
Connect Ribbon SBC Edge to Microsoft Teams Direct Routing to Support Direct Routing Carrier

In this section:

- [Overview](#)
- [Step 1: Install SBC Edge \(if required\)](#)
- [Step 2: Prerequisites](#)
- [Step 3: Configure each Tenant](#)
- [Step 4: Confirm SBC Edge Links to Microsoft Teams](#)
- [Step 5: Place a Test Call](#)

Related articles:

- [Microsoft Teams Direct Routing Planning](#)
- [Connect SBC Edge to Microsoft Teams Direct Routing](#)
- [Connect SBC Edge to Microsoft Teams Direct Routing for Enterprises with Cloud PBX](#)
- [Connect SBC Edge to Microsoft Teams Direct Routing for Enterprises with Skype for Business On-Premises](#)

Overview

The SBC Edge is certified to offer Microsoft Teams Direct Routing services; the SBC Edge can be used to connect any Teams client to:

- A PSTN trunk, whether based on TDM (e.g. PRI, BRI, etc.), CAS, or SIP
- 3rd-party, non-Teams-certified SIP/TDM based PBXs, analog devices, and SIP clients

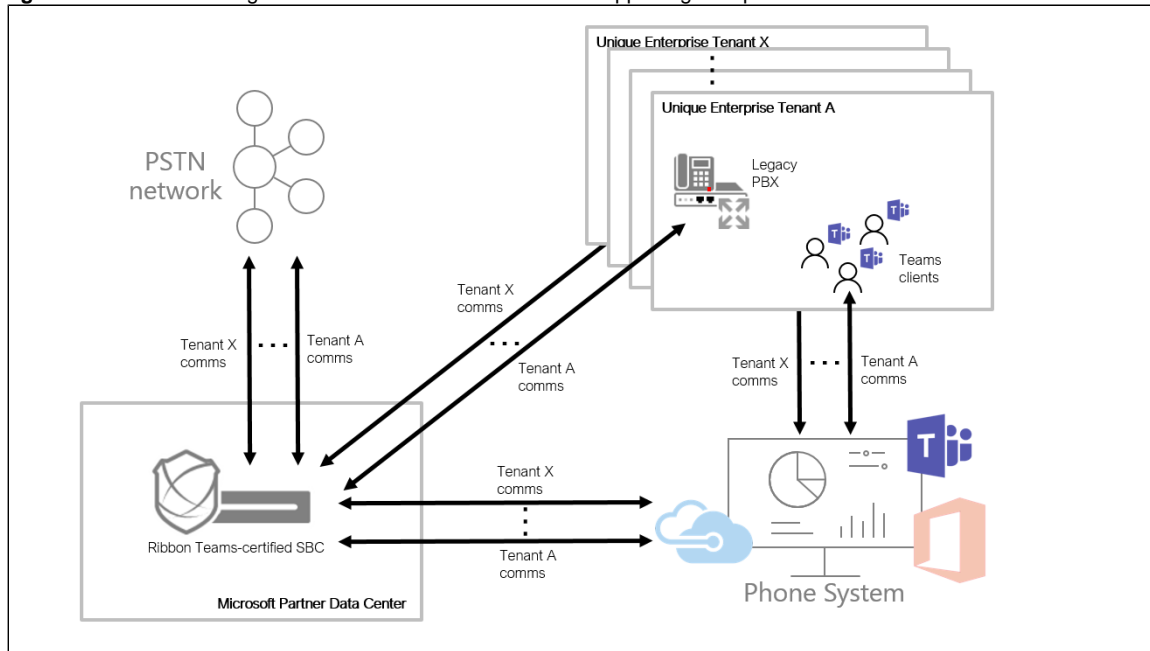
These instructions detail how to configure the SBC Edge (SBC 1000/2000 and SBC SWe Lite) deployed with a Microsoft partner (sells telephony services delivered to Microsoft Teams) to connect Microsoft Teams Direct Routing services for multiple independent enterprise customers (Tenants). A Tenant is used within the Microsoft environment as a single independent enterprise that has subscribed to Office 365 services; through this Tenant, administrators manage projects, users, and roles. Refer to [Configure a Session Border Controller for multiple Tenants](#) for Microsoft partner requirements in support of multiple Tenants.

Network Topology - SBC Edge Deployed in a Microsoft Partner Network to Connect Microsoft Teams Direct Routing for Multiple Tenants

The network diagram below shows an SBC Edge device deployed at the Microsoft partner data center, including communication between:

- Tenants and the enterprise's legacy PBX based clients, and
- Tenants and the PSTN supported by the Microsoft partner.

Figure 1: Ribbon SBC Edge at Microsoft Partner Data Center Supporting Multiple Tenants



Microsoft offer an advanced solution called "Carrier/Derived Trunk" that allows the Partner to control specific parameters on the end-user Tenants (list of codecs, port to use, Media Bypass activation, and such). This advance solution requires the following:

- Requires all the Derived Trunks (used by end customer) being a subdomain of the Carrier Trunk.
- Requires all Derived Trunks (used by end customer) to use Carrier Wild card certificate.
- Requires all the Derived Trunk (used by end customer) being configured with the same PSTN Gateway parameter (Codec, Max Call allowed, Media Bypass, and such).

For more information, refer to: <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants>.

How Call Traffic Routes between the SBC Edge and Microsoft Teams Tenants

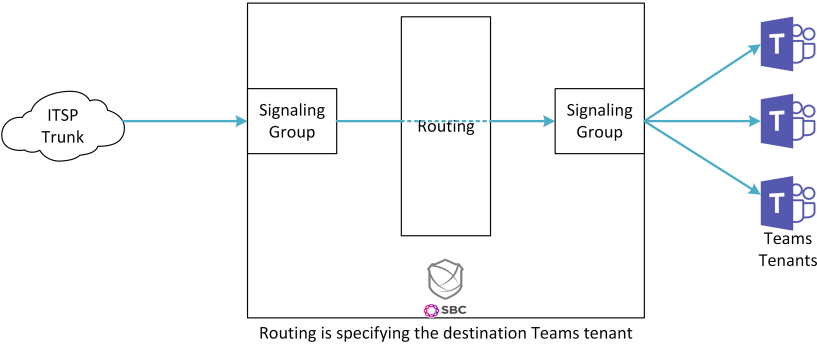
The network topology supported are detailed below.

Topology 1 - ITSP Aggregation for all Teams Tenants

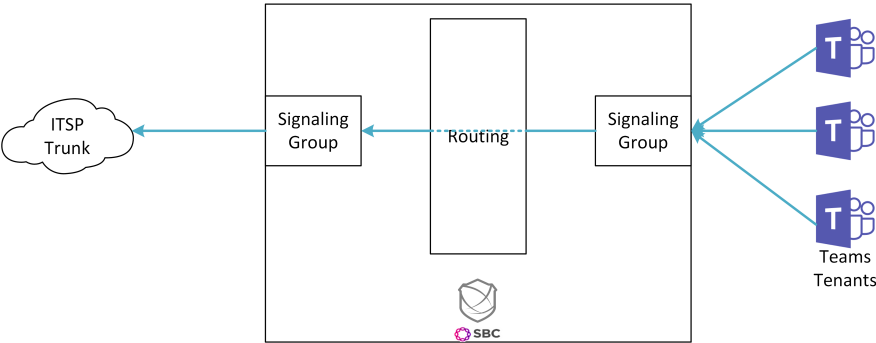
This network topology is referred to as "Microsoft Teams Direct Routing Carrier." This topology enables the partner to offer Microsoft Teams external calling capability to the end customer. Usually the partner owns the ITSP contract. For lower cost routing, the partner can choose to have more than one ITSP; routing is then decided based on destination, time of the day, and such.

Figure 2: Routing Summary for ITSP Aggregation

Multi-Tenant Direct Routing ITSP aggregation to Teams 8.1



Multi-Tenant Direct Routing Teams to ITSP aggregation

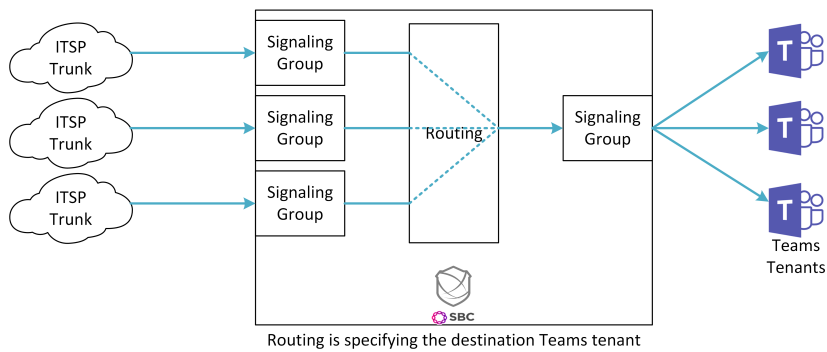


Topology 2 - ITSP Segregation per Teams Tenant

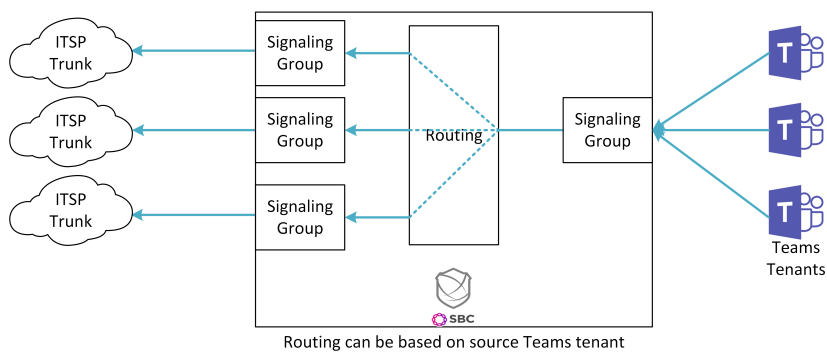
This network topology is referred to as "Teams Direct Routing Bring your Own Trunk." This topology enables the partner to offer the SBC management to the end customer. Usually the end customer owns the ITSP contract; only a specific Tenant can use the associated ITSP.

Figure 3: ITSP Segregation per Teams Tenant

Multi-Tenant Direct Routing ITSP segregation to Teams 8.1



Multi-Tenant Direct Routing Teams to ITSP segregation 8.1



Topology 3 - Teams Tenant Segregation

This network topology splits the inbound Teams traffic. For example, it can be useful to limit the number of sessions allowed per Teams Tenant from the SBC side or use a different certificate per Tenant. This topology requires an SBC configuration that limits the number of Tenants that can be supported on the SBC. Since this implementation requires one signaling port per Tenant, it does not support the Carrier/Derived Trunk capability.


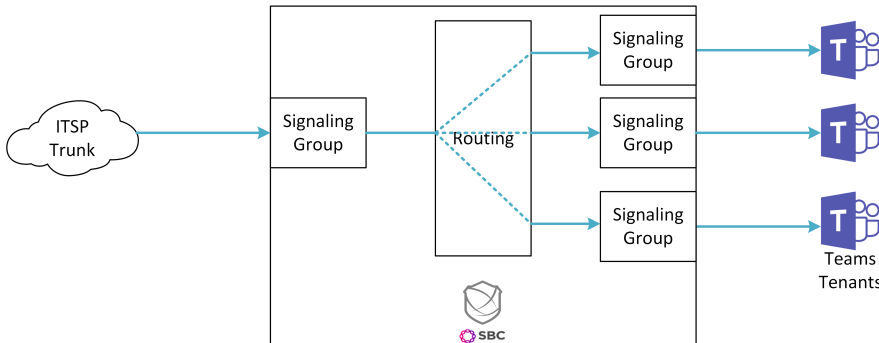
 This topology is not detailed in this Best Practice.

Figure 4: Teams Tenant Segregation

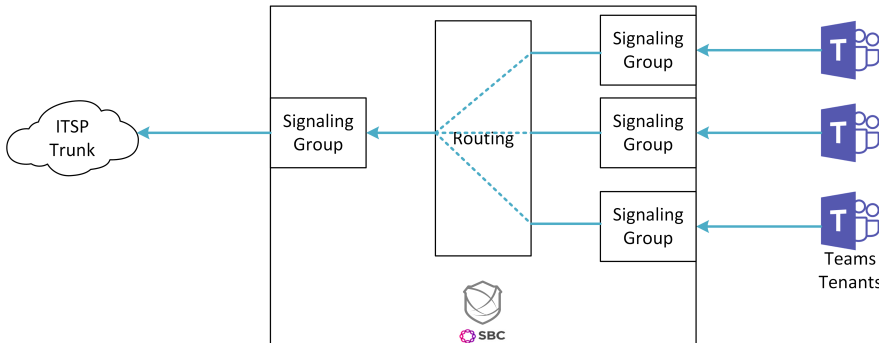
Multi-Tenant Direct Routing

ITSP to Teams segregation



Multi-Tenant Direct Routing

Teams segregation to ITSP



Step 1: Install SBC Edge (if required)

These instructions assume the SBC Edge product (SBC SWe Lite, SBC 1000/2000) is installed and running. If the product is not installed, refer to the links below.

Table 1: Installation Requirements

Product	Installation
SBC SWe Lite	On KVM: Installing SBC SWe Lite on KVM Hypervisor On VMware ESXi: Installing SBC SWe Lite on VMware ESXi On Hyper-V: Installing SBC SWe Lite on Microsoft Hyper-V
SBC 1000	Prepare for Installation Installing the SBC 1000 Hardware
SBC 2000	Prepare for Installation Installing the SBC 2000 Hardware

Step 2: Prerequisites



Microsoft Teams Direct Routing Configuration

Consult the Microsoft [documentation](#) for detailed information on Direct Routing interface configuration guidelines, including the RFC standards and the syntax of SIP messages.

SBC Edge Software

Ensure you are running the latest version of SBC software:

- To locate the SBC Edge software current running, refer to: [Viewing the Software Version and Hardware ID](#).
- To download and upgrade a new version of SBC Edge software, refer to: [Installing and Commissioning the SBC Edge and SBC SWe Lite](#).

Obtain IP Address and FQDN

Requirements for configuring the SBC Edge in support of Teams Direct Routing include:

Table 2: SBC Edge Requirements

Requirement	How it is Used
Public IP address of NAT device (must be Static) *	Required for SBC Behind the NAT deployment.
Private IP address of the SBC	
Public IP address of SBC	Required for SBC with Public IP deployment.
Public FQDN	The Public FQDN must point to the Public IP Address.

*NAT translates a public IP address to a Private IP address.

Domain Name

For the SBC Edge to pair with Microsoft Teams, the SBC FQDN domain name must match a name registered in both the **Domains** and **DomainUriMap** fields of the Tenant. Verify the correct domain name is configured for the Tenant as follows:

1. On the Microsoft Teams Tenant side, execute **Get-CsTenant**.
2. Review the output.
3. Verify that the Domain Name configured is listed in the **Domains** and **DomainUriMap** attributes for the Tenant. If the Domain Name is incorrect or missing, the SBC will not pair with Microsoft Teams.

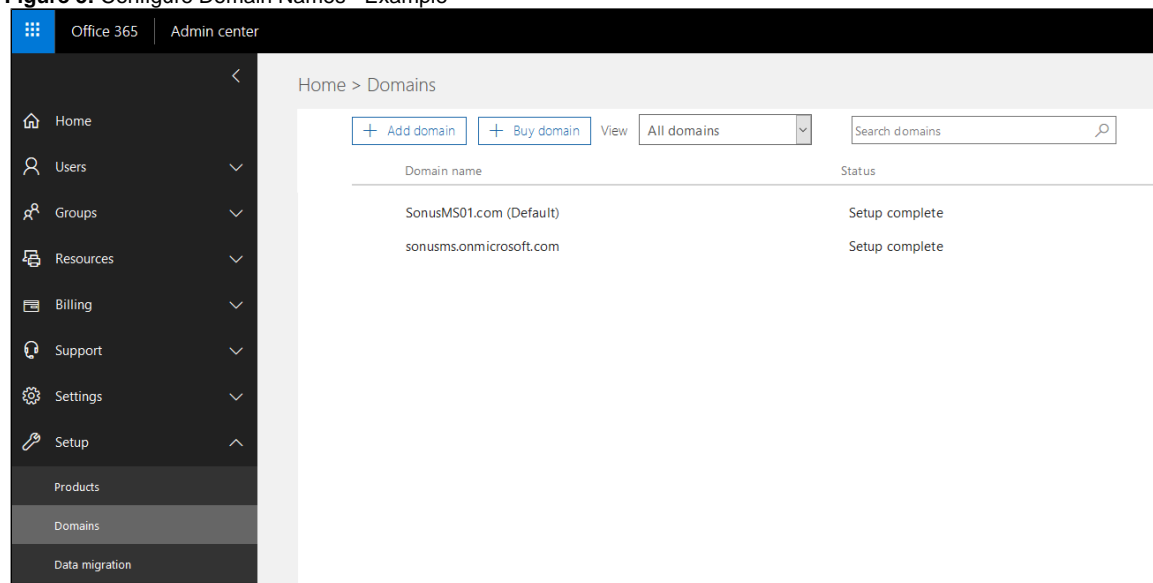
Users may be from any SIP domain registered for the tenant. For example, you can configure user **user@SonusMS01.com** with the SBC FQDN name **sbcs1.hybridvoice.org**, as long as both names are registered for the tenant.

Table 3: Domain Name Examples

Domain Name*	Use for SBC FQDN?	FQDN Names - Examples
SonusMS01.com	✓	Valid names: <ul style="list-style-type: none"> • aepsite6.SonusMS01.com
hybridvoice.org	✓	Valid names: <ul style="list-style-type: none"> • sbc1. hybridvoice.org • ussbcs15. hybridvoice.org • europe. hybridvoice.org Non-Valid name: <p>sbc1.europe.hybridvoice.org (requires registering domain name europe. hybridvoice.org in "Domains" first)</p>

*Do not use the *.onmicrosoft.com tenant for the domain name.

Figure 5: Configure Domain Names - Example



Obtain Certificate

Public Certificate

The Certificate must be issued by one of the supported certification authorities (CAs). Wildcard certificates are supported.

- Refer to [Microsoft documentation](#) for the supported CAs.
- Refer to [Domain Name](#) for certificate formats.

Configure and Generate Certificates on the SBC



Warning: Common Encryption Certificate Issues Arise from Missing Root Certificates

- Did you **only** install the CA-signed SBC certificate, along with the intermediate certificate(s) sent by your issuing CA?
- Did you get the following error message from the SBC?



If so, the likely reason is a **missing CA Root Certificate**. The SBC does not have any pre-installed CA root X.509 certificates, unlike typical browsers found on your PC. Ensure the entire certificate chain of trust is installed on the SBC, including the root certificate. Acquire the CA root certificate as follows:

1. Contact your system administrator or certificate vendor to acquire the root, and any further missing intermediate certificate (s) to provision the entire certificate chain of trust within the SBC;
2. Load the root certificate, along with the intermediate and SBC certificates, according to [Importing Trusted Root CA Certificates](#).

NOTE: Root certificates are easily acquired from the certificate authorities. For example, the root certificate for the **GoDaddy Class 2 Certification Authority** may be found at <https://ssl-cpp.godaddy.com/repository?origin=CALLISTO> . For more information about root certificates, intermediate certificates, and the SBC server ("leaf") certificates, refer to this [tutorial](#).

For other certificate-related errors, refer to [Common Troubleshooting Issues with Certificates in SBC Edge](#).

Microsoft Teams Direct Routing allows only TLS connections from the SBC for SIP traffic with a certificate signed by one of the trusted certification authorities.

Request a certificate for the SBC External interface and configure it based on the example using GlobalSign as follows:

- Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority.
- Import the Public CA Root/Intermediate Certificate on the SBC.
- Import the Microsoft CA Certificate on the SBC.
- Import the SBC Certificate.



The certificate is obtained through the Certificate Signing Request (instructions below). The Trusted Root and Intermediary Signing Certificates are obtained from your certification authority.

Step 1: Generate a Certificate Signing Request and obtain the certificate from a supported Certification Authority (CA)

Many CA's do not support a private key with a length of 1024 bits. Validate with your CA requirements and select the appropriate length of the key.

1. Access the WebUI.
2. Access **Settings > Security > SBC Certificates**.
3. Click **Generate SBC Edge CSR**.
4. Enter data in the required fields.
5. Click **OK**. After the Certificate Signing request finishes generating, copy the result to the clipboard.

Figure 6: Generate Certificate Signing Request

Generate Certificate Signing Request

Subject Distinguished Name

Common Name * Hostname or FQDN

Subject Alternative Name DNS comma-separated FQDN list

Email Address

ISO Country Code

State/Province

Locality e.g.: City

Organization e.g.: Company

Organizational Unit e.g.: Department

Key Length

Result

Copy CSR

```

-----BEGIN CERTIFICATE REQUEST-----
MIIDCTCAfECAQAwfDEfMB0GA1UEAxMWYVWVwc2l0ZTYuU29udXNNUzAxLmNvbTEi
MCAGCSqGSIb3DQEJARYTc21pdGhAU29udXNNUzAxLmNvbTElMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAK5KM0QwDAYDVQQKEwVtb251czELMAkGA1UECmMCSVQwggeiMA0
G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdCuUpCp6dbrXAAEO8mPCQ7Pbi6MX2U
YCsTahykvqLIZCuototW96pa7lwA41rdA3ZqiyxLjqEuV3aRYRk/3PKTZK6Ccv
g3fqnsIhn0KdvRBYjOIGHTj+7dx3gGgQh2PH9VYsHGkiMluqFw0Ib6afLeYiYk4A
XKdJLTes7YOlusGXHldg+itbaYVaxc5A2kUV0okR1LI1YsVJ3XgXllu5u4hZR
HGPVEMPcNxeQUmyC/86vNdp0bMLxg8smA+dYq2Mk43VQHDH3321DLjHwT+yVYR9o
rNCAALWgsxDzbdVkl3NaiEd3Yo/WM4Ad0wVvB9KC+CxVfWScvS2k3FAVAgMBAAAg
SDBGBgkqhkiG9w0BCQ4xOTA3MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMB0GA
1Ud
JQQuWMBGCCcGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAtwp
e
QHMXWTziiWAgHbY//WkV+CFV2fCxILPZWw6dNprhdG+Dv0EcYqGS4ZKPRViBN9h

```

6. Use the generated CSR text from the clipboard to obtain the certificate.

Step 2: Deploy the SBC and Root/Intermediate Certificates on the SBC

After receiving the certificates from the certification authority, install the SBC Certificate and Root/Intermediate Certificates as follows:

1. Obtain Trusted Root and Intermediary signing certificates from your certification authority.
2. Access the WebUI.
3. To install Trusted Root Certificates, click **Settings > Security > SBC Certificates > Trusted Root Certificates**.
4. Click **Import** and select the trusted root certificates.
5. To install the SBC certificate, open **Settings > Security > SBC Certificates > SBC Primary Certificate**.
6. Validate the certificate is installed correctly.

Figure 7: Validate Certificate

Trusted CA Certificate Table							
Total 3 Certificate Rows							
	Common Name	Issuer	Start Validity	Expiration	Key Length	Display	Primary Key
▶	GlobalSign Root CA	GlobalSign Root CA	Sep 1, 1998	Jan 28, 2028	2048		2
▶	GlobalSign Domain Va...	GlobalSign Root CA	Feb 20, 2014	Feb 20, 2024	2048		3
▶	Baltimore CyberTrust...	Baltimore CyberTrust...	May 12, 2000	May 12, 2025	2048		4

7. Click **Import** and select **X.509 Signed Certificate**.
8. Validate the certificate is installed correctly.

Figure 8: Validate Certificate

SBC Primary Certificate

Import | Export

October 20, 2019 17:40:37

Subject

Common Name

ISO Country Code

State or Province

Locality

Organization

Organizational Unit

Email Address

Certificate

Not Valid Before

Not Valid After

Serial Number

Signature Algorithm

Key Length

Enhanced Key Usage

Key Usage

Subject Alternative Name

Verify Status

Oct 14, 2019 08:38:58

Oct 13, 2021 08:38:58

sha1WithRSAEncryption

2048

TLS Web Server Authentication

Digital Signature, Key Encipherment

None

OK

Issuer

Common Name

ISO Country Code

State or Province

Locality

Organization

Organizational Unit

Email Address

interopdomain-AD-CA

Firewall Rules

Ribbon recommends the deployment of the SBC Edge product behind a firewall, within the DMZ, regardless of the assignment of a public IP to the SBC in question. Refer to [SBC Edge Security Hardening Checklist](#) for more information about the SBC and firewalls.

This section lists the ports, protocols and services for firewalls that are in the path of the SBC connecting to Teams Direct Routing.

Basic Firewall Rules for All Call Flows

Inbound Public (Internet to SBC)

- SIP TLS: TCP 5061*
- Media for SBC 1000: UDP 16384-17584**
- Media for SBC 2000: UDP 16384-19384*
- Media for SBC SWe Lite: UDP 16384-21384

Outbound Public (SBC to Internet)

- DNS: TCP 53
- DNS: UDP 53
- NTP: UDP 123
- SIP TLS: TCP 5061
- Media: UDP 49152-53247

Public Access Information

The tables below represent [ACL](#) (Access Control List) examples that protect the SBC Edge. When using Easy Configuration Teams related wizards in an Enterprise deployment, these attributes are automatically provisioned. If you are manually configuring the SBC Edge as part of a Microsoft Teams Direct Routing migration scenario (for example Skype for Business or CCE), you must manually configure these ports. For details on ACLs, refer to [Creating and Modifying Rules for IPv6 Access Control Lists](#).

Table 4: Public Access In - Requirements

Description	Protocol	Action	Src IP Address	Src Port	Dest IP Address	Dest Port
Outbound DNS Reply	TCP	Allow	0.0.0.0/0	53	SBC/32	0-65535
Outbound DNS Reply	UDP	Allow	0.0.0.0/0	53	SBC/32	0-65535
Outbound NTP Reply	UDP	Allow	0.0.0.0/0	123	SBC/32	123
Outbound SIP Reply	TCP	Allow	0.0.0.0/0	5061	SBC/32	1024-65535
Inbound SIP Request	TCP	Allow	0.0.0.0/0	1024-65535	SBC/32	5061*
Inbound Media Helper	UDP	Allow	52.112.0.0/14	49152-53247	SBC/32	16384-17584**
Deny All	Any	Deny	0.0.0.0/0		0.0.0.0/0	

Table 5: Public Access Out - Requirements

Description	Protocol	Action	Src IP Address	Src Port	Dest IP Address	Dest Port
Outbound DNS Request	TCP	Allow	SBC/32	0-65535	0.0.0.0/0	53
Outbound DNS Request	UDP	Allow	SBC/32	0-65535	0.0.0.0/0	53
Outbound NTP Request	UDP	Allow	SBC/32	0-65535	0.0.0.0/0	123
Outbound SIP Request	TCP	Allow	SBC/32	0-65535	0.0.0.0/0	5061
Inbound SIP Reply	TCP	Allow	SBC/32	5061*	0.0.0.0/0	1024-65535
Outbound Media Helper	UDP	Allow	SBC/32	16384-17584**	52.112.0.0/14	49152-53247
Deny All	Any	Deny	0.0.0.0/0		0.0.0.0/0	

* Define in Tenant configuration

** SBC SWe Lite does not require this rule to be created since Media ports are opened as needed. This rule is required only for SBC 1000, SBC 2000 and then depends of the Media Port paired configured in the SBC.

Firewall Rules for the SBC with Media Bypass

Apply the following firewall rules below:



The Teams Client IP address cannot be predicted. As a result, allow Any IP (0.0.0.0/0).

Inbound Public (Internet to SBC)

Media for SBC 1000: UDP 17586-21186**

Media for SBC 2000: UDP 19386-28386**

Outbound Public (SBC to Internet)

Media: UDP 50000-50019

If the device that handles the NAT between the Teams Client and SBC Public IP is performing PAT (Port Address Translation), verify that this device has the source port range of the Teams Client media or open all the ports from 1024 to 65535.

For SBC behind NAT, the firewall should allow access between the firewall IP and the NAT device's IP.

For SBC not using NAT, there must be access between the firewall and the SBC's Public IP.

Public Access

The tables below represent [ACL](#) (Access Control List) examples that protect the SBC Edge; these ACL attributes are automatically provisioned if the Teams-related [Easy Configuration](#) wizards are used (applies to the greenfield deployment scenario only).

Table 6: Public Access In - Requirements (Media Bypass Scenario)

Description	Protocol	Action	Src IP Address	Src Port	Dest IP Address	Dest Port
Inbound Media Bypass Helper	UDP	Allow	0.0.0.0/0	1024-65535	SBC/32	16384-21186**

Table 7: Public Access Out - Requirements (Media Bypass Scenario)

Description	Protocol	Action	Src IP Address	Src Port	Dest IP Address	Dest Port
Outbound Media Bypass Helper	UDP	Allow	SBC/32	16384-21186**	0.0.0.0/0	1024-65535

* Define in Tenant configuration

** SBC SWe Lite does not require this rule to be created since Media ports are opened as needed. This rule is required only for SBC 1000, SBC 2000 and then depends of the Media Port paired configured in the SBC.

Wildcard Certificate

Microsoft Teams Direct Routing in support of multiple Tenants requires wildcard certificate support to protect the Microsoft partner's SBC FQDN and Tenant's SBC FQDN (that is, SAN=myMicrosoftPartner.com, SAN=*.myMicrosoftPartner.com). The SBC Edge products fully support wildcard certificates.

SBC Edge Configuration for Microsoft Teams Direct Routing



These instructions assume the SBC Edge has been configured for Microsoft Teams Direct Routing through the Easy Configuration wizard. For details on Easy Configuration, refer to: [Working with SBC Easy Configuration](#).

- **For SBC Edge Not configured for Microsoft Teams Routing:** If the SBC Edge has not been configured for Microsoft Teams Direct Routing through the Easy Configuration Wizard, configure the SBC Edge per [Connect SBC Edge to Microsoft Teams Direct Routing](#). Once complete, move to Step 3 below.

OR

- **For SBC Edge Previously Configured for Microsoft Teams Direct Routing:** Move to Step 3.

Step 3: Configure each Tenant

The SBC Easy Configuration wizard configures the SBC Edge for one Tenant; additional Tenants subscribed to Microsoft Office 365 services (Microsoft Teams Direct Routing) must be configured manually with the configuration items below. For documentation purposes, the following terms are used in the configuration examples.

Table 8: Configuration Used in This Document

Configuration	Example used in this document
SBC FQDN for Microsoft partner	myMicrosoftPartner.com
SBC FQDN for Tenant	tenant2.myMicrosoftPartner.com
Microsoft description	Microsoft Phone System

Tenant Name	Microsoft Phone System Tenant 2
-------------	---------------------------------

Access the WebUI

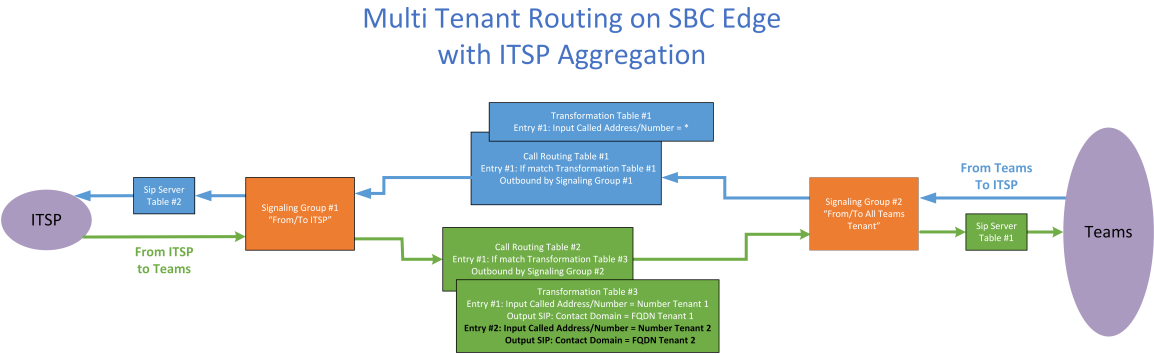
You must access the SBC Edge's WebUI to configure the items below. To access the WebUI, refer to: [Logging into the SBC Edge](#).

Topology 1 - Configure the SBC for ITSP Aggregation for all Teams Tenants

To implement ITSP Aggregation, the SBC configuration must contain the following:

- Call traffic from the ITSP to Microsoft Teams uses a single SIP Signaling Group to Teams Direct Routing. The destination Tenant is included in the Transformation table; each Microsoft Teams Tenant requires a dedicated Transformation Entry that matches the Microsoft Online PSTN Gateway created on the Microsoft Teams Tenant.
- Call traffic from Microsoft Teams to ITSP uses the default call route to the ITSP.

Figure 9: Multi Tenant Routing on SBC Edge with ITSP Aggregation



Create a Transformation entry for the call from ITSP to the new Tenant

In the SBC, configure a Transformation table entry for Teams Direct Routing (Entry #2 on previous diagram). This entry will match the input of the new end customer number and configure the proper Teams Tenant output.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation page, access **Call Routing > Transformation**.
3. Select the **Transformation Table** called **From Microsoft Teams: Passthrough** (the entry created in the Easy Configuration Wizard).
4. Click the (+) icon.
5. Configure the parameters as shown below. Leave all other parameters as default.
6. Click **OK**.

Table 9: Transformation Entry Tenant 2 Configuration - Example

Parameter	Example Value
Description	To Microsoft Phone System Tenant 2 (example name)
Match Type	Optional
Input Type	Called Address/Number
Input Value	<Enter Tenant 2 Phone Number > (\+151048512\d{2})
Output Type	SIP: Contact Domain
Output Value	tenant2.myMicrosoftPartner.com

Figure 10: Transformaton Entry Tenant 2 - Example

Create Transformation Table Entry

Row ID 2

Description

Admin State

Match Type

Input Field

Type

Value

Output Field

Type

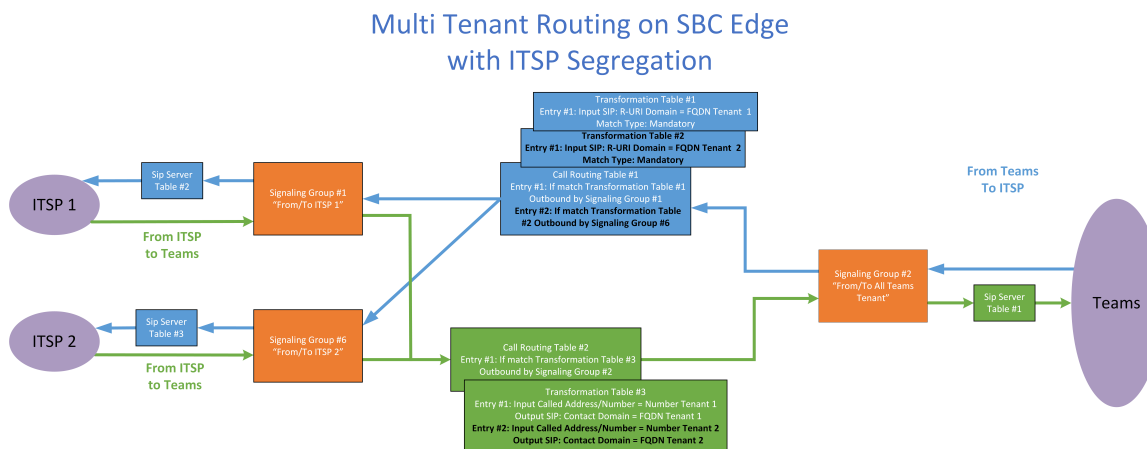
Value

Topology 2 - Configure the SBC for ITSP Segregation per Teams Tenant

To implement ITSP Segregation, the SBC configuration must contain the following:

- Call traffic from the ITSP to Microsoft Teams uses the single SIP Signaling Group to Teams Direct Routing. The destination Tenant is used in the Transformation table. Each Microsoft Teams Tenant requires a dedicated Transformation Entry that matches the Microsoft Online PSTN Gateway created on the Microsoft Teams Tenant.
- Call traffic from Microsoft Teams to the SBC Edge is aggregated onto the single SIP Signaling Group for all Tenants. The Call Routing Table associated with this SIP Signaling Group is configured to distribute the traffic to a specific ITSP, based on the original tenant (SIP: R-URI Domain).

Figure 11: Multi Tenant Routing on SBC Edge with ITSP Segregation



i The instructions below require that you have created the SIP Signaling Group, SIP Server Table, Call Routing Table, and Transformation Table for the new ITSP. For details, refer to the following:

- [Creating and Modifying SIP Signaling Groups](#)
- [Creating and Modifying Entries in SIP Server Tables](#)
- [Creating and Modifying Entries to Call Routing Tables](#)
- [Creating and Modifying Entries to Transformation Tables](#)

Create a Transformation entry for the call from ITSP to the new Tenant

- 1. In the WebUI, click the **Settings** tab.
- 2. In the left navigation page, access **Call Routing > Transformation**.
- 3. Click on the **Transformation Table > From SIP Trunk 2: Passthrough** (the entry created when you added your ITSP 2 configuration).
- 4. Click the (+) icon.
- 5. Configure the parameters as shown below. Leave all other parameters as default.
- 6. Click **OK**.

Table 10: Transformation Entry Tenant 2 Configuration - Example

Parameter	Example Value
Description	From ITSP 2 To Microsoft Phone System Tenant 2 (example name)
Match Type	Optional
Input Type	Called Address/Number
Input Value	(.*)
Output Type	SIP: Contact Domain
Output Value	tenant2.myMicrosoftPartner.com

Figure 12: Transformation Entry Tenant 2 - Example

Create Transformation Table Entry

Row ID1

DescriptionFrom ITSP 2 To Microsoft Phone System Tenant 2

Admin StateEnabled

Match TypeOptional (Match One)

Input Field

TypeCalled Address/Number

Value(.*)

Output Field

TypeSIP: Contact Domain

Valuetenant2.myMicrosoftPartner.com

Create a New Transformation Table for the call from the new Tenant to ITSP 2

- 1. In the WebUI, click the **Settings** tab.
- 2. In the left navigation page, access **Call Routing > Transformation**.
- 3. Click the (+) icon at the top left corner to add a new Transformation Table.
- 4. Configure the parameters as shown below and click **OK**. For details on parameter definitions, refer to [Creating and Modifying Transformation Tables](#).

Table 11: Transformation Table - Example Values

--	--

Parameter	Example Value
Row ID	Assigned by the system
Description	From Microsoft Phone System Tenant 2 To ITSP 2

Figure 13: Create Transformation Table

Create Transformation Table

Row ID 5

Description From Microsoft Phone System Tenant 2 To ITSP 2

- From the left navigation pane, click on the **Transformation > From Microsoft Phone System Tenant 2 To ITSP 2** (the entry created in the last step).
- Click the (+) icon.
- Configure the parameters as shown below. Leave all other parameters as default.
- Click **OK**.

Table 12: Transformation Entry Tenant 1 Configuration - Example

Parameter	Example Value
Description	To ITSP 2 (example name)
Match Type	Mandatory
Input Type	SIP: R-URI Domain
Input Value	(tenant2.myMicrosoftPartner.com):5061
Output Type	SIP: R-URI Domain
Output Value	\1

Figure 14: Transformation Entry Tenant 2 - Example

Create Transformation Table Entry

Row ID 1

Description To ITSP 2

Admin State Enabled

Match Type Mandatory (Must Match)

Input Field

Type SIP: R-URI Domain

Value (tenant2.myMicrosoftPartner.com):5061

Output Field

Type SIP: R-URI Domain

Value \1

Add New Routing Table Entry for the Call from the new Tenant to ITSP 2

The Easy Configuration process (used for initial configuration) creates the first connection to Teams Direct Routing. This configuration also creates two Call Routing Tables for transporting calls between the SBC's SIP Trunk and Microsoft Teams:

From SIP Trunk. Calls from SIP Trunk to Teams.

From Microsoft Team. Calls from Teams to SIP Trunk.

For calls to be routed from an individual Tenant to the proper ITSP, an entry must be added to the **From Microsoft Teams** Routing table (this Routing Table was created as part of Easy Configuration) for each Tenant. Add an entry in the **From Microsoft Teams** Call Routing table for each Tenant as follows:


- 1. In the WebUI, click the **Settings** tab.
- 2. From the left navigation pane, click on the **Call Routing table**. Click on the **From Microsoft Teams** Call Routing Table.
- 3. Click the  icon to add an entry.
- 4. Configure the parameters as shown below. Leave all other parameters as default. For details on parameter definitions, refer to [Creating and Modifying Entries to Call Routing Tables](#).
- 5. Click **OK**.

Table 13: Call Routing Entry - Example Values

Parameter	Example Value
Description	To ITSP 2
Number/Name Transformation Table	From Microsoft Phone System Tenant 2 To ITSP 2
Destination Signaling Groups	ITSP 2 (from the previous steps)

Figure 15: Create Call Routing Entry - Example

Create Call Routing Entry

Route Details

Row ID2

DescriptionTo ITSP 2

Admin StateEnabled

Route Priority1

Call PriorityNormal

Number/Name Transformation TableFrom Microsoft Phone System Te

Time of Day RestrictionNone

Destination Information

Destination TypeNormal

Message Translation TableNone

Cause Code ReroutesNone

Cancel Others upon ForwardingDisabled

Fork CallNot Licensed

Destination Signaling Groups

(SIP) Demo: Border Element 2

Up

Down

Add/Edit

Remove

Enable Maximum Call DurationDisabled

Step 4: Confirm SBC Edge Links to Microsoft Teams

1. Access the WebUI. Refer to [Logging into the SBC Edge](#).
2. Click **Monitor**.
3. Under each newly created Signaling Group (created for each Tenant), confirm the channels are green. For details on channel status, refer to [Monitoring Real Time Status](#).

For troubleshooting steps, refer to [Best Practice - Troubleshoot Issues with Microsoft Teams Direct Routing](#).

Step 5: Place a Test Call

Place a test call as follows:

- 1. Access the WebUI. Refer to [Logging into the SBC Edge](#).
- 2. In the WebUI, click the **Diagnostics** tab.
- 3. In the left navigation pane, click **Test a Call**.
- 4. Configure the parameters as shown below.
- 5. Click **OK**.

Table 14: Place a Test Call - Parameters

Parameter	Value
Destination Number	Number assigned to a Teams user.
Origination/Calling Number	Number assigned to a Local user.
Call Routing Table	The routing table that handles the call from Microsoft Teams.

Figure 16: Test a Call - Configuration

Test a Call

Destination Number

+15101061005

* +15105551234

Origination/Calling Number

+15101011001

+15105554321

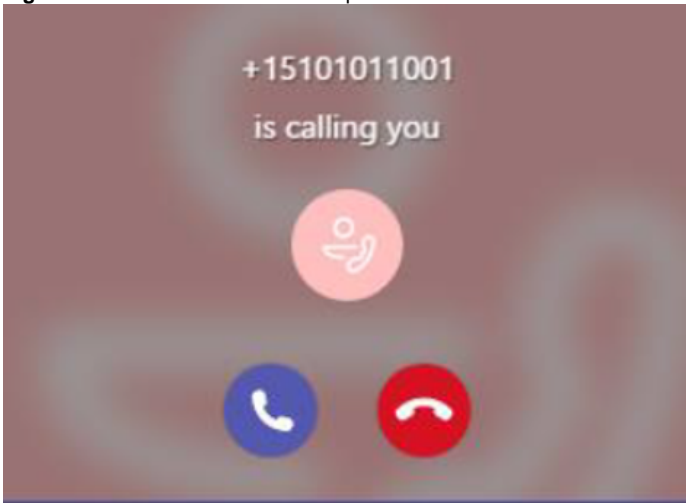
Call Routing Table

From Microsoft Teams

*

OK

Figure 17: Place a Test Call - Example



The test call is now complete. For troubleshooting steps, refer to [Best Practice - Troubleshoot Issues with Microsoft Teams Direct Routing](#).

