CallerID.com
IDENTIFY | CONNECT | EMPOWER

Vertex: EdgeMarc SBC & UDP Setup

Provider-assisted installation guide • October 22, 2026

1. Why an SBC may be needed

The standard CallerID.com Vertex reads caller name and number from **unencrypted SIP signaling carried over UDP**. If the phone service presents only encrypted SIP signaling (TLS), or only SIP over TCP, the standard Vertex cannot read that feed directly.

An ordinary firewall does not decrypt a phone provider's traffic. A compatible **session border controller (SBC)**, such as an appropriately configured Edgewater/Ribbon EdgeMarc, can act as an authorized SIP endpoint: it terminates the provider-approved TLS connection and creates a separate, unencrypted UDP SIP connection on a trusted local voice network. It is not a passive encryption bypass.

Provider → encrypted SIP/TLS → EdgeMarc SBC
EdgeMarc → local unencrypted SIP/UDP → PBX or phones
Mirrored local SIP → Vertex → caller-ID records → POS

Two different UDP connections: SIP signaling is the input Vertex reads. UDP port **3520** is the usual *output* destination for the caller-ID records Vertex sends to your application. Opening port 3520 does not decrypt SIP or convert TCP to UDP.

Connection	Purpose	Setting
Provider ↔ EdgeMarc WAN	Secure provider SIP signaling	TLS; often 5061, but use the provider's assigned port
EdgeMarc ↔ local PBX/phones	Readable SIP signaling for Vertex monitoring	Unencrypted UDP; often 5060, per the approved design
Vertex → POS/application	Extracted caller-ID records, not SIP	UDP 3520 by default; match the application's configured port

SRTP is different: it encrypts audio, not the SIP caller-ID headers. SRTP alone does not prove signaling is encrypted. This guide does not instruct you to disable encryption throughout the phone system.

Compatibility gate — before purchasing or changing anything

Your VoIP provider must approve an SBC/B2BUA deployment and provide the necessary trunk, authentication and certificate requirements. Provider-managed phones may not permit this topology. An EdgeMarc cannot universally decrypt arbitrary hosted services. If the provider cannot support a readable local UDP SIP leg, stop and contact CallerID.com and the provider before buying equipment.

Scope: standard Vertex, using a provider-approved PBX/SBC topology. Menu examples are based on Ribbon EdgeMarc 2900A VOS 15.8.0 and the documented EdgeMarc 6000/VOS 15.7 interface. Exact model, firmware, licensing and provider support must be confirmed. This is not a CallerID.com hardware interoperability certification.

2. Preparation and network connections

1. **Record the design.** Obtain the provider's registrar/proxy FQDN, SIP transport and port, permitted SBC IPs, authentication method, DID routing, certificate/CA requirements, media policy and rollback contact. Do not substitute another provider's published example values.
2. **Back up before changes.** Export the current EdgeMarc configuration using its supported backup procedure. Record the model, VOS version, licenses and existing phone/PBX settings. Schedule a maintenance window; retain a tested rollback path. Do not factory-reset an in-service unit.
3. **Use an approved topology.** Connect the EdgeMarc WAN to the provider-facing network and its LAN to the local voice network/PBX. Place a managed switch with port mirroring, or a suitable network TAP, on the *local UDP SIP leg*. Do not connect Vertex to the encrypted WAN feed.
4. **Sign in securely.** Use the EdgeMarc's assigned management address and your administrator account. Under **Network**, verify LAN/WAN addressing, subnet, gateway, DNS and any required routes. Configure correct time/NTP for certificate validation. Restrict management access to authorized administrators.

3. Keep the provider-facing SIP connection encrypted

1. **Certificates:** open **Security → Certificates**. If the provider requires an SBC certificate, create a CSR for the approved SBC FQDN, obtain a signed certificate from an accepted CA, and install the certificate, matching private key and required trust chain using Ribbon's procedure. Protect private keys.
2. **Provider SIP:** open **VoIP → SIP**. Set **SIP Server Address** to the provider's approved FQDN/address, **SIP Server Transport** to **TLS**, and **SIP Server Port** to the assigned TLS port (commonly 5061). Apply the provider's domain and proxy restrictions.
3. **TLS policy:** in the SIP page's TLS settings, select the installed certificate for the WAN interface and use the provider's supported secure TLS policy. Verify the remote certificate/hostname as supported and required. Do not copy a sample "No check" policy or disable certificate validation to force a connection.
4. **Apply carefully:** use the page's **Submit** control when the complete change set is ready. Confirm the provider-side registration or trunk status and logs. IP-authenticated trunks may not register; use the provider's expected health checks instead. Resolve certificate or routing failures before proceeding.

> **Preserve security:** do not turn off the EdgeMarc's SIP/B2BUA processing globally. An upstream router's SIP ALG and the SBC's required SIP processing are different controls. Change either only under the provider-approved design.

CallerID.com
IDENTIFY | CONNECT | EMPOWER

Local UDP SIP & Vertex delivery

The Vertex monitors SIP; it is not a SIP trunk or telephone endpoint

4. Configure the readable local SIP leg

1. **Enable the intended signaling path:** in the documented VOS interface, open **VoIP** and locate **B2BUA Options → Route all SIP signalling through B2BUA**. Enable it when required by the approved trunk/PBX design. Do not reroute a working hosted-phone deployment without provider approval.
2. **Add the actual PBX:** open **VoIP → SIP → B2BUA → Trunking Devices** and choose **New Row/New Entry**. Enter a descriptive name, the PBX model (or approved Generic PBX profile), and its real LAN IP/FQDN. Set **Transport = UDP** and **Port = 5060**, unless a different local UDP SIP port is explicitly required. Click **Update**. Do *not* enter the Vertex IP as the PBX.
3. **Check the listener:** under **VoIP → SIP → UDP**, verify **Client Listening Port(s)** includes the local SIP port used by the PBX/phones. Do not replace the provider's WAN TLS settings with UDP. Apply the provider-approved local trust/ACL restrictions.
4. **Route the calls:** in the B2BUA **Actions** and **Match** sections, route inbound calls to the defined PBX and outbound calls to the approved provider leg. Preserve DID matching, caller-ID headers, dial plan, emergency calling and existing number-format rules. These values are site-specific; do not add permissive "Any" outbound rules just for Vertex.
5. **Save and verify:** click **Submit** to apply the completed B2BUA changes. If the menu or required transport/certificate options are absent, stop and use the model-specific Ribbon documentation rather than guessing. Confirm normal inbound and outbound calling before adding capture equipment.

5. Make the local signaling visible to Vertex

1. **Mirror the correct link:** configure the managed switch's SPAN/port-mirror source for the local PBX/voice link carrying both directions of the unencrypted UDP SIP traffic. Connect the Vertex monitoring interface to the mirror destination according to its installation manual. Merely sharing a switched LAN does not guarantee visibility.
2. **Configure application delivery:** using the normal Vertex setup procedure, set the destination to the receiving POS/application computer's stable LAN IP and set the output UDP port to **3520**, or the port required by that application. Match the application's listener settings exactly.
3. **Permit only necessary local traffic:** allow inbound UDP on that application port from the Vertex IP in the receiving computer's firewall. Provide LAN/VLAN routing only as approved. Do not expose SIP, the management interface or UDP 3520 to the public internet.

The mirror destination and normal network-delivery connection must follow the Vertex model's wiring instructions. Do not assume a mirrored switch port provides a normal two-way management or output connection.

Acceptance checks & troubleshooting

Confirm both the SIP input and the application output

6. Test before returning the site to service

1. **Check the capture point.** Make an authorized test call. At the local mirrored link, inspect a packet capture with a filter such as `sip && udp`. If a nonstandard port is not decoded, use Wireshark's Decode As SIP or inspect `udp.port == 5060` using the actual local SIP port.
2. **Confirm readable signaling.** Verify a SIP `INVITE` with the expected caller-number headers; confirm caller name when the provider supplies it. Capture on the correct side of the SBC. TLS Application Data, unrelated UDP discovery packets, or RTP audio are not evidence of readable SIP.
3. **Check Vertex output independently.** On the POS/application network, verify a datagram from the Vertex to the correct computer and UDP destination port, normally 3520. Confirm that the actual POS/CRM caller-ID popup shows the expected number/name. A working SIP trace alone does not prove application delivery.
4. **Complete service checks.** Test inbound/outbound audio, caller-ID presentation, transfers and the site's required features. Follow the provider's approved emergency-calling test procedure; do not place an unarranged emergency test call. Save the accepted configuration and document results.

Symptom	Check next
No readable SIP at the mirror	Wrong mirror source, voice VLAN, TLS/TCP-only local leg, or phones bypassing the SBC. Changing the POS's 3520 firewall rule will not fix this.
Readable UDP INVITEs, no Vertex output	Vertex connection/setup, SIP header/number format and model compatibility. Ask CallerID.com to review a minimum, authorized capture.
Vertex UDP reaches the PC, no popup	Application listener, port mismatch, selected interface, firewall scope, duplicate listeners or application record-format settings.
Trunk registration or calls fail	Provider authorization, TLS certificate/trust, routing and B2BUA rules. Restore the backed-up configuration if service is affected.

When to stop

If the provider cannot authorize the topology, the model lacks the required features, readable UDP SIP cannot be produced, or existing calling is disrupted, stop and involve the provider and CallerID.com. Do not disable internet-side security, bypass authentication, or promise compatibility from an SBC model name alone.

References and support

Technical steps were checked against these published configuration references, not an in-house EdgeMarc hardware test. Provider-specific sample addresses and credentials have intentionally not been reproduced.

- Ribbon: EdgeMarc SBC Configuration with Zoom BYOC — VOS 15.8.0; Network, VoIP/B2BUA and Section C TLS settings.
- Telnyx: Ribbon EdgeMarc 6000 Setup — VOS 15.7 compatibility; SIP, Trunking Devices, Update/Submit and routing controls.
- CallerID.com Vertex information and installation video • Contact CallerID.com

Packet captures can contain customer information. Obtain permission, minimize/redact sensitive data, and use an approved private support channel.