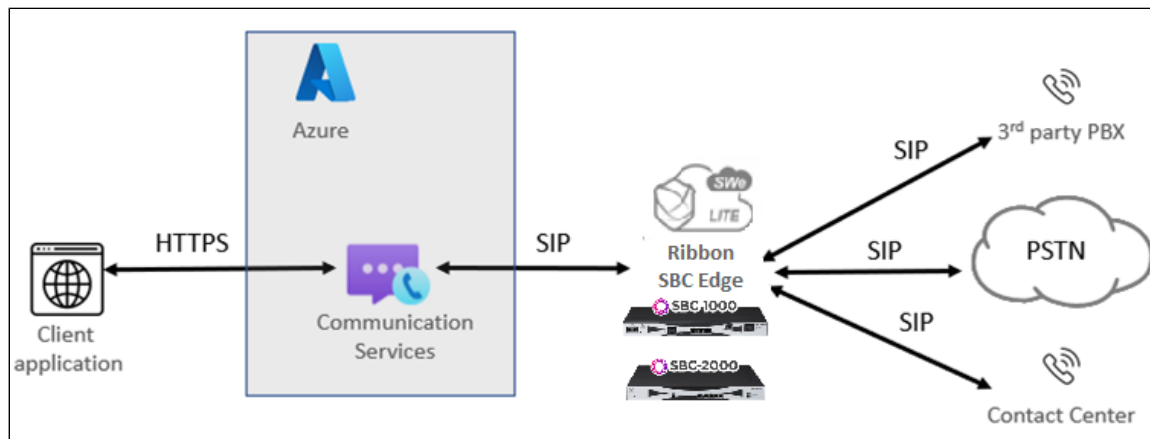


# Best Practice - Configure SBC Edge for Azure Communication Services Direct Routing

- [Overview](#)
- [Prerequisites](#)
- [Step 1: Install SBC Edge](#)
- [Step 2: Configure Azure Communication Service Configuration on the Azure Portal](#)
- [Step 3: Configure SBC Edge for ACS Direct Routing](#)
  - [Obtain Certificate](#)
  - [Configure SBC Edge for ACS Direct Routing via Easy Configuration Wizard](#)
- [Step 4: Verify SBC Pairing with ACS Direct Routing](#)
- [References](#)

## Overview

Azure Communication Services are cloud-based services with REST APIs and client library SDKs available to help the user integrate communication into your applications.



For more details related to ACS, visit: <https://docs.microsoft.com/en-us/azure/communication-services/>

ACS will use Microsoft Direct Routing Signaling Framework for the telephony services with configured SBCs. Prior Direct Routing knowledge is helpful for the understanding of call flows.



### Note

The Ribbon SBC Edge was tested with ACS direct routing along with web calling sdk client "version :4.46.0".

## Prerequisites

The following prerequisites apply to the configuration:

- The FQDN should not be registered onto the Office 365 network.
- The TLS certificate should be occupied by Microsoft verified CA which will be used for pairing of the SBC to ACS direct routing.

Ensure you are running version at least 9.0.3 of the 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.](#)
- To install SBC Edge, refer to [Install SBC Edge.](#)

## Step 1: Install SBC Edge

These instructions assume the SBC Edge is installed and running. If the product is not installed, refer to the links below.

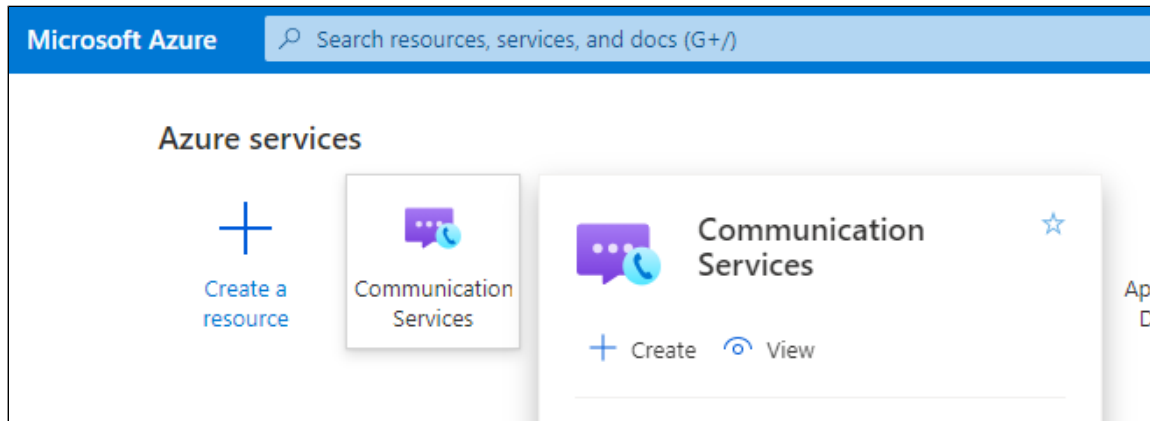
**Table 1:** Installation Requirements

Product	Installation
SBC SWe Lite	<p><b>On KVM:</b> <a href="#">Installing SBC SWe Lite on KVM Hypervisor</a></p> <p><b>On VMware ESXi:</b> <a href="#">Installing SBC SWe Lite on VMware ESXi</a></p> <p><b>On Hyper-V:</b> <a href="#">Installing SBC SWe Lite on Microsoft Hyper-V</a></p> <p><b>On Azure:</b> <a href="#">Deploying an SBC SWe Lite with Quick Launch for Azure</a></p>
SBC 1000	<p><a href="#">Prepare for Installation</a></p> <p><a href="#">Installing the SBC 1000 Hardware</a></p>
SBC 2000	<p><a href="#">Prepare for Installation</a></p> <p><a href="#">Installing the SBC 2000 Hardware</a></p>

## Step 2: Configure Azure Communication Service Configuration on the Azure Portal

To register a Session Border Controller with Azure Communication Service:

1. Login to the Azure portal at [portal.azure.com](https://portal.azure.com)
2. Search for **Communication Services** and then click **Create** as shown below.



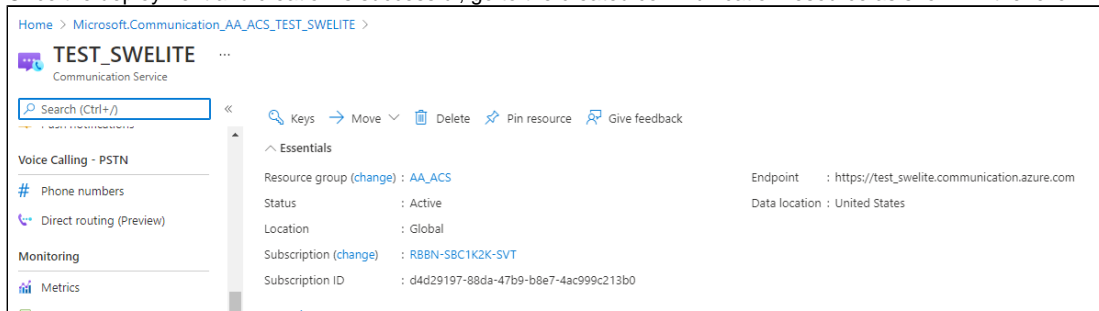
3. Use the required active subscription and resource group, give a resource name, and click **Review+Create**.

The screenshot shows the "Create resource" form for Communication Service. The form is titled "Create resource" and has tabs for "Basics", "Tags", and "Review". The "Basics" tab is selected. The form includes the following fields:

- Project Details:**
  - Subscription \*: RBBN-SBC1K2K-SVT
  - Resource group \*: AA\_ACS
- Instance Details:**
  - Resource Name \*: TEST\_SWELITE
  - Data location ⓘ: United States

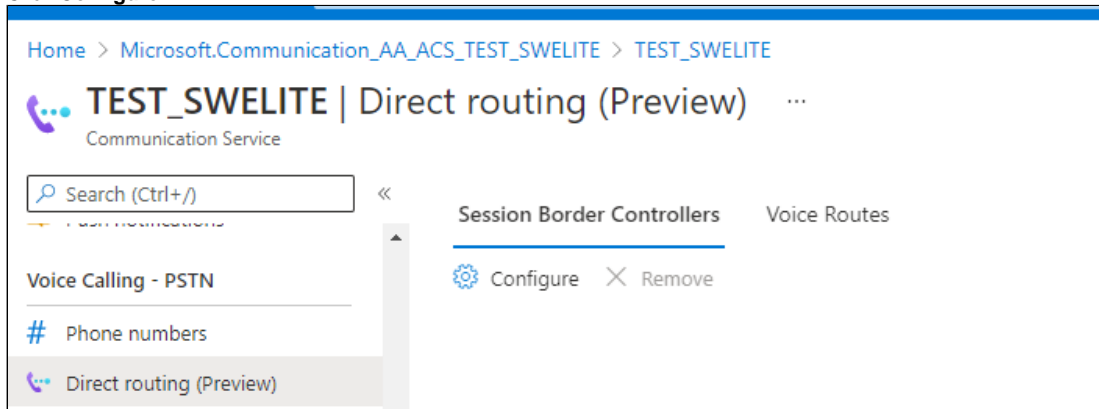
At the bottom of the form, there are three buttons: "Review + Create" (highlighted in blue), "Previous", and "Next: Tags".

4. Once the deployment and creation is successful, go to the created communication resource as shown in the following image.

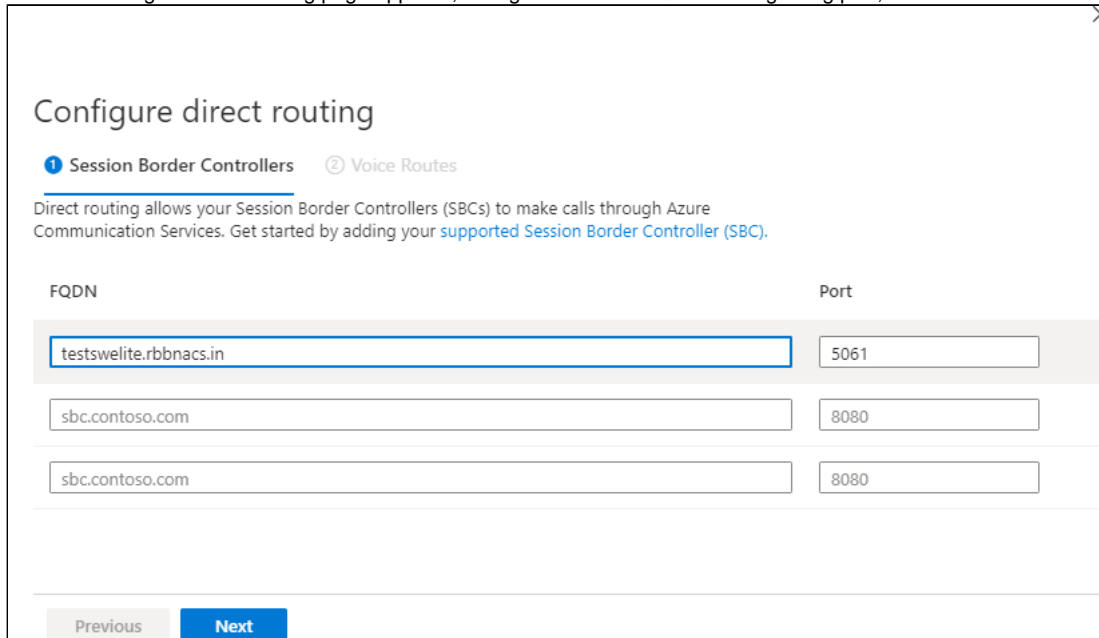


5. Click the **Direct Routing** option to pair the SBC with Azure Communication Service.

6. Click **Configure**.



7. Once the configure direct routing page appears, configure the SBC FQDN and signaling port, and click **Next**.



8. Enter the Voice Route Name and Number pattern to be used for landing the call onto the SBC and select the created SBC from the dropdown.

9. Click **Save**.

**Configure direct routing**

✓ Session Border Controllers    2 Voice Routes

Azure Communication Services allows balancing and routing outgoing calls based on called number. Set voice routes to complete your direct routing configuration.

Voice Route Name	Number pattern	Session Border Controller(s)
swelite	^\+1(777000)(\d{4})\$	testswelite.rbbnacs.in

---

**Session Border Controllers**    Voice Routes

⚙️ Configure    ✕ Remove

FQDN	Port
testswelite.rbbnacs.in	5061

---

**Session Border Controllers**    Voice Routes

⚙️ Configure    ✕ Remove

<input type="checkbox"/>	Voice Route Name	Number pattern	Session Border Controller(s)
<input type="checkbox"/>	swelite	^\+1(777000)(\d{4})\$	testswelite.rbbnacs.in

The above images are example results of successful ACS direct routing configuration.

## Step 3: Configure SBC Edge for ACS Direct Routing

**Note**  
Only outbound calls from the ACS client to the SBC are currently supported.

### 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 certificate information.
- Refer to [CCADB Documentation](#) for the comprehensive list of supported CAs.
- See [Domain Name](#) for certificate formats.

### Configure and Generate Certificates on the SBC

ACS 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 1:** 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-----
MIIDCTCCAFCAQAwfDEFMB0GA1UEAxMWYyVWwvc2I0ZTYuU29udXNNUzAxLmNvbTEi
MCAGCSqGSIb3DQEJARYTc21pdGhAU29udXNNUzAxLmNvbTElMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAk5KMzQ4wDAYDzYwQKEwVTb251czELMAkGA1UECmMCSVQwgwEiMA0
G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdcuUpCp6dbrXAAEO8mPCQ7Pbi6MX2U
YCsTahykvqmLiZCuototW96pa7lwA41rdA3ZqiyxLjqEuV3aRYRk/3PKTZK6Ccv
g3fqnsIhn0KdvRBVjOIGHtj+7dx3gGgQh2PH9VYsHGkiMluqFw0Ib6afLeYiYk4A
XKdJLTesx7Y0IuSGXHldg+itxaYVvaxc5A2kUV0okR1LI1YsVJ3XgXllu5u4hZR
HGPVEMPCnXeQUmyC/86vNdp0bMLxg8smA+dYq2Mk43VQHDH321DLjHwT+yVYR9o
rNCAALWgsDzbdVkl3NaiEd3Yo/WM4Ad0wVvB9KC+CxVfWScvS2k3FAVAgMBAAAg
SDBGBgkqhkiG9w0BCQ4xOTA3MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMB0GA
1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAtwp
e
QHMXWTziiWAgHbY//WkV+CFV2fCxiLPZWW6dNprhdG+Dv0EcYqeGS4ZKPRViBN9h
-----END CERTIFICATE REQUEST-----
```

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 2:** Validate Certificate

Trusted CA Certificate Table							April 17, 2018 11:49:50
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 3:** Validate Certificate

**SBC Primary Certificate** | Import | Export | October 20, 2019 17:40:37

**Subject**

Common Name: [redacted]

ISO Country Code: US

State or Province:

Locality:

Organization:

Organizational Unit:

Email Address:

**Issuer**

Common Name: interopdomain-AD-CA

ISO Country Code:

State or Province:

Locality:

Organization:

Organizational Unit:

Email Address:

**Certificate**

Not Valid Before: Oct 14, 2019 08:38:58

Not Valid After: Oct 13, 2021 08:38:58

Serial Number: [redacted]

Signature Algorithm: sha1WithRSAEncryption

Key Length: 2048

Enhanced Key Usage: TLS Web Server Authentication

Key Usage: Digital Signature, Key Encipherment

Subject Alternative Name: None

Verify Status: **OK**

9. To install the Baltimore CyberTrust Root Certificate, click **Settings > Security > SBC Certificates > Trusted Root Certificates**.
10. Click **Import** and select **Baltimore CyberTrust Root Certificate**.
11. Validate the certificate is installed correctly.

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

## Configure SBC Edge for ACS Direct Routing via Easy Configuration Wizard

The SBC Edge is configured via the Easy Configuration Wizard.

1. Access the WebUI. Refer to [Logging into the SBC Edge](#).

2. Click on the **Tasks** tab.
3. From the left side menu, click **SBC Easy Setup > Easy Config Wizard**.
4. From the Application drop down box, select the **SIP Trunk Microsoft Teams Easy Configuration Wizard**. Depending on your network, follow a relevant Easy Configuration wizard. Refer to the table below for guidance.

Deployment Type	Refer to Configuration:
SBC Connects to Microsoft Teams via SIP Trunk	<a href="#">SIP Trunk Microsoft Teams</a>

5. On the signaling group, under RTCP Multiplexing, select **Disable**.
6. On the signaling group, under ICE Support, select **Disabled**.

## Step 4: Verify SBC Pairing with ACS Direct Routing

---

1. Access the WebUI. Refer to [Logging into the SBC Edge](#).
2. In the WebUI, 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](#).

Once SBC is paired successfully with ACS direct routing, you can begin making calls from the ACS client. Currently, only outbound calls are supported.

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

## References

---

- **ACS** – For a list of Ribbon SBC products supported for ACS, refer to the following page on Microsoft's website: <https://docs.microsoft.com/en-us/azure/communication-services/concepts/telephony-sms/certified-session-border-controllers>.
- **Ribbon** – For more information, refer to: <https://ribboncommunications.com/solutions/enterprise-solutions/microsoft-solutions>.