) networks. Early deployments of SBCs were focused on the borders between two service provider networks in a peering environment. This role has now expanded to include significant deployments between a service provider's access network and a backbone network to provide service to residential and/or enterprise customers.

The SBC Core (SBC 5K, 7K, SWe) addresses the next-generation needs of SIP communications by delivering embedded media transcoding, robust security, and advanced call routing in a high-performance, small form-factor device enabling service providers and enterprises to quickly and securely enhance their network by implementing services like SIP Trunking, secure Unified Communications, and Voice over IP (VoIP).

The SBC Core provides a reliable, scalable platform for IP interconnect to deliver security, session control, bandwidth management, advanced media services, and integrated billing/reporting tools in an SBC appliance. This versatile series of SBCs can be deployed as peering SBCs, access SBCs, or enterprise SBCs (eSBCs). The SBC product family is tested for interoperability and performance against a variety of third-party products and call flow configurations in the customer networks.



SBC 5400, 7000, and SWe are represented as SBC Core in the subsequent sections.

About Virtual Survivable Branch Appliance (vSBA)

The Direct Routing Virtual Survivable Branch Appliance (vSBA) is a Ribbon Communications SBC SWe Edge offer accomplished through close cooperation with Microsoft®. The vSBA allows users to make and receive Public Switched Telephone Network (PSTN) calls when there is an outage.

When a customer site using Direct Routing to connect to Microsoft Phone System experiences an internet outage, the intranet inside the branch is still fully functional. Users can connect to the Session Border Controller (SBC) that is providing the PSTN connectivity.

During an internet outage, the Teams client should switch to the SBA automatically. No action is required from the user. As soon as the Teams client detects that the internet service is restored and any outgoing calls are finished, the client will fall back to normal operation mode and connect to other Teams services.

The interoperability compliance testing focuses on verifying inbound and outbound call flows between the Ribbon SBC SWe Core & Teams vSBA.



Direct Routing vSBA is available on the **SBC SWe Edge** Release 11.0x and later.

Contact your authorized Ribbon sales representative/partner for more information regarding approved SBC SWe Edge Direct Routing vSBA platforms and acquisition.

This guide contains the following configuration sections:

- [Section A: Ribbon SBC SWeCore Configuration](#)
 - Captures general SBC SWeCore configurations for deploying SBC with Teams vSBA.
- [Section B: Virtual SBA Configuration](#)
 - Captures the Microsoft SBA configuration.
- Basic Calls and Call Hold/Resume features can be tested with configurations from Section A and Section B.

Non-Goals

It is not the goal of this guide to provide detailed configurations that will meet the requirements of every customer. Use this guide as a starting point and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring both the Ribbon SBCs and the third-party product.

To perform this interop, you need to:

- use the graphical user interface (GUI) or command line interface (CLI) of the Ribbon product.
- understand the basic concepts of TCP/UDP/TLS and IP/Routing.
- have SIP/RTP/SRTP to complete the configuration, and for troubleshooting.



Note

This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided "AS IS". Users must take full responsibility for the application of the specifications and information in this guide.

Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC SWe Core
- Ribbon SWe Edge
- Public IP Addresses
- Microsoft admin account - a special type of account where the Teams user can be configured for Direct Routing SBA (Survivable Branch Appliance).
- TLS Certificates for Ribbon SBC Core signed by one of the Microsoft approved CA vendors.
- Certificates must have the FQDN or domain name that is configured on the Microsoft admin portal.
- A Windows Server 2019 VM with a minimum of four virtual processors, 8GB memory, and 80GB of disk space to install vSBA.

Product and Device Details

The sample configuration in this document uses the following equipment and software:

Table 1: Requirements

	Appliance/Application/Tool	Software Version
Ribbon Communications	SBC SWe Core	V10.01.01-R002
	SWe Edge	11.0.1 build 42
Microsoft	Survivable Branch Appliance (SBA)	v.2022.6.14.1

	Teams Client	1.5.00.17656 (64-bit)
PSTN Phone	PhonerLite	2.79
Administration and Debugging Tools	Ribbon LX Tool	2.1.0.6

Note

- Microsoft SBA version is v.2022.6.14.1 or later
- Teams Client version is 1.5.00.17656 (64-bit) or later
- PhonerLite version is 2.79 or later

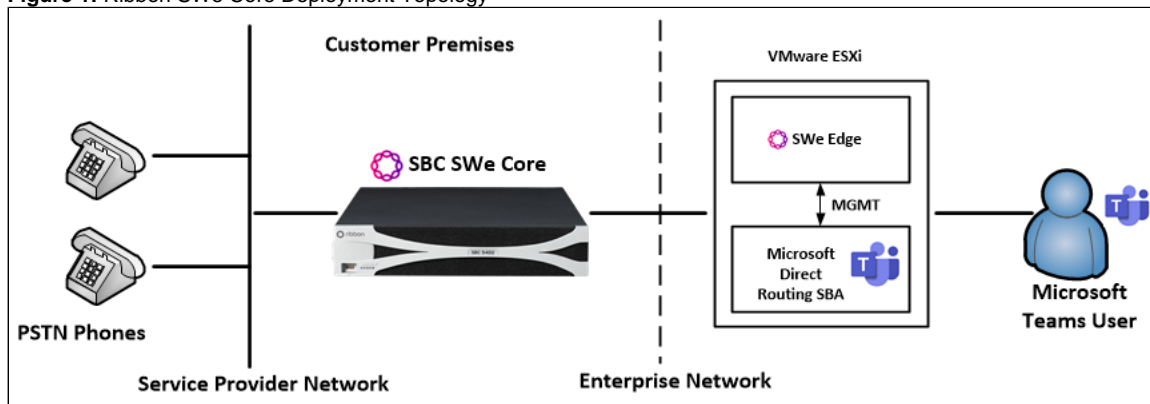
⚠ SoftPhones and IP-PBX are used to simulate PSTN.

Network Topology Diagram

This section covers the Ribbon SWe Core deployment topology and the Interoperability Test Lab Topology.

Deployment Topology

Figure 1: Ribbon SWe Core Deployment Topology



Interoperability Test Lab Topology

The following lab topology diagram shows connectivity between Ribbon SWe Core on virtual platform and Microsoft SBA.

Figure 2: SWe Core and Teams Direct Routing test lab topology

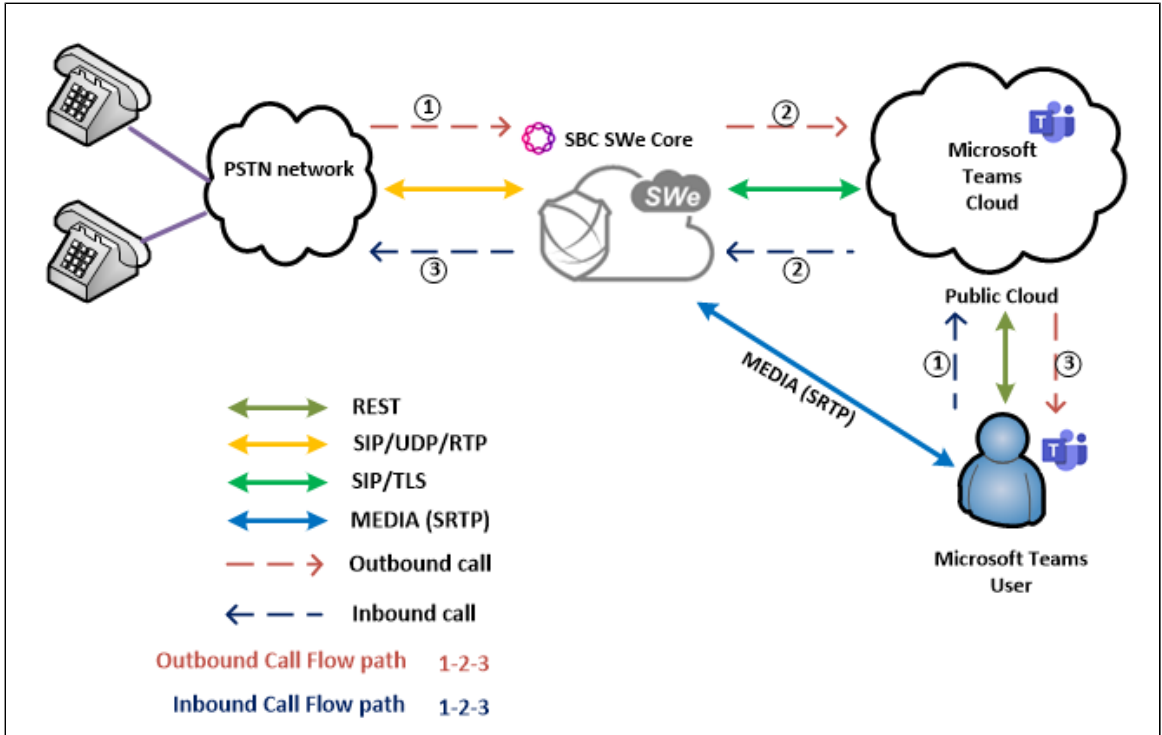
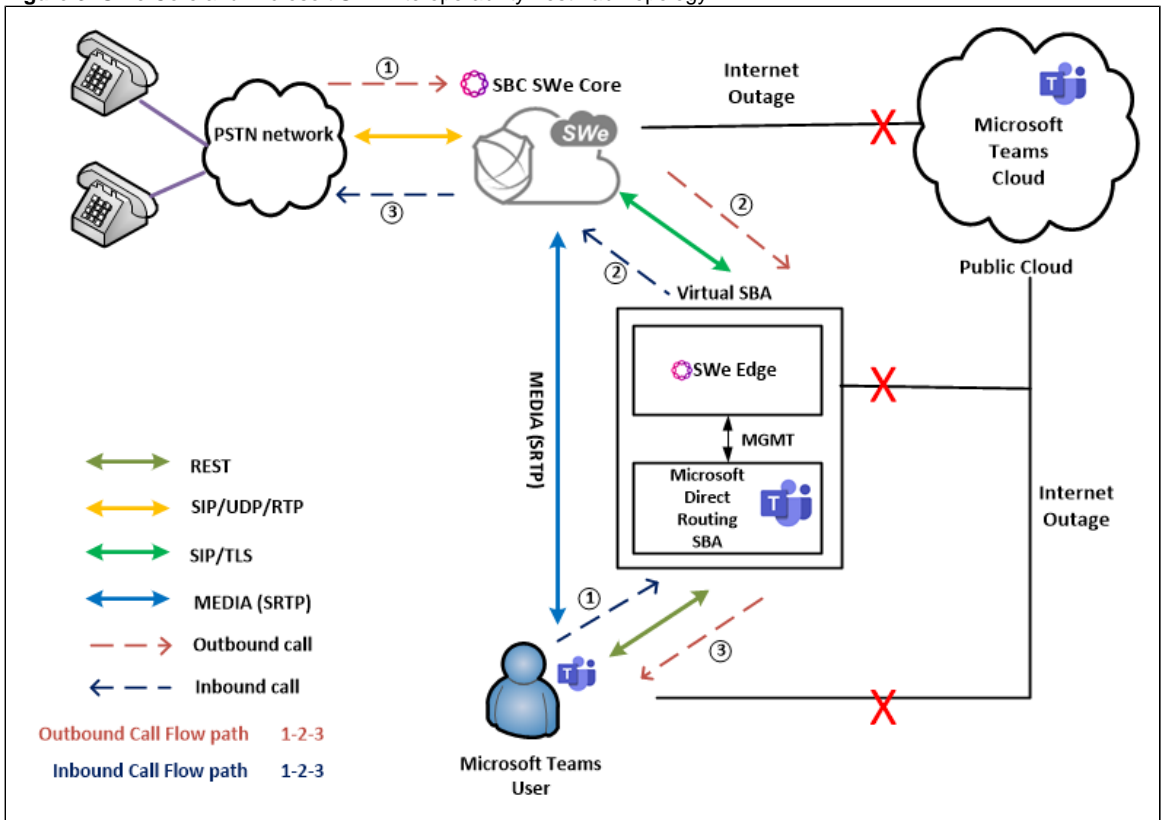
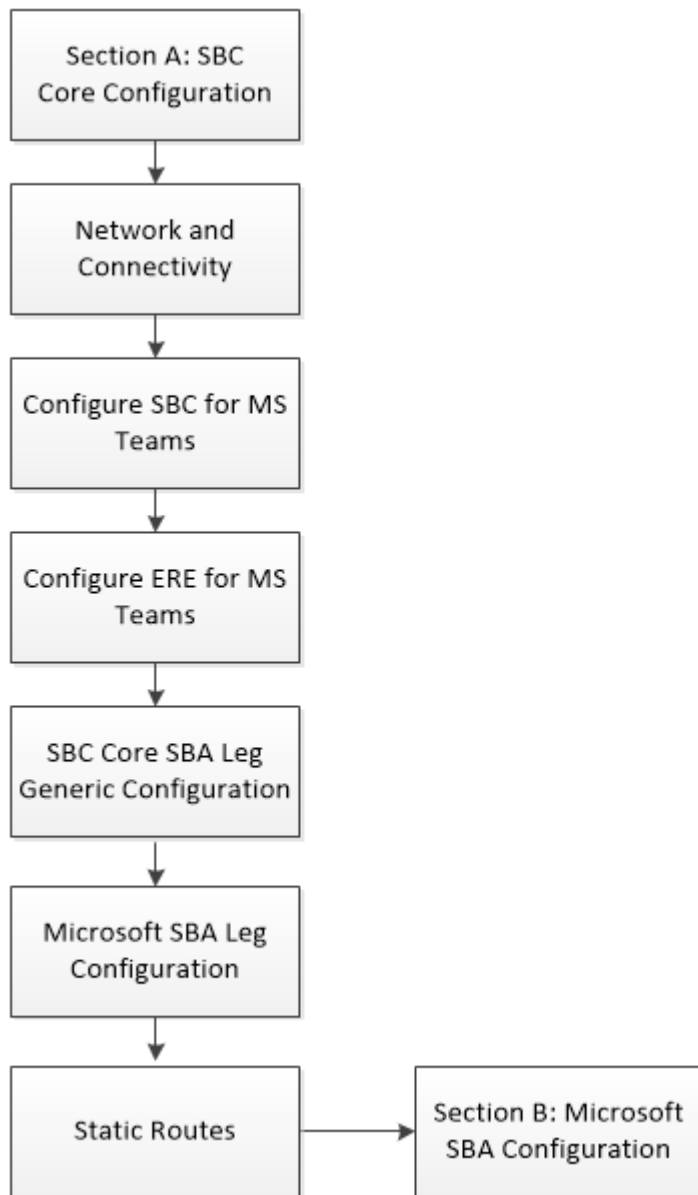


Figure 3: SWe Core and Microsoft SBA interoperability Test Lab Topology



Document Workflow



Section A: SBC Core Configuration

The following SBC Core configurations are included in this section:

[Network and Connectivity](#)

[Static Routes](#)

[Configure SBC for MS Teams](#)

[Configure ERE for MS Teams](#)

[SBC Core SBA Leg Generic Configuration](#)

[Microsoft SBA Leg Configuration](#)

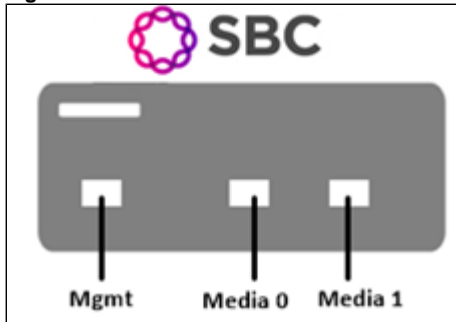
- SBC Core can connect to the network as mentioned in [Network and Connectivity](#).
- Microsoft SBA prefers transport as TLS. Establishing a TLS connection between SBC SWe Core and Microsoft SBA is covered under Configure SBC for TLS.
- SBC Core configuration for MS Teams Direct Routing and PSTN are covered under [Configure SBC for MS Teams](#).

- SBC Core configuration's PSP, IPSP, SIP Trunk Group, IP Peer, Routing Label, and Call Routing are covered under [Configure ERE for MS Teams](#).
- SBC Core generic configurations such as: crypto suite profile, codec entry and SMM are covered in [SBC Core SBA Leg Generic Configuration](#).
- SBC Core specific configuration in relation to the Microsoft SBA Leg is covered under [Microsoft SBA Leg Configuration](#).

Network and Connectivity

Ribbon SBC is as shown below:

Figure 4: Ribbon SBC



Mgmt is an RJ45 port and the management interface of the SBC.

Media 0/Media1, depicted as pkt0/pkt1, are RJ45 OR optical SFP ports. Media 0 and Media 1 are used in the current deployment and the same interfaces can be used in SBC Core 5K and 7K (appliance based). Typically, on 5K/7K these ports would be optical SFPs.

For the SBC SWe (virtualized platform), the logical pkt0/pkt1 interface must be mapped to a physical port.

Static Routes

Static routes are used to create communication to remote networks. In a production environment, static routes are mainly configured for routing from a specific network to a network that can only be accessed through one point or one interface (single path access or default route).

Tip

- For smaller networks with just one or two routes, configuring static routing is preferable. This is more efficient since a link is not wasted by exchanging dynamic routing information.
- For networks that have a LAN-side Gateway on Voice VLAN or Multi-Switch Edge Devices (MSEs) with Voice VLAN towards SBC Core, static routing configurations are not required.

Static route towards SBA

```
set addressContext default staticRoute 0.0.0.0 0 172.16.X.X LIF2 PKT1_V4 preference 100
commit
```

Configure SBC for MS Teams

SBC Core should be configured for Teams Direct Routing and PSTN with the below link:

<https://doc.rbbn.com/display/ALLDOC/Configure+SBC+for+MS+Teams>

Follow the section from Common SBC Configuration till Configure SBC for MS Teams Media Bypass.

Configure ERE for MS Teams

SBC Core has an Embedded Routing Engine (ERE). It can be configured as mentioned in the link below:

<https://doc.rbbn.com/display/ALLDOC/Configure+ERE+for+MS+Teams>



Once the above 2 sections are configured, proceed with the below mentioned sections.

SBC Core SBA Leg Generic Configuration

Crypto Suite Profile

Since there is a SRTP between the SBA and the SBC, a crypto suite profile needs to be created as follows:

```
set profiles security cryptoSuiteProfile CRYPT_PROF entry 1 cryptoSuite AES-CM-128-HMAC-SHA1-80
commit
```

Codec Entry

Codec entry allows you to specify the codec used for the call. Create the codec entry for G711 codec with a packet size 20 and rfc2833 method for dtmf.

```
set profiles media codecEntry G711-TEAMS codec g711
set profiles media codecEntry G711-TEAMS packetSize 20
set profiles media codecEntry G711-TEAMS law deriveFromOtherLeg
set profiles media codecEntry G711-TEAMS dtmf relay rfc2833
commit
```

RTCP for Media

To configure the RTCP for media, execute the following commands:

```
set system media mediaRtcpControl senderReportInterval 5
set system media mediaRtcpControl sendBYEPacket disabled
commit
```

SIP Domain

The SBC SIP domain is configured as follows:

```
set global sipDomain x.x.x.x
commit
```



Replace "x.x.x.x" with the SBC fqdn.

The SBA SIP domain is configured as follows:

```
set global sipDomain y.y.y.y
commit
```



Replace "y.y.y.y" with the SBA fqdn.

Path Check Profile

Create and attach a Path Check Profile to the SBA side:

```
set profiles services pathCheckProfile SBA_OPTIONS protocol sipOptions sendInterval 50 replyTimeoutCount 1
recoveryCount 1
set profiles services pathCheckProfile SBA_OPTIONS transportPreference preference1 tls-tcp
commit
```

SIP Message Manipulation (SMM)

Microsoft expects the fqdn in the From and Contact header of the OPTIONS message. Replace <user_input1> with the SBC's fqdn in the SMM below.

- rule 1 - replace the From header with the SBC's fqdn.
- rule 2 - replace the Contact header with the SBC's fqdn.
- rule 3 - add the User Agent header.

```

set profiles signaling sipAdaptorProfile SBAOPT state enabled
set profiles signaling sipAdaptorProfile SBAOPT advancedSMM disabled
set profiles signaling sipAdaptorProfile SBAOPT profileType messageManipulation
set profiles signaling sipAdaptorProfile SBAOPT rule 1 applyMatchHeader one
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 1 type message
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 1 message
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 2 type header
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 2 header
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 2 header name From
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 3 type token
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 3 token
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 3 token condition exist
set profiles signaling sipAdaptorProfile SBAOPT rule 1 criterion 3 token tokenType urihostname
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 type token
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 operation modify
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 from
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 from type value
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 from value <user_input1>
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 to
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 to type token
set profiles signaling sipAdaptorProfile SBAOPT rule 1 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile SBAOPT rule 2 applyMatchHeader one
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 1 type message
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 1 message
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 2 type header
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 2 header
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 2 header name Contact
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 3 type token
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 3 token
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 3 token condition exist
set profiles signaling sipAdaptorProfile SBAOPT rule 2 criterion 3 token tokenType urihostname
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 type token
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 operation modify
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 from
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 from type value
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 from value <user_input1>
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 to
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 to type token
set profiles signaling sipAdaptorProfile SBAOPT rule 2 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile SBAOPT rule 3 applyMatchHeader one
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 1 type message
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 1 message
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 2 type header
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 2 header
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 2 header name From
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 3 type token
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 3 token
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 3 token condition exist
set profiles signaling sipAdaptorProfile SBAOPT rule 3 criterion 3 token tokenType urihostname
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 type header
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 operation add
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 headerPosition last
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 from
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 from type value
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 from value "Ribbon SBCvirtual V10.01.01R002"
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 to
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 to type header
set profiles signaling sipAdaptorProfile SBAOPT rule 3 action 1 to value User-Agent

```

Apply this SMM globally as follows:

```
set global signaling messageManipulation outputAdapterProfile SBAOPT
commit
```

Microsoft SBA Leg Configuration

Create profiles with a specific set of characteristics corresponding to the Microsoft SBA. This includes the configuration of the following entities on the Microsoft SBA leg:

[IP Interface Group](#)

[Zone](#)

[SIP Signaling Port](#)

[IP Peer](#)


[SIP Trunk Group](#)

[Routing Label](#)

[Call Routing](#)

IP Interface Group

Create an IP interface group.


 Replace "x.x.x.x" with the SBC's packet interface (pkt) IP address towards SBA (example pkt1 IP), and "Y" with its prefix length. Provide the ceName used during an SBC deployment.

For example, the ceName is "TEAMSSBA1".

```
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ceName TEAMSSBA1 portName pkt1
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ipAddress x.x.x.x prefix Y
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 mode inService state enabled
commit
```

Zone


Create a Zone towards the SBA and specify the ID of the zone.

 This Zone groups the set of objects used for communication towards the SBA.

```
set addressContext default zone SBA_ZONE id 6
commit
```

SIP Signaling Port

Set the SIP Signaling port, which is a logical address used to send and receive SIP call signaling packets and is permanently bound to a specific zone.

 Replace "x.x.x.x" with the SIP Signaling Port IP address of the SBC towards the SBA.

```
set addressContext default zone SBA_ZONE sipSigPort 7 ipInterfaceGroupName LIF2
set addressContext default zone SBA_ZONE sipSigPort 7 ipAddressV4 x.x.x.x
set addressContext default zone SBA_ZONE sipSigPort 7 portNumber 5060
set addressContext default zone SBA_ZONE sipSigPort 7 tlsProfileName SBA_TLS
set addressContext default zone SBA_ZONE sipSigPort 7 transportProtocolsAllowed sip-tls-tcp
set addressContext default zone SBA_ZONE sipSigPort 7 mode inService
set addressContext default zone SBA_ZONE sipSigPort 7 state enabled
commit
```



Attach the TLS Profile created earlier in Configure SBC for TLS.



There are a few areas that result in a TLS negotiation issue. One area involves assigning the incorrect port. Ensure the following are accomplished:

- SBA listens on port number 5061 (default setting).
- Configure port number 5060 on the SBC IP-Peer, since Ribbon SBC Core increments the port by 1 when the transport protocol is TLS.

IP Peer

Create an IP Peer with the signaling fqdn of the SBA and assign it to the SBA Zone.



Replace "x.x.x.x" with the SBA fqdn.

```
set addressContext default zone SBA_ZONE ipPeer SBA policy description ""
set addressContext default zone SBA_ZONE ipPeer SBA policy sip fqdn X.X.X.X
set addressContext default zone SBA_ZONE ipPeer SBA policy sip fqdnPort 5060
set addressContext default zone SBA_ZONE ipPeer SBA pathCheck profile SBA_OPTIONS
set addressContext default zone SBA_ZONE ipPeer SBA pathCheck hostName X.X.X.X
set addressContext default zone SBA_ZONE ipPeer SBA pathCheck hostPort 5060
set addressContext default zone SBA_ZONE ipPeer SBA pathCheck state enabled
commit
```

SIP Trunk Group

Create a SIP Trunk Group towards the SBA and assign corresponding profiles such as PSP and IPSP, that were created in earlier steps.



You must configure Trunk Group names using capital letters.

```
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG media mediaIpInterfaceGroupName LIF1
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG ingressIpPrefix 0.0.0.0 0 commit
commit

set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG policy callRouting elementRoutingPriority TEAMS_ERP
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG policy media packetServiceProfile TEAMS_PSP
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG policy media toneAndAnnouncementProfile
TEAMS_LRBT_PROF
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG policy services classOfService DEFAULT_IP
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG policy signaling ipSignalingProfile TEAMS_IPSP
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG signaling relayNonInviteRequest enabled
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG signaling messageManipulation outputAdapterProfile
SBAOPT
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG services natTraversal iceSupport iceWebrtc
set addressContext default zone SBA_ZONE sipTrunkGroup SBA_TG ingressIpPrefix 0.0.0.0 0
commit
```

Routing Label

Create a Routing Label with a single Routing Label Route to bind the SBA Trunk Group with the SBA IP Peer.

```
set global callRouting routingLabel TEAMS_RL routingLabelRoute 4 trunkGroup SBA_TG
set global callRouting routingLabel TEAMS_RL routingLabelRoute 4 ipPeer SBA
set global callRouting routingLabel TEAMS_RL routingLabelRoute 4 inService inService
commit
```



Add the sipTrunkGroup SBA_TG and ipPeer SBA to the TEAMS_RL as routingLabelRoute 4, as this would be active only in Teams Survivable mode.

Call Routing

To route all the calls coming from the PSTN towards the Teams SBA:



Provide ceName used during an SBC deployment. "TEAMSSBA" is the ceName.

```
set global callRouting route trunkGroup PSTN_TG TEAMSSBA standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel TEAMS_RL
commit
```

To route all the calls, coming from the Teams SBA towards PSTN endpoints (irrespective of digits or FQDN):

```
set global callRouting route trunkGroup SBA_TG TEAMSSBA standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel PSTN_RL
commit
```

To route all the calls, coming from the Teams SBA towards PSTN endpoint depending on different numbers:

```
set global callRouting route none Sonus_NULL Sonus_NULL standard 2414445 1 all all ALL none Sonus_NULL
routingLabel PSTN_RL
commit
```



Above number based call routing is useful, when there are multiple PSTN service providers towards PSTN leg.

Section B: Microsoft SBA Configuration

For information on configuring the Survivable Branch Appliance (SBA) for Direct Routing refer to following link:

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-survivable-branch-appliance>

For the Prerequisites, Installation and Configuring the Direct Routing SBA refer to following link:

<https://doc.rbbn.com/display/UXDOC110/Best+Practice++Configure+Direct+Routing+Virtual+Survivable+Branch+Appliance#>

Prerequisites

For Prerequisites on Direct routing SBA, refer to the following link:

<https://doc.rbbn.com/display/UXDOC110/Best+Practice++Configure+Direct+Routing+Virtual+Survivable+Branch+Appliance#BestPracticeConfigureDirectRoutingVirtualSurvivableBranchAppliance-Prerequisites>

Installation

For Installation on Direct routing SBA refer to Step 1 in the following link:

<https://doc.rbbn.com/display/UXDOC110/Best+Practice++Configure+Direct+Routing+Virtual+Survivable+Branch+Appliance#BestPracticeConfigureDirectRoutingVirtualSurvivableBranchAppliance-Step1:InstallVirtualSBASoftware>

Configuration

For Configuring on Direct routing SBA refer to Step 2 in the following link:

<https://doc.rbbn.com/display/UXDOC110/Best+Practice++Configure+Direct+Routing+Virtual+Survivable+Branch+Appliance#BestPracticeConfigureDirectRoutingVirtualSurvivableBranchAppliance-Step2:SetuptheOffice365DirectRoutingvSBA>



- Strictly follow [Prerequisite](#), [Installation](#) and [Configuration](#) of the SBA respectively.
- To configure Ribbon SWe Core for Microsoft SBA follow the [Section A: SBC SWe Core Configuration](#).



As SWe Core would be interacting with Virtual Survivable Branch Appliance (vSBA) in the current deployment scenario, configuring [Step 3: Configure SBC SWe Edge](#) is not required, as this step is strictly for deployment scenarios involving Ribbon SWe Edge and vSBA.

Name Resolution

- A Public or Private Fully Qualified Domain Name (FQDN) that points to the Direct Routing vSBA IP - No Public IP is required for the Direct Routing vSBA.
- The Direct Routing vSBA should resolve the SBC Public FQDN with an address it can access, this is completed automatically for the SBC that hosts the ASM.



Use of Private FQDN for Direct Routing SBA

If you use a Private FQDN for Direct Routing SBA:

- The SBC will have to be configured to use the DNS that host this Private zone.
- You can not use a Public certificate for Direct Routing SBA, so Direct Routing SBA can not share the SBC Public Certificate.

Certificates

Microsoft requires a SHA256 certificate for the Direct Routing vSBA in order to establish a TLS connection with the SBC. See the following options:

1. **Shared SBC Public certificate (recommended)**. This is only possible if your SBC certificate matches one of the following options:
 - SBC Certificate is a wildcard certificate
 - SBC Certificate Common Name "CN: *.mydomain.com" or SBC Certificate Subject Alternative Name "SAN: *.mydomain.com".
 - SBC Certificate has a SAN for Direct Routing vSBA
 - SBC Certificate Common Name "CN: sbc.mydomain.com" and SBC Certificate Subject Alternative Name "SAN: sba.mydomain.com".
2. **Use an existing Public or Private Certificate that covers the Direct Routing vSBA FQDN.**
3. **Create a new Public or Private Certificate that covers the Direct Routing vSBA FQDN.** In this case, a Public or Private Certificate Authority must be ready to sign the certificate for the Direct Routing vSBA.

Importing a vSBA Certificate

You can import the following kinds of certificates:

- X.509 Signed Certificate.
- PKCS12 Certificate and Key.



Before importing a new Signed Server Certificate, you must first [import a valid Trusted CA Certificate](#).

X.509 Signed Certificate

Use the following procedure to import the X.509 Signed Certificate.

1. Log into the WebUI of the SBC SWe Edge.
2. Click the **Tasks** tab.
3. In the left navigation pane, select **Office 365 Direct Routing SBA > Setup**.
4. Click the **Manage Certificate** tab.
5. From the Action drop-down menu, select **Import X.509 Signed Certificate**.

Figure 5: X.509 Signed Certificate

The screenshot shows a web interface with a navigation bar at the top containing four tabs: 'Virtual DR SBA', 'Generate CSR', 'Manage Certificate', and 'Configure Office 365 Direct Routing SBA'. The 'Manage Certificate' tab is active. Below the navigation bar, the page title is 'Certificate' and the date/time is 'October 25, 2021 17:27:00'. The main content area is divided into three sections. The first section, titled 'Action', contains a dropdown menu with 'Import X.509 Signed Certificate' selected. The second section, titled 'Import X.509 Signed Certificate', contains a large text area with the label 'Paste Base64 Certificate'. The third section, titled 'Current Activity Status', shows a green checkmark icon and the text 'Last ASM IP Configuration action successfully completed.' Below this, it says 'Additional Information: Failed to send the ASM configuration parameter, configuration is stored and will be sent at the next attempt.' At the bottom right of the interface is a pink 'OK' button.

6. Paste the SBC CA certificate in the window and click **OK**.

Import PKCS12 Certificate and Key

Use the following procedure to import the PKCS12 Certificate and Key.

1. Log into the WebUI of the SBC SWe Edge.
2. Click the **Tasks** tab.
3. In the left navigation pane, select **Office 365 Direct Routing SBA > Setup**.
4. Click the **Manage Certificate** tab.
5. From the Action drop-down menu, select **Import PKCS12 Certificate and Key**. This option imports a certificate you created.

Figure 6: PKCS12 Certificate and Key

Virtual DR SBA Generate CSR **Manage Certificate** Configure Office 365 Direct Routing SBA

Certificate October 25, 2021 17:27:00 ?

Action


Action

Import PKCS12 Certificate and Key

Password *

Select File No file selected. *Extensions [.pfx or .p12] **

Current Activity Status

 Last ASM IP Configuration action successfully completed.

Additional Information: Failed to send the ASM configuration parameter, configuration is stored and will be sent at the next attempt.

6. In the **Password** field, enter the same password you created to export the certificate and key. Refer to [Exporting a vSBA Certificate](#).
7. Click **Browse** and select the desired PKCS12 file and key.
8. Click **OK**.

Exporting a vSBA Certificate

You can export the existing certificate installed on the Direct Routing vSBA.

1. Log into the WebUI of the SBC SWe Edge.
2. Click the **Tasks** tab.
3. In the left navigation pane, select **Office 365 Direct Routing SBA > Setup**.
4. Click the **Manage Certificate** tab.
5. From the Action drop-down menu, select **Export PKCS12 Certificate and Key**.

Figure 7: Exporting a vSBA Certificate

Certificate

Action

Action

Export PKCS12 Certificate and Key

Password *

Current Activity Status



Last ASM IP Configuration action successfully completed.

Additional Information: *Configuring ASM IP Address..*

OK

6. In the Password field, enter a password for the certificate file you want to export. This password is user generated/supplied and will be required if you [import this certificate](#) on another node.

7. Click **OK**.

Managing Trusted CA Certificate

A Trusted CA Certificate is a certificate issued by a trusted certificate authority. Trusted CA Certificates are imported to the SBC Edge Portfolio to establish its authenticity on the network.



Most Certificate Vendors sign the SBC Edge Portfolio certificate with an intermediate certificate authority. There is at least one, but there could be several intermediate CAs in the certificate chain. When importing the Trusted Root CA Certificates, be sure to import the root CA certificate and all Intermediate CA certificates. Failure to import all certificates in the chain causes the import of the SBC Edge Portfolio certificate to fail.

Importing a Trusted CA Certificate



Before you begin:

You must obtain a Trusted Root CA Certificate before you can proceed - your options are:

- Contacting your System Administrator or Certificate Vendor (e.g. Godaddy, Verisign etc).
- Obtaining the Trusted CA certificate from your local [Standalone Windows Certificate Authority](#).
- When importing a new certificate, make sure the root certificate is still valid and hasn't expired.

To import a Trusted CA Certificate:

1. Click the Import Trusted CA Certificate (📄) Icon.

Figure 8: Import Trusted CA Certificate

The screenshot shows a dialog box titled "Import Trusted CA Certificate" with a timestamp of "October 24, 2018 14:50:55". The "Mode" dropdown menu is set to "Copy and Paste". Below the mode menu is a large, empty text area labeled "Paste Base64 Certificate". At the bottom right of the dialog is a pink "OK" button.

The screenshot shows the same dialog box, but the "Mode" dropdown menu is now set to "File Upload". Below the mode menu, there is a "Select File" section with a "Choose File" button, the text "No file chosen", and "Extensions [der] *". At the bottom right of the dialog is a pink "OK" button.

2. Select either **Copy and Paste** or **File Upload** from the **Mode** menu.
 - a. If you choose **File Upload**, use the **Browse** button to find the file.
3. Click **OK**.

Verify Trusted CA Certificate

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Trusted CA Certificates**.

Figure 9: Trusted CA Certificate Table

Trusted CA Certificate Table							
Common Name	Issuer	Start Validity	Expiration	Key Length	Display	Primary Key	
njsbclab-RDC2-CA	njsbclab-RDC2-CA	Mar 5, 2015	Mar 5, 2020	2048		3	


 When the **Verify Status** field in the Certificate panel indicates Expired or Expiring Soon, the Trusted CA Certificate must be replaced. The old certificate must be deleted before a new certificate can be successfully imported.

Figure 10: Verify Status OK

Certificate	
Not Valid Before	Mar 5, 2015 14:40:03
Not Valid After	Mar 5, 2020 14:50:02
Serial Number	29F489B6D48FE8AE4A61B35C0EC8338D
Signature Algorithm	sha1WithRSAEncryption
Key Length	2048
Enhanced Key Usage	None
Key Usage	Digital Signature, Certificate Sign, CRL Sign
Subject Alternative Name	None
Verify Status	OK

Supplementary Services and Features Coverage

The following checklist depicts the set of services/features covered through the configuration defined in this Interop Guide.

Sr. No.	Supplementary Features/Services	Coverage
1	OPTIONS ping (SBC to SBA)	✓
2	OPTIONS ping (SBA to SBC)	✓
3	Basic Call from PSTN to Teams	✓
4	Basic Call from Teams to PSTN	✓
5	Call Hold & Call Resume	✓

Legend

✓	Supported
✗	Not Supported
N/A	Not Applicable

Caveats

The following items have been observed during this Interop - these are either limitations, untested elements, or useful information pertaining to the Interoperability.

- Media Bypass is a prerequisite for vSBA deployments.
- When using media bypass, the media between the Teams client and the SBC is using the SBC external (public) interface.
- This solution is to allow calls to/from the SIP trunk/PSTN, when connectivity to Microsoft Teams is lost – survivability mode.
- If the site loses internet connectivity and SIP trunk provider accesses the same internet connection, then the call will still fail because there is no path to the SIP trunk.
- LMO is currently not supported. Microsoft will need to support.

Support

For any support related queries about this guide, contact your local Ribbon representative, or use the details below:

- Sales and Support: 1-833-742-2661

- Other Queries: 1-877-412-8867
- Website: <https://ribboncommunications.com/services/ribbon-support-portal>

References

For detailed information about Ribbon products & solutions, go to :

<https://ribboncommunications.com/products>

For information about microsoft products & solutions, go to:

<https://docs.microsoft.com/en-us/microsoftteams/>

Conclusion

This Interoperability Guide describes a successful configuration of the Microsoft SBA interoperability with Ribbon SBC Core.

All features and capabilities tested are detailed within this document - any limitations, notes or observations are also recorded in order to provide the reader with an accurate understanding of what has been covered, and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - there maybe additional configuration changes required to suit the exact deployment environment.

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved.

