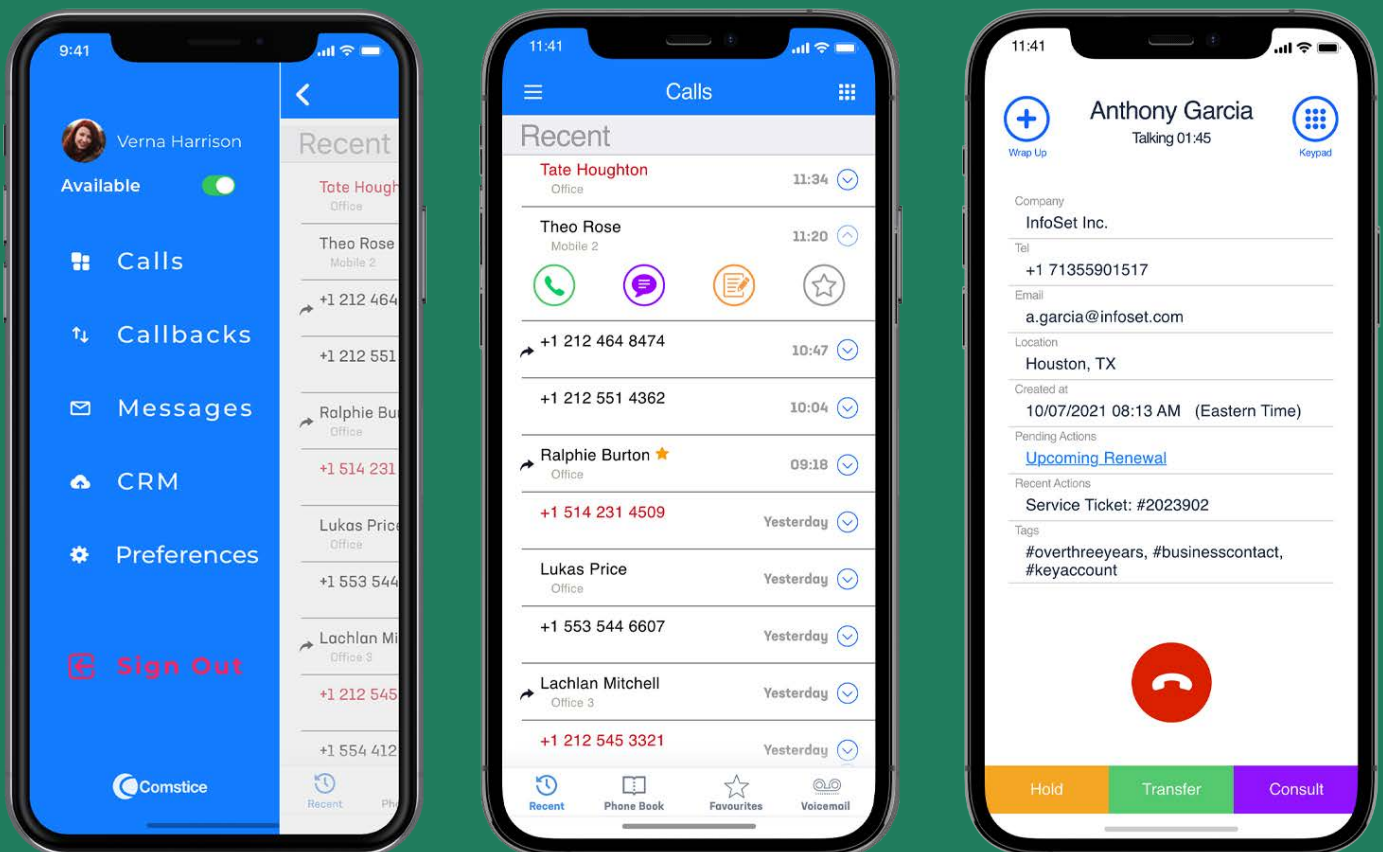


Comstice Mobilr Softphone App for Avaya

Datasheet



Comstice Mobile Softphone for Avaya

Comstice Mobile Softphone app is a universal softphone app that can be integrated with different platforms including Avaya. It can be used directly as a mobile softphone or through Avaya Contact centers for better reporting, presence-specific call routing

Who is it for?

Comstice Mobile Softphone is mainly used by the employees and partners outside the customer service

- doctors and nurses
- regional sales specialists
- universities
- pharmaceuticals
- IT departments
- Campus environments such as airports, manufacturing plants where many people are on the move

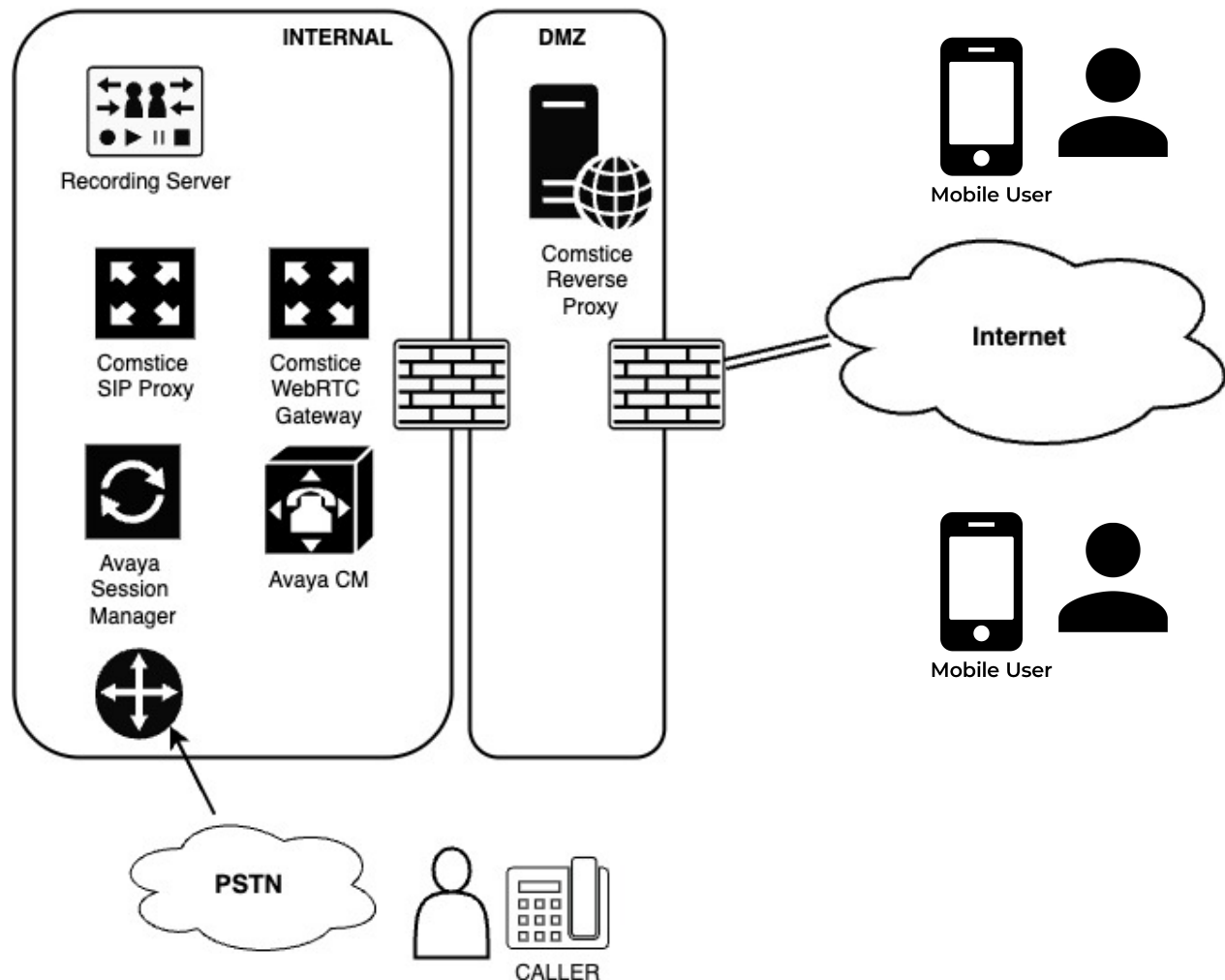
Features

Comstice Mobile Softphone offers;

- VoIP and non-VoIP (mobile) calling (mainly used when mobile internet is not good)
- **SSO Support:** Single sign-on with your SSO provider.
- Mobile Business calls with an on-premises or privately hosted solution
- **Secure access with audio and signaling encryption**
- Reporting through Avaya CMS or Comstice Quartz Reporting
- User availability and state changes with Avaya AES state change and re-routing
- offers VPNLess enterprise telephony with encrypted audio and signaling
- ability to record mobile business calls on your network
- SMs, Whatsapp and Webchat integration via Comstice Unified Messaging
- Access to third-party voicemail systems
- Integration with CRM Services
- support video as well as audio for each user

It can also be bundled with **Comstice Agent Webphone app**

Comstice Mobile Softphone Locally Hosted



Comstice Mobile Softphone solution can be hosted on-premises. **In this case, Comstice Reverse Proxy handles the HTTPS communication, provides extra layer of security with IP Whitelisting and DDoS Protection.**

Comstice Mobile Softphone is a WebRTC-based phone on the browser. Therefore, encryption is built-in on the audio stream and the HTTPS-based signaling.

SSO can be enabled for the mobile user with MFA support.

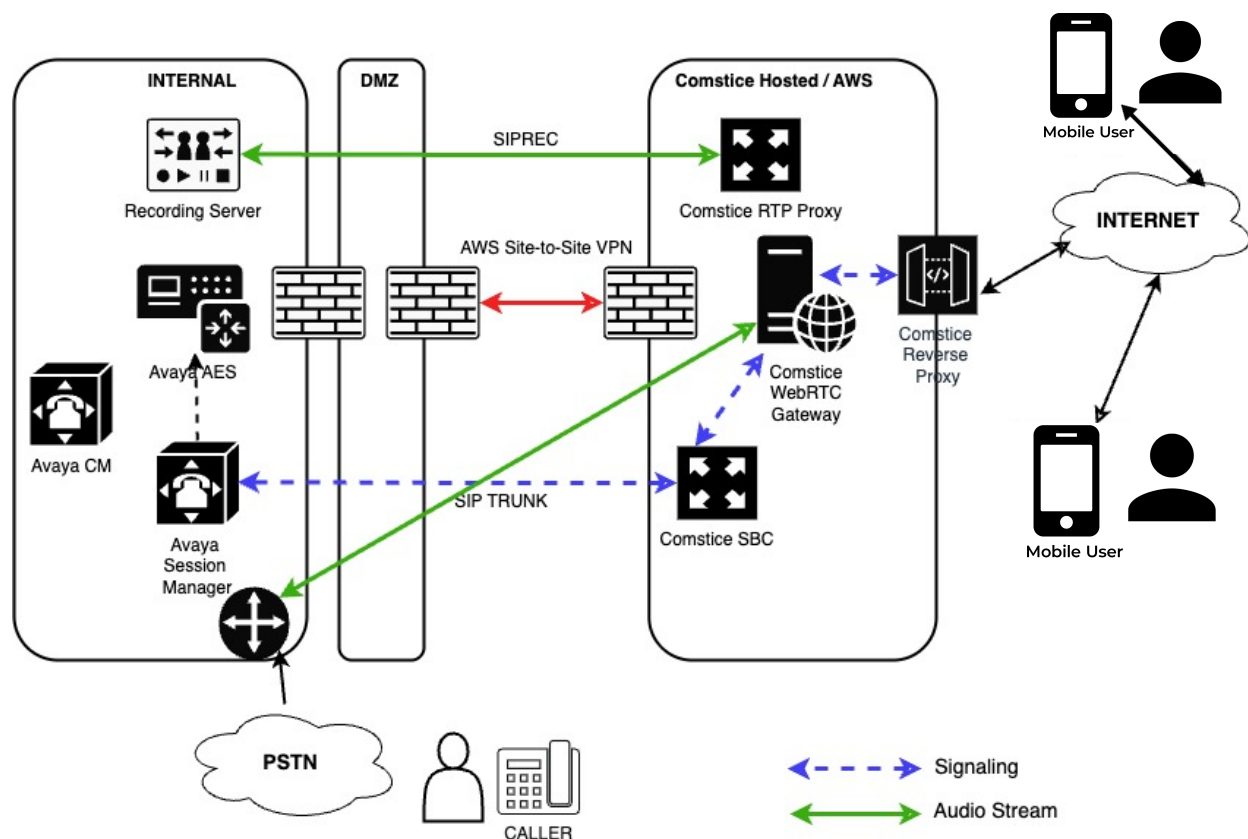
Only TCP port 443 is open to the public access which is terminated at Comstice Reverse Proxy in the DMZ. This port is configurable.

Comstice Mobile Softphone with Avaya - Comstice Hosted

.Comstice Mobile Softphone solution can be hosted by Comstice. Using a site-to-site VPN between Comstice Private Cloud allocated for this project and the client network, the solution topology can be simplified.

SOC 2 and ISO 27001 Certifications

Comstice Cloud Service is certified for the maximum data privacy and information security.



SOC2 Type II
CERTIFIED



ISO
27001



Project Plan: Roles and Responsibilities

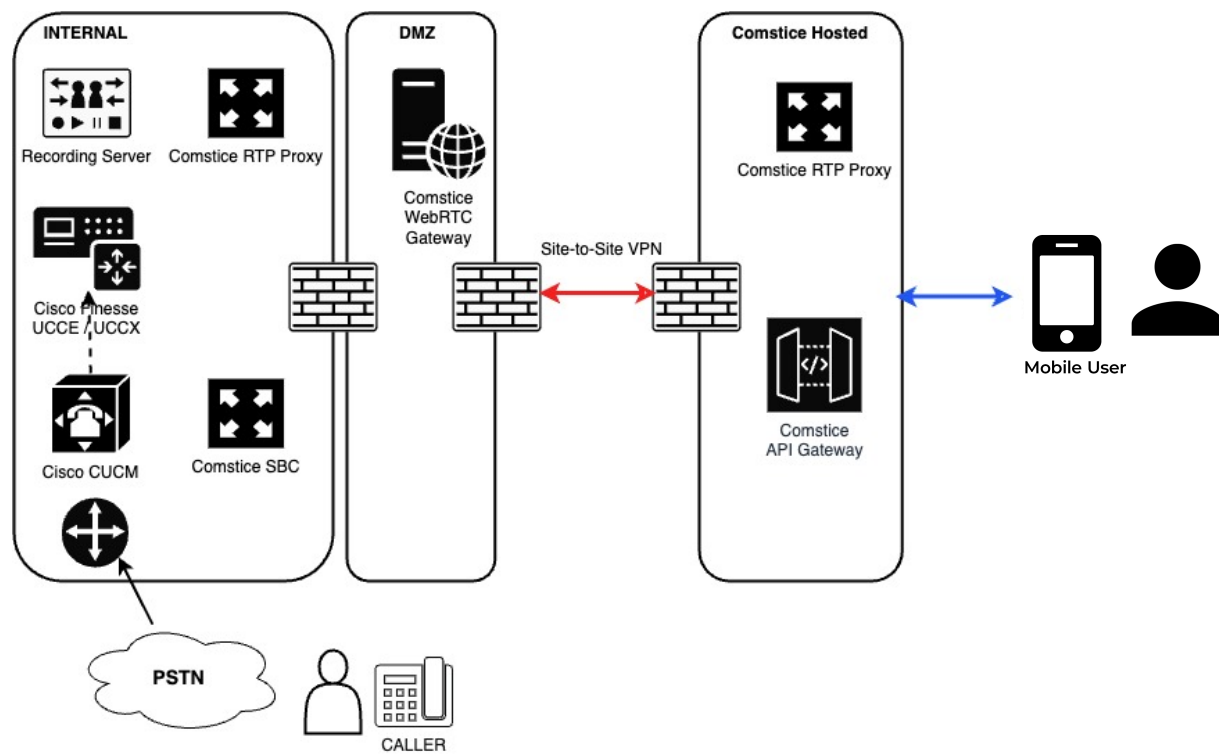
Create low level design - LLD with the IP addressing, firewall and SIP trunk details	Comstice and the Client
Provide Linux OVAs or build on a client provided RedHat for the server components	Comstice
Bring up Virtual servers and allocate IP addreses	Client
Create public FQDNs and HTTPS SSL certificates	Client
Apply the firewall changes as agreed on the LLD	Client
SSO Integration	Client Comstice
End to end testing	Comstice
UAT	Comstice and Client
Handover to Day2	Comstice and Client

Cybersecurity

Comstice Mobile Softphone users are often working remotely with no VPN. Opening local firewall ports is not acceptable in many Cybersecurity policies. Comstice offers two options in this case;

Comstice API Gateway

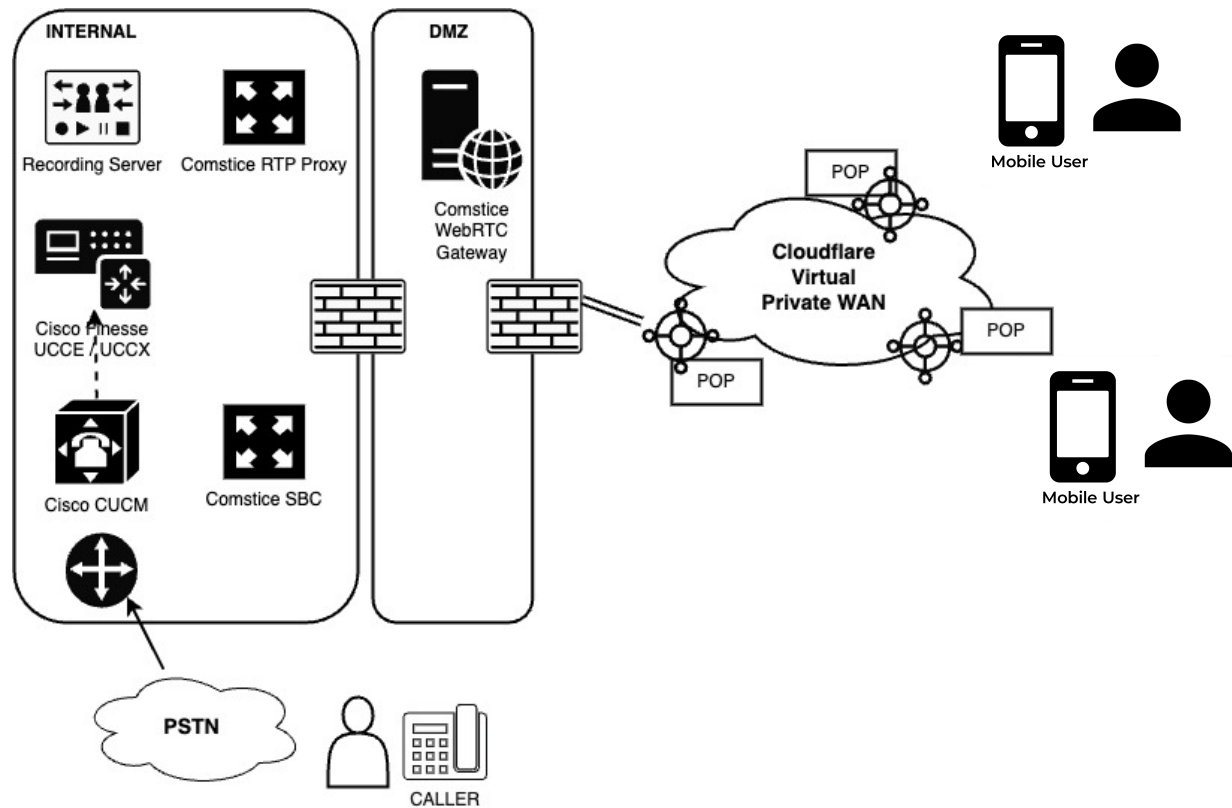
Comstice can handle the initial communication using API Gateways in the cloud. Using site-to-site VPN, this traffic is then proxied to client's internal network.



Cybersecurity - 2

Cloudflare Private WAN

This option offers a private virtual cloud from Cloudflare; remote user enters the private cloud from the nearest POP location and the overall communication is secured within the private WAN.



Comstice Webphone vs MS Teams

Comstice Webphone and Comstice Mobile Softphone Advantages

- MS Teams is cloud-based service, whereas Comstice Webphone can be hosted on-premises or privately hosted for your organization.
- MS Teams allows to access many confidential information, therefore it is not suitable for rolling out for the partners and contractors. Comstice Webphone has various security layers and can be restricted.
- MS Teams does not offer any integration with CRM
- Comstice Mobile Softphone can be customized for your business needs. Mobile Softphone has multiple skins i.e. user interface options that can be changed for different use cases
- Comstice Mobile Softphone can use a third-party phone line if audio quality over the current Wi-Fi connection is not suitable.
- **Comstice Mobile Softphone app also works through the mobile networks as an alternative.** If the mobile internet is not working as expected, user can make and receive calls through cell networks. This means there will be two call legs and the last leg of the call will be via cell networks. This guarantees the acceptable level of audio quality and calls will still go through Avaya and will be recording, DID masking will still work.

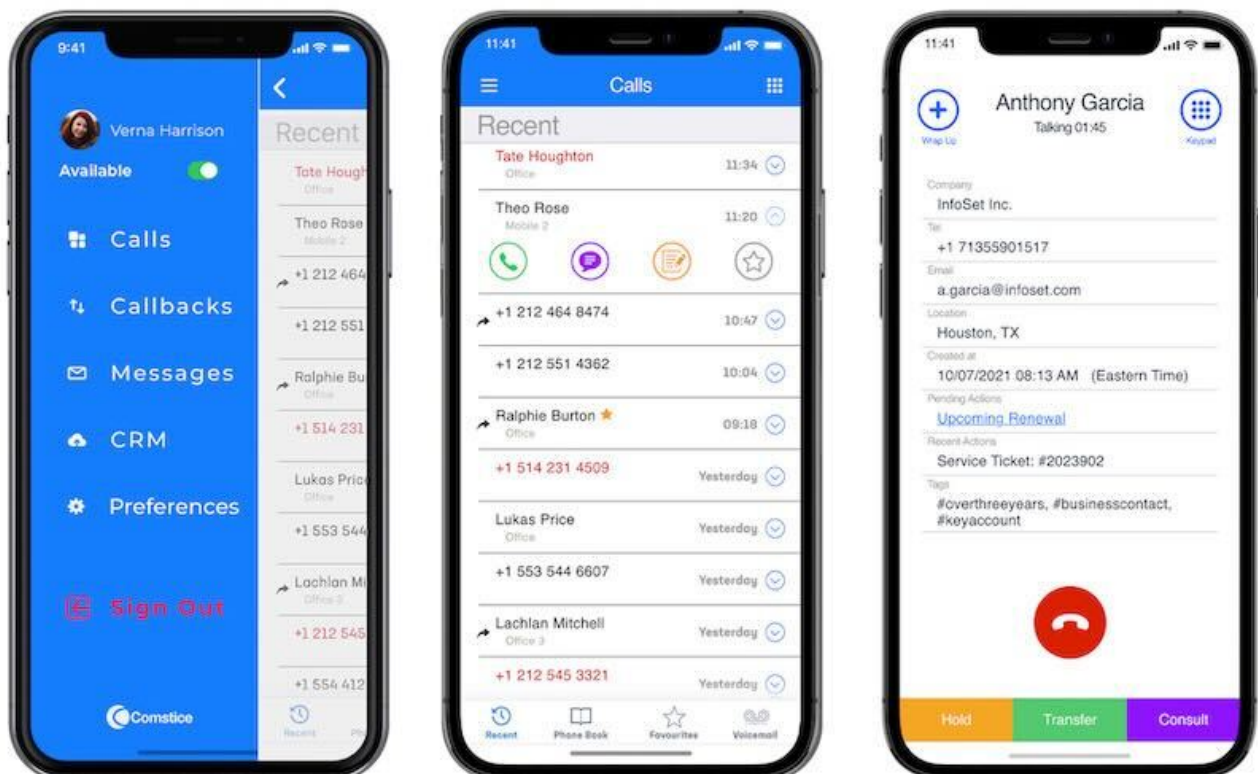
Comstice Mobile Softphone User Interface

Configurable App Interface for Business Users

Comstice app is easy to use. It offers a simple call logs section to list the recent calls. User can see the call details and call back the numbers if needed.

User can change the presence to stop and start receiving calls. This option can be automated on the server side; The system can set the user available in the working hours and set it to not available after hours.

User can also have SMS chats, handle Whatsapp and webchats if the solution is integrated with Comstice Customer Messaging solution. SMS number can be the same as the user's DID, depending on the DID provider.



Webphone Monitoring

Comstice offers the following monitoring actions

SIP Results and Session Tracing

You can search for a particular session or callerID / Called number to see the SIP session events saved.

Display Results										Regex Results Filter
☐ Date	Session ID	SIP Method	SIP From user	SIP To user	Source IP	Src Port	Destination IP	Dst Port	Alias Dest	
☐ 2020-09-13 15:59:33.851	1BEphBnVhK	200	259	5000		5060	172.24.0.2	5060	7139393714	
☐ 2020-09-13 15:59:33.851	1BEphBnVhK	200	259	5000	172.24.0.2	5060	172.24.0.1	5060	7139393714	
☐ 2020-09-13 15:59:33.852	1BEphBnVhK	200	259	5000	172.24.0.1	38188	172.24.0.2	5060	7139393714	
☐ 2020-09-13 15:59:33.852	1BEphBnVhK	200	259	5000	172.24.0.2	5060	172.24.0.1	44449	7139393714	
☐ 2020-09-13 15:59:33.896	1BEphBnVhK	ACK	259	5000	172.24.0.1	44449	172.24.0.2	5060	984563	
☐ 2020-09-13 15:59:33.896	1BEphBnVhK	ACK	259	5000	172.24.0.2	5060		5060	984563	
☐ 2020-09-13 15:59:33.896	1BEphBnVhK	ACK	259	5000	172.24.0.1	38188	172.24.0.2	5060	984563	
☐ 2020-09-13 15:59:33.896	1BEphBnVhK	ACK	259	5000	172.24.0.2	5060	172.24.0.1	38188	984563	
☐ 2020-09-13 15:59:35.852	1BEphBnVhK	200	259	5000		5060	172.24.0.2	5060	7139393714	
☐ 2020-09-13 15:59:35.852	1BEphBnVhK	200	259	5000	172.24.0.2	5060	172.24.0.1	5060	7139393714	
☐ 2020-09-13 15:59:35.853	1BEphBnVhK	200	259	5000	172.24.0.1	38188	172.24.0.2	5060	7139393714	

You can see the RTCP events with MoS values (1-5) for the cal



Webphone Call Logs and Daily Stats

You can monitor the XLog events under Logs tab

Call-ID: 1BEphBnVhK

Messages

Flow

QoS

Logs

Export

HEP Logs

Loki

☐ Timeseconds

Timestamp

Messages

2020-09-13 15:59:31.236

ERROR:time [Sun Sep 13 13:59:31 2020] method (INVITE) r-uri (sip:5000@sip. .com) relay pass-through

2020-09-13 15:59:31.237

ERROR:Attempt to route with preloaded Route's [sip:259@sip. .com/sip:5000@sip. .com/sip:5000@sip. .com/1BEphBnVhK]

2020-09-13 15:59:31.237

ERROR:time [Sun Sep 13 13:59:31 2020] method (INVITE) r-uri (sip:5000@sip. .com) preload route remove & pass-through

2020-09-13 15:59:31.237

ERROR:new branch at sip:5000@sip. .com

2020-09-13 15:59:31.291

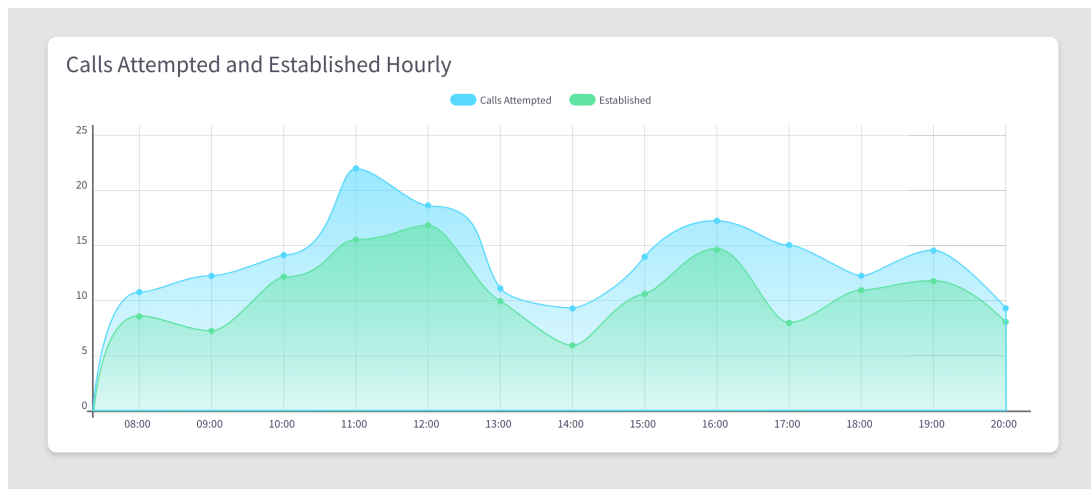
ERROR:time [Sun Sep 13 13:59:31 2020] method (INVITE) r-uri (sip:5000@sip. .com) relay pass-through

2020-09-13 15:59:31.292

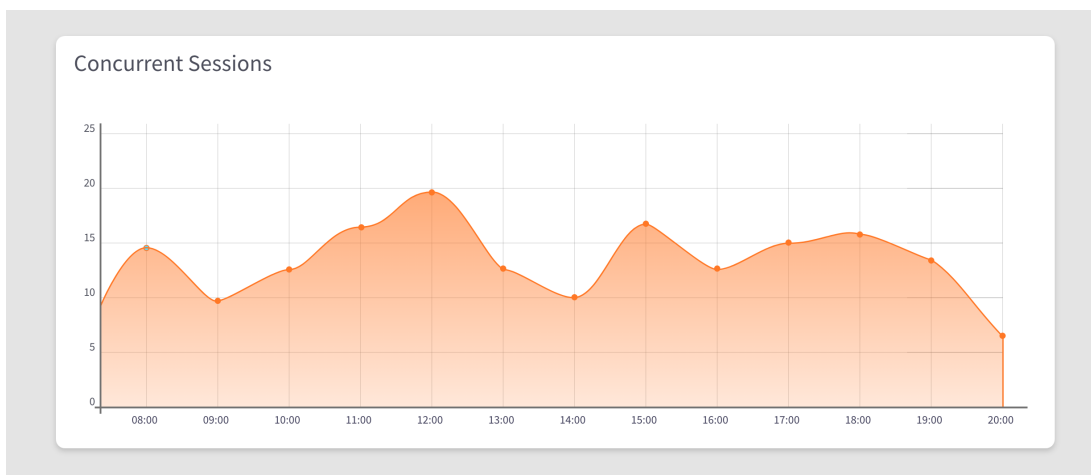
ERROR:new branch at sip:5000@sip. .com

Calls Attempted and Established

This report can show interval-based calls attempted and established



Concurrent Calls



Mobile App Always Receives a Call

Comstice Mobile Softphone always receives a call even when making outbound calls; Comstice Mobility server receives the "Make Call" event, calls the mobile softphone first, then dials the destination via Avaya CM and Session Manager and merges both calls.

This model helps to secure the call traffic, eliminates the malicious calls and offers a secure activity. Softphone has no Avaya dependency, it can be implemented into any SIP-based Telephony Network.

Support

Comstice offers priority support available 24/7 for the deployments that have high availability servers. We aim to respond in an hour and resolve in 24 hours based around all the dependencies for the customer-hosted deployments.

Comstice-hosted deployments will be responded in an hour and will be resolved in eight hours.

Comstice provides admin training to customer IT departments for the basic troubleshooting.

Comstice Managed Service team acts as an escalation. Customer IT department can open tickets via comstice.com, support@comstice.com or +1 713 828 3714.

Comstice does not accept tickets directly from the end users.