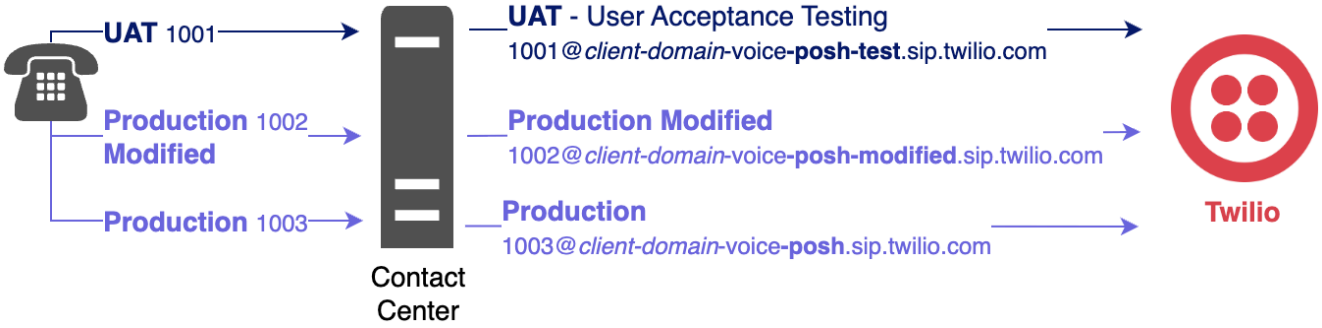
Posh Voice SIP Configuration

Document version: 7.1

Overview

This document provides networking and SIP configuration information for establishing SIP trunks between your Session Border Controller (SBC) and Posh's telephony provider, Twilio, for connectivity to Posh Voice.



Three Concurrent Environments

Your Posh Voice **UAT** (User Acceptance Testing) and **Production Modified** environments allow you to test changes and new features before they are rolled out to your **Production** environment. That is true during the implementation project *and after*. **That means you'll want separate phone numbers to reach UAT, Production Modified, and Production, and to keep those numbers available after the project is complete.**

Network Topology and Failover

Posh Voice uses Twilio as its telephony provider. You'll be creating SIP trunks to Twilio which interacts with Posh Voice.

Twilio has two points of ingress: **Ashburn VA** and **Umatilla OR**. You are free to choose which Twilio site is your primary and which is your secondary, but we encourage you to consider geographic

proximity. You may choose to configure each of your SBCs differently, with one using Ashburn VA as its primary and the other using Umatilla OR as its primary.

Configure each SBC to automatically send calls to its secondary Twilio site if its primary Twilio site is not reachable. **For this Twilio site failover to work, you must configure it in your SBC.** Requests to one Twilio site will *not* be automatically redirected to the other site by the network or Twilio. Your SBC must be configured to send calls to its secondary Twilio site if calls to its primary Twilio site fail.

Firewall Configuration

Configure your firewall or router access control list (ACL) to allow both **egress and ingress** to/from the following IP addresses and ports.

SIP Signaling connections using TCP/5061 (and optionally TCP/5060 for testing) will be created outbound from your SBC to Twilio, but **they will also be created inbound from Twilio to your SBC:**

- The firewall must allow these inbound connections
- If the firewall is NATing, there must be an Internet IP address reserved for your SBC so, when traffic is received on that IP address, the firewall knows to always send it to your SBC

The **RTP Media** IP address and port ranges are for the flow of audio. They are UDP and, therefore, are connectionless. But audio will be flowing in both directions, so those IP addresses and ports **need to be allowed outbound and inbound as well**.

SIP Signaling

Ashburn VA

54.172.60.0
54.172.60.1
54.172.60.2
54.172.60.3

Umatilla OR

54.244.51.0
54.244.51.1
54.244.51.2
54.244.51.3

Ports:

- TCP/5060 (in case we need to test with unencrypted calls)
- TCP/5061

Applications (if you are using an application firewall):

- SIP
- TLS (Palo Alto firewalls call it SSL)

RTP Media/Audio

168.86.128.0/18

Port range: UDP/10,000 to 60,000
Application: RTP

Twilio security FAQ: https://www.twilio.com/docs/voice/voice-media-ip-expansion-security-faq

Encryption, Trust, and Certificates

SIP signaling and RTP media are encrypted. To facilitate the encryption, a TLS connection is established between your SBC and Twilio.

To enable TLS, your SBC will require that an identity certificate be installed. That certificate can be issued by any Certificate Authority (CA) – public or private/internal. It can even be self-signed by the SBC itself. And **Twilio automatically trusts your SBC**, meaning they do *not* validate the CA that signed your SBC's identity certificate, so you do *not* need to provide Twilio a CA certificate or anything else.

For your SBC to trust Twilio, it must trust the certificate authorities that issued Twilio's identity certificates:

- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3

To do that, download and install one of these options in your SBC's trusted root CA store:

- Twilio's Root CA Bundle
- DigiCert Global Root Certificates

See below for more information.

Twilio's Root CA Bundle

https://www.twilio.com/docs/documents/586/ca-bundle-sip.crt

DigiCert Global Root Certificates

Instead of a bundle, you can download and install each **DigiCert Global Root** certificate separately.

- DigiCert Global Root CA: https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem
- DigiCert Global Root G2: https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem
- DigiCert Global Root G3: https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem

Support

Twilio supports TLS version 1.2.

Sending SRTP (encrypted media) to Twilio
Twilio supports the following crypto suites:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Receiving SRTP from Twilio
Only a single crypto suite is advertised:

- AES_CM_128_HMAC_SHA1_80

The optional master key identifier (MKI) parameter is *not* supported.

Media Codec

Twilio supports the G.711 μ-law (PCMU) and A-law (PCMA) codecs for media.

DTMF

Twilio supports RFC 2833 (RTP Payload for DTMF Digits).

Twilio also supports in-band DTMF. But in-band DTMF is not as reliable and, therefore, is not recommended.

Bandwidth Requirements

The G.711 μ-law (PCMU) and A-law (PCMA) codecs code voice at 64 Kbps. Add the required packet overhead and putting those codecs on the network requires 87.2 Kbps. (Reference: Introduction to Codecs [Cisco Unified Border Element] - Cisco)

Bandwidth	Concurrent Calls
1 Mbps	11
10 Mbps	114
100 Mbps	1,146

Or, put more conservatively and simply, 100 Kbps per call:

Bandwidth	Concurrent Calls
1 Mbps	10
10 Mbps	100
100 Mbps	1,000

The bandwidth quoted is **symmetrical**. For example, a 10 Mbps connection would need 10 Mbps upload and 10 Mbps download because a call consists of two G.711 audio streams, one in each direction.

Session Border Controller Licensing

Session Border Controllers (SBCs) are typically licensed by **SIP trunk** and/or **concurrent SIP sessions** (calls). You need licensing for:

- Three SIP trunks:
    - UAT (User Acceptance Testing)

    - Production Modified
    - Production
- Enough SIP sessions to support your maximum concurrent call volume

If you have **two SBCs**, Posh recommends that each SBC be licensed to carry a full load of **production** calls in case the other SBC is unavailable.

Example:

> Anticipated maximum concurrent production call volume: 200

SBC #1	**SBC #2**
Posh Voice **Production** SIP trunk 200 SIP sessions	Posh Voice **Production** SIP trunk 200 SIP sessions
Posh Voice **Production Modified** 10 SIP sessions, enough for testing	Posh Voice **Production Modified** (optional) 10 SIP sessions, enough for testing (optional)
Posh Voice **UAT** SIP trunk 10 SIP sessions, enough for testing	Posh Voice **UAT** SIP trunk (optional) 10 SIP sessions, enough for testing (optional)

posh

DNS FQDN / SIP Domain

Configure your SBC to send calls to the following DNS FQDNs based on which Posh Voice environment you want to reach at which Twilio site:

UAT (User Acceptance Testing)
Ashburn VA: *client-domain*-voice**-posh-test**.sip.ashburn.twilio.com
Umatilla OR: *client-domain*-voice**-posh-test**.sip.umatilla.twilio.com

- Because UAT is only used for testing, it doesn't need both Ashburn and Umatilla paths, so feel free to build just one path or the other.

Production Modified
Ashburn VA: *client-domain*-voice**-posh-modified**.sip.ashburn.twilio.com
Umatilla OR: *client-domain*-voice**-posh-modified**.sip.umatilla.twilio.com

- Because Production Modified is only used for testing, it doesn't need both Ashburn and Umatilla paths, so feel free to build just one path or the other.

Production
Ashburn VA: *client-domain*-voice**-posh**.sip.ashburn.twilio.com
Umatilla OR: *client-domain*-voice**-posh**.sip.umatilla.twilio.com

Where *client-domain* is your organization's website domain, like *mycreditunion-org*, for example.

In order to resolve the DNS FQDNs to IP addresses, your SBC will need access to a DNS server.

Inside the SIP messages you send to Twilio is a destination SIP URI (a.k.a. SIP address). Configure your SBC to set that SIP URI's domain per the examples below. Optionally – if you set them to match the DNS FQDNs above – they can contain the locations **ashburn** or **umatilla**:

UAT (User Acceptance Testing)
sip:1001@*client-domain*-voice**-posh-test**.sip.twilio.com

Production Modified
sip:1002@*client-domain*-voice**-posh-modified**.sip.twilio.com

Production
sip:1003@*client-domain*-voice**-posh**.sip.twilio.com

Where *client-domain* is your organization's website domain, like *mycreditunion-org*, for example.

The phone number to the left of the @ symbol doesn't matter to Twilio – Twilio keys on the SIP domain to the right of the @ symbol – so feel free to use any phone numbers you like.

Monitoring with SIP OPTIONS Requests

To monitor the connection between your SBC and Twilio, you may configure your SBC to send a SIP **OPTIONS** request periodically. Twilio will respond with **200 OK**. Typical intervals are 30 or 60 seconds, depending on how quickly you want your SBC to know if its connection to Twilio is down.

> **Important:** Do not send more than one SIP **OPTIONS** request every 10-15 seconds or your requests may be banned by Twilio.

Twilio will *not* send SIP **OPTIONS** requests to your SBC.

Working with Posh

Your Posh contact for telephony questions, help, and testing:

Matt Augustine
Principal Telephony Engineer
matt.augustine@posh.tech
M: 857-400-8220

What Posh Needs to Know

Your SBC or cloud-based contact center Internet IP addresses. Posh needs to add them to Twilio's Access Control List (ACL). Monitoring with SIP OPTIONS will work without the ACL, but calls will not.

> **Note:** If the ACL is the reason for call failure, Twilio will respond **403 Forbidden** with the following SIP header "X-Twilio-Error: 32202 Authentication failure – source IP address not in ACL."

The 3 phone numbers you configure to send calls to your Posh Voice UAT, Production Modified, and Production environments. Testing is easier if they are Direct Inward Dial (DID) numbers that can be reached from the outside.