Spectrum Enterprise SIP Trunking IP PBX Configuration

Physical Connectivity to network:

- Assign a local private IP Address to the local area network (LAN) side of the gateway. This IP address must be on the same subnet as your IP PBX (Wide area network (WAN) side of the IP PBX if it has an integrated session boarder controller (SBC)). This is the IP address that Spectrum Enterprise will provision on the Spectrum Enterprise provided gateway and will become the SIP proxy IP address.
- Verify connectivity to the gateway from the PBX on day of install.

PBX configuration:

- Spectrum Enterprise will provide the appropriate proxy IP Address to be used in the IP PBX.
- Spectrum Enterprise will only support 1 IP address to the IP PBX for all RTP call traffic.
- Configure your IP PBX to use codec G.711 µlaw. Spectrum Enterprise recommends G.711 µlaw codec for both audio and fax.
- Packetization rate recommendation is 20ms.
- Outbound Caller ID sent from the PBX on all 911 calls must be the Spectrum Enterprise billing telephone number (BTN) assigned to your Trunking Service. If you have Spectrum Enterprise Trunking that serves multiple locations and you requested multiple location Enhanced 911 (E911) service you can send any fully 911 authenticated DID provisioned on your account.
- The IP PBX must support responding to SIP “Option Pings” on port 5060. This is the method by which Spectrum Enterprise keeps connectivity to the PBX.
- Configure the dial tone multi-frequency (DTMF) setting using RFC-2833 for DTMF signaling and payload type 101. Out of band DTMF is not supported.
- Only Voice traffic (no data) should be sent to the IAD. A separate VLAN or connection for data traffic is recommended.
- IP PBX registration: Static IP (local, private IP address) registration is recommended.

Telephone Numbers:

- Ported and Native telephone numbers are supported.
- Digits; to/from PBX: 10 or 11 digits are supported for outbound, 10 digits for inbound.

Security:

It is the Customer’s (and/or the Customer’s Agent’s) responsibility to properly secure the PBX to prevent the PBX from being compromised and fraudulent calls from being made by internal or external users. You should make sure your PBX is secure.

The following are general recommendations for securing your PBX. Your PBX's manufacturer may be able to provide specific guidelines.

- It is important to utilize secure passwords for both administrative access to the PBX and for any voicemail boxes utilized on the PBX. Make sure you change the default passwords provided by the manufacturer. The manufacturer default passwords can be easily found in the manual or on line. Use strong passwords. Do not use the last four numbers of the phone number, repetitive or sequential numbers like 1111 or 1234. If a password becomes compromised, unauthorized access can be obtained to make unauthorized calls.
- To minimize the exposure to fraudulent calling, limit toll calling capability to just those users that require it, especially international calling. You can also have International calling disabled for your account by calling Spectrum Enterprise customer care.
- Keep systems up-to-date with operating system patches. Your system may have vulnerabilities that can be fixed with periodic software/firmware updates.
- Disable any unused services in order to avoid misuse. For example, if you don't use the voicemail system, disable it, as an attacker might exploit a weakness to gain access to further services.
- Restrict out dialing on Voicemail systems: Out dialing from a voicemail system is when you allow outgoing calls to be placed directly from your voicemail box. It is recommended to turn off this feature if it is not required.