SmartVideo for Genesys Cloud

1. Technology

SmartVideo for Genesys is based on the de-facto standard in real time communications - WebRTC. WebRTC is an open source project that provides browsers and mobile applications with Real-Time Communications (RTC) capabilities. SmartVideo utilize the best in class audio (OPUS, G722) and video (VP8, VP9, H264) codecs.

SmartVideo is a cloud solution. SmartVideo is developed on its own backend, which is hosted on AWS. It is a lightweight App and serves two basic purposes:

- Signalling - needed to facilitate the process of establishing a video connection
- Presence

SmartVideo follows the best practices in real time communication - a standard called ICE. When recording is not required, SmartVideo establishes a direct - peer-to-peer connection between the two parties. The benefits of this are:

- High quality video;
- Very low latency;

When recording is required, the audio/video traffic is channelled through the SmartVideo backend. The recording service can be configured to record both audio and video, or just the audio. For storage and retrieval the customer can provide their own storage solution or use SmartVideo storage and retrieval.

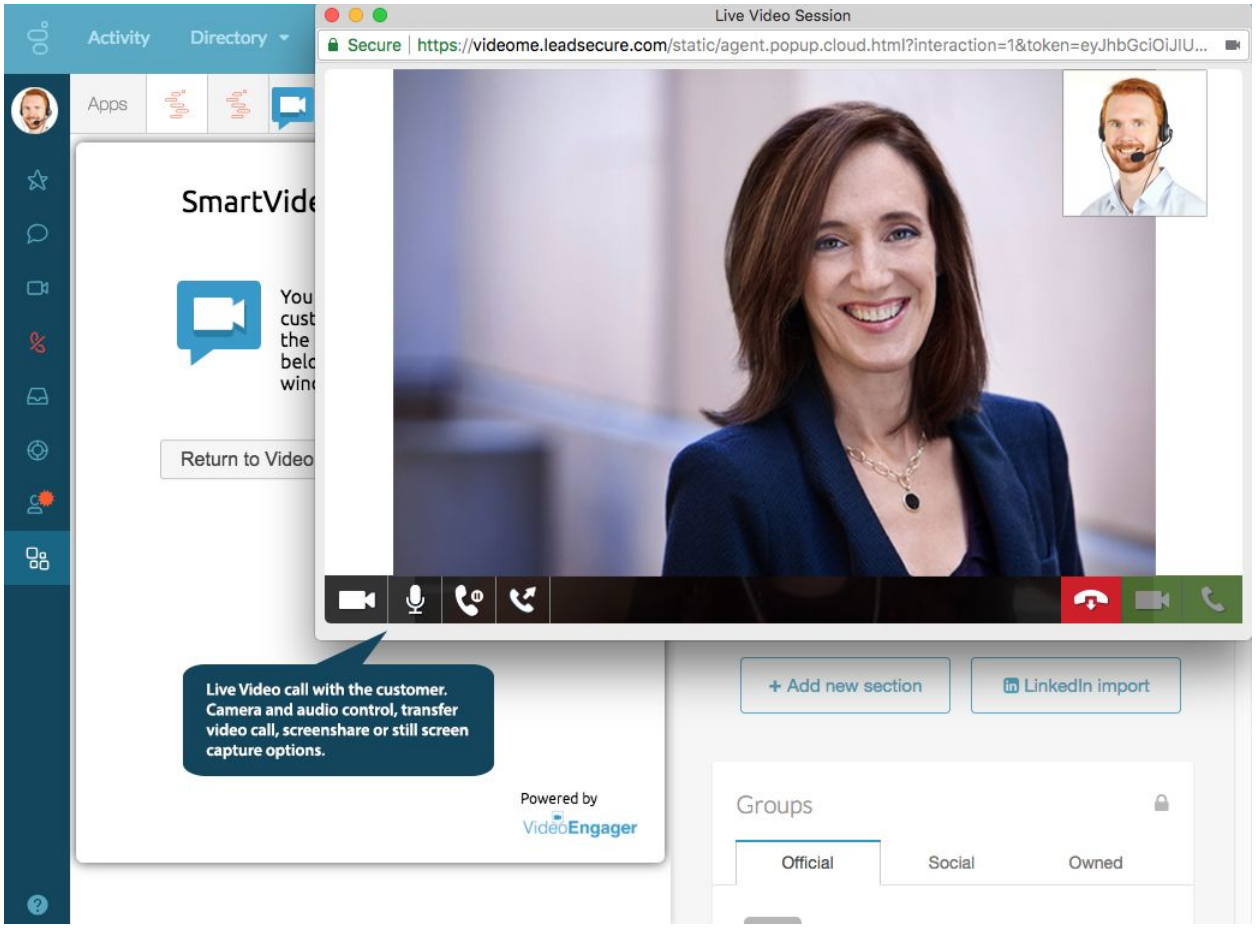
SmartVideo is developed using its own web widgets. One for the agent, which does the integration in the Interaction Connect and one for the customer. The widgets use responsive design and work equally well on desktop and mobile browsers. For WDE there is a window plugin which is added to the Genesys Cloud deployment.

Nomadic agents can receive video calls on their mobile phone or tablet by installing the SmartVideo mobile application software.

2. Experience

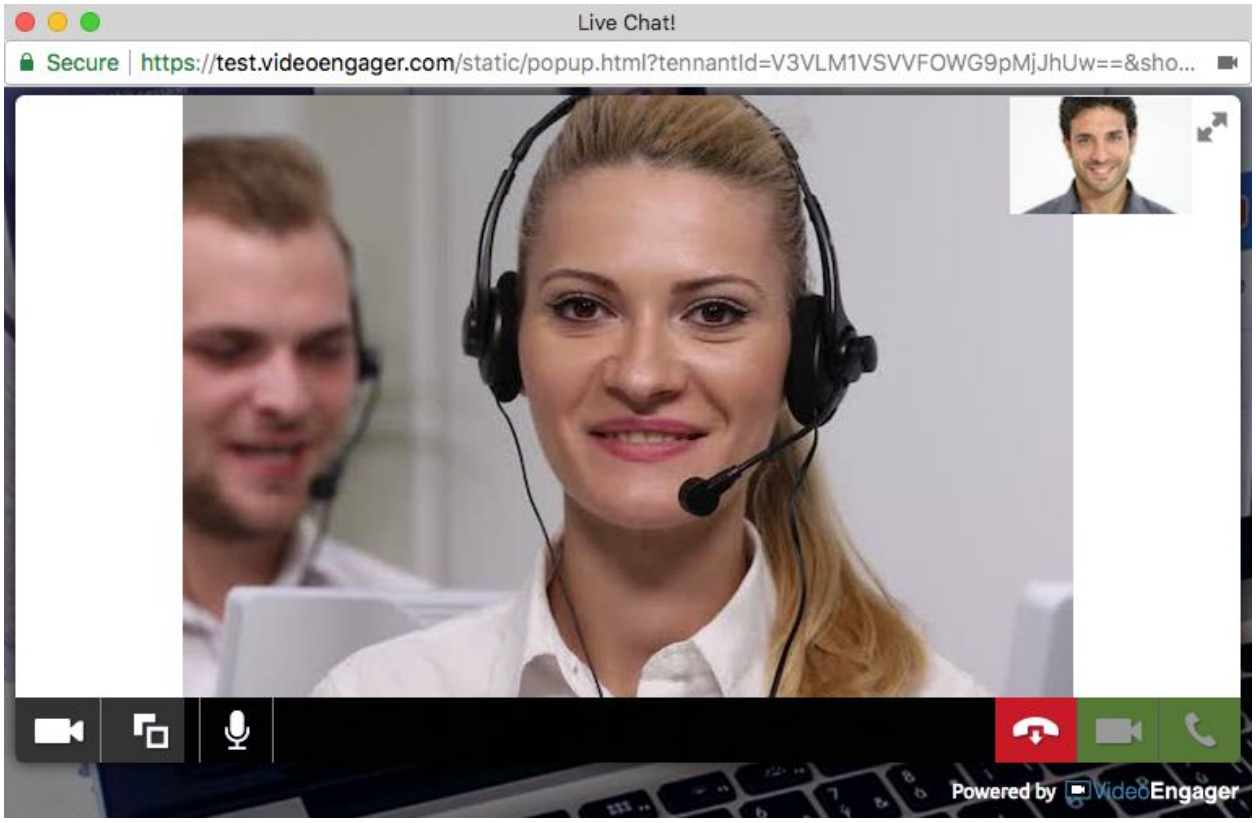
For Agents

The SmartVideo solution integrates inside the Genesys Cloud platform. Agents are not required to switch between applications/windows or remember different login credentials. The video capability is made available in the context of the active interaction. SmartVideo appears as a separate application or widget. Before sending a video chat invitation, the agent is presented with a screen to adjust camera and voice settings in preparation of the video call. Once in a video call, the agent has all the standard call control capabilities like mute microphone, call hold, pause camera as well as a number of advanced features like screen sharing, video call transfer to a field expert and call record.

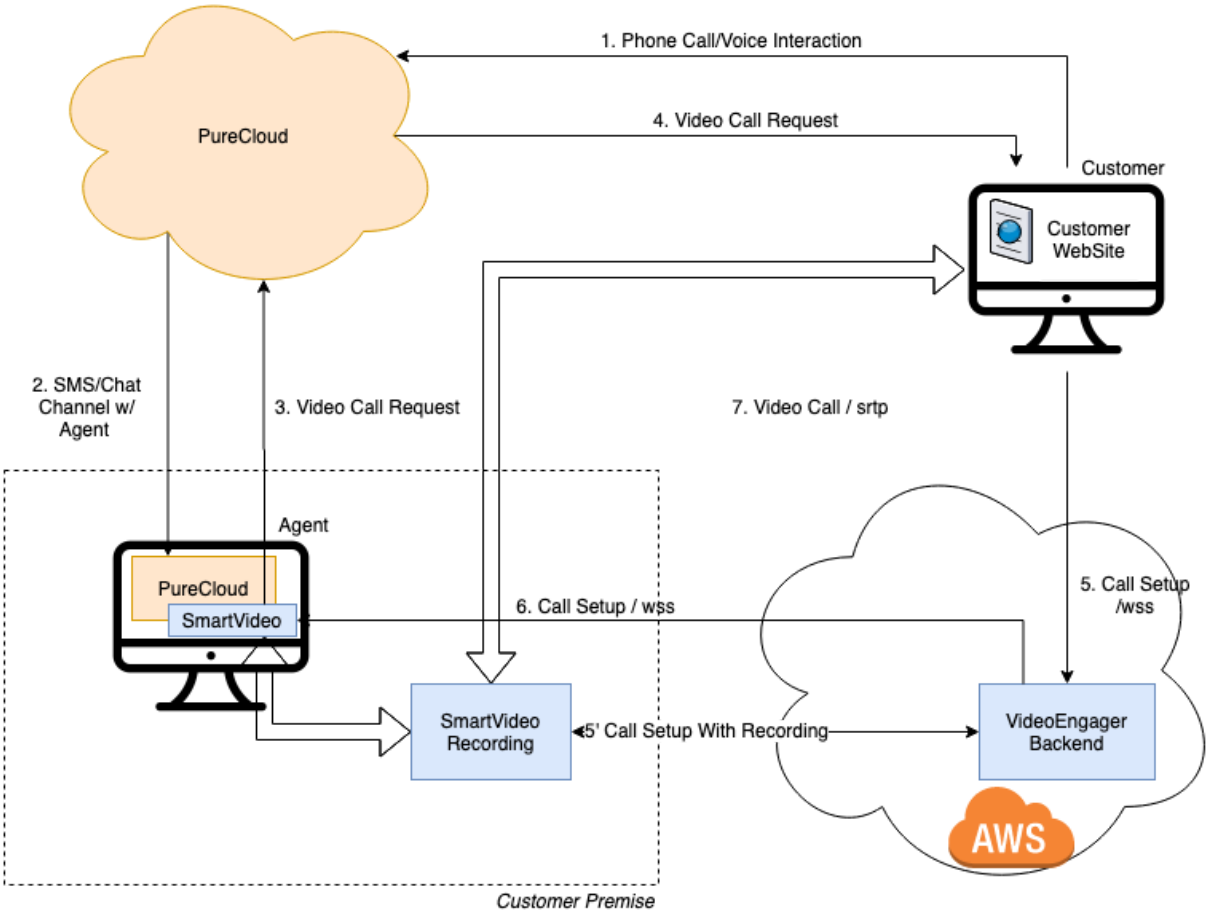


For Customers

All a customer needs is a browser. Customers browsing the company website can either escalate an existing Genesys web-chat to a SmartVideo video call or go straight to video, calling a company representative. Customers are not required to perform installations in order to use audio/video communication. The SmartVideo web widget supports equally well desktop and mobile browsers. Customers can choose to call with no camera or select the camera they want to use so they can show their face, a product experiencing a technical issue or a product for sale on the showroom floor.



3. Solution Architecture



This diagram explains in more detail how SmartVideo integrates with Genesys Cloud. The consumer starts an interaction with an agent via voice interaction.

Agent initiates/generates a unique video link and sends it to the user through Genesys Cloud via SMS or EMail. Then both sides are able to start video sessions. The agent is notified in Genesys Cloud integration if a user enters video session first. Video Link is valid for 30 minutes by default, this time can be customized to suit your needs. The Video Call is finalized only by

the Agent, if the call drops the customer can re-open the link at any time, even from another device.

The agent and the customer The SmartVideo Solution negotiates a connection between the consumer’s web browser and the agent’s workspace. Once the call is set up, the actual audio/video media flows directly between the consumer’s endpoint and the agent’s device.To implement optional call recording, SmartVideo employs a dedicated recording server and channels the audio/video traffic through it.

4. Security

The SmartVideo App does not store or retain any user information or credentials. SmartVideo is built on WebRTC technology which is encrypted and very secure. Any information that is stored would be done so on the Genesys Cloud platform. The Genesys platform meets the HIPAA compliance requirements in the US which is also equivalent to GDPR, so SmartVideo is "compliant" for both HIPAA and GDPR.

More detailed explanation of what SmartVideo does:

- VideoEngager SmartVideo does not store any participant information at any point in an interaction, nor is any participant information transmitted over the SmartVideo network. Any Participant information will be stored in the applicable Genesys platform.

- VideoEngager uses two channels of communication between the clients and the SmartVideo backend – signaling and media signalling Signaling is to facilitate the discovery of the video call participants and media carries the audio and video streams between the participants. Both channels are encrypted.

- For the signaling channel SmartVideo uses SSL with AES-256 bit encryption. This channel only carries IP addresses and codec information to facilitate the establishment of the media channel.

- For media, SmartVideo uses WebRTC, which uses DTLS-SRTP. DTLS-SRTP exchanges keys over the media plane, rather than the signaling plane.The significance of this is that an SRTP media channel has no need to reveal the secret encryption keys through an SDP message exchange, as is the case with SDES. The WebRTC specification asserts that WebRTC implementations are required to support DTLS-SRTP for key management. Moreover, it is specified to be the default and preferred scheme, and there is no provision for other key management schemes to be implemented. In other words, other schemes may or may not be supported at all. If an offer or "call" is received from a peer advertising support for both DTLS-SRTP and SDES, DTLS-SRTP must be selected - irrespective of whether the signaling is secured or not. SmartVideo does not store encryption keys and does not store user’s credentials.

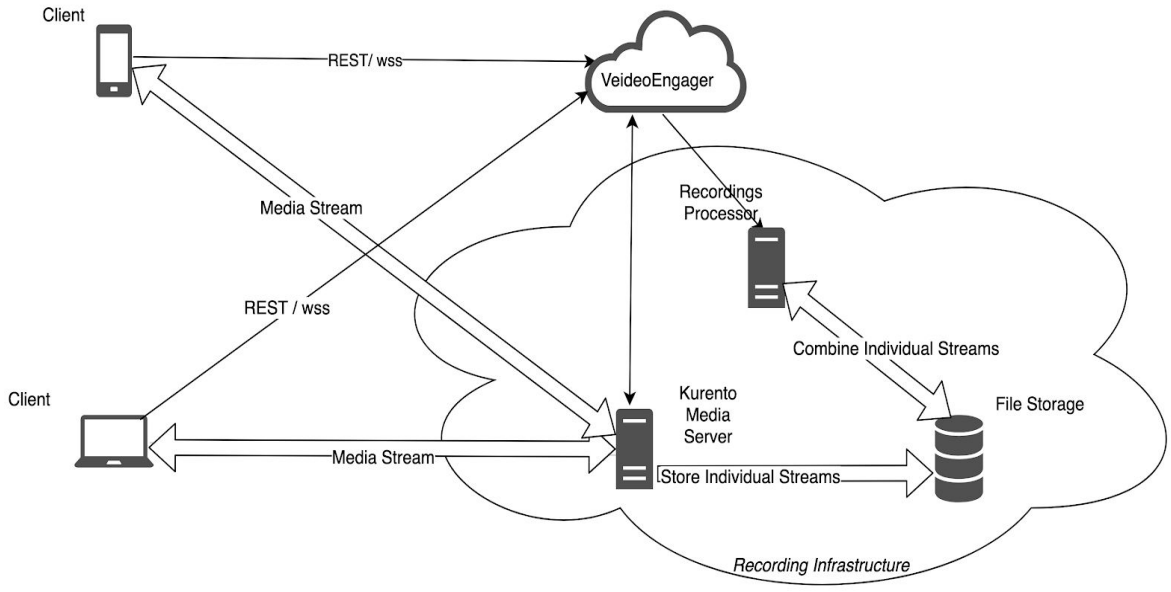
5. Recoring

Overview

In a case of recording deployment, streams from customer and agent are routed through a Media Server, which captures and records them to a dedicated file storage.

Recordings Processor does post-processing of the recorded media streams, by combining them into a final file.

Media Server and Recordings Processor share common File Storage, mounted in both servers. In the case of on premise deployment of the Recording Infrastructure, File Storage should be provided by the customer.



Recording Architecture

On premise customers are configured by VideoEngager to use its own recording infrastructure.

Recording integration

The integration for premise based or cloud based recording is identical. The video recording servers are installed on the end user (customer) premise or in an end user private cloud or Smartvideo AWS cloud. The end user recording configuration is done in the SmartVideo AWS cloud and transferred to the end user servers. The configuration consists of:

- Enablement of recording in SmartVideo
- Addresses of the videorecording servers
- Type of recording - mandatory all calls are recorded or optional. Optional calls are agent controlled, agent decides what and when to record during a video call.
- Recording URL, optionally used to access video recordings via web UI.

Recording access and review

The Recordings can be viewed from the SmartVideo reports application within Genesys Cloud. The second alternative is to retrieve recordings as a file through an end user controlled process from the on-premises storage device.

Each video call can have many video recordings associated with him. Genesys Cloud SmartVideo Reports reports page has additional section with a video recordings information, that includes:

- ID - each recording is assigned a unique ID.
- Type - can be either Video or Screen Sharing
- State – after a call is done, the recording is enqueued for mixing, status reflects stages in recording processing. Processing time (availability) is affected by the length of the recording.
- URL - optional URL pointed to the on premise servers or cloud server where the recording is located.
- Start - start time of the recording in the user timezone
- End - end time of the recording in the user timezone
- Duration - duration of the recording
- MIME - Type of the recording can be H.264 or Webm
- Media - A final media file with a unique name.

Recordings

ID:	d4232ab0-e511-11e9-9ad0-ff6d355f9cd4
Type:	video
State:	finished
URL:	https://prod.leadsecure.com/api/recordings/play/d4232ab0-e511-11e9-9ad0-ff6d355f9cd4
Start:	02.10.2019 15:40:34 +0300
End:	02.10.2019 15:40:47 +0300
Duration	00:00:13
MIME:	video/webm
Media:	d4232ab0-e511-11e9-9ad0-ff6d355f9cd4.webm

Recordings Section in SmartVideo Reports

Recorded files retention

The administration for the retention policies is EndUser/Customer controlled. The storage is premise/or private cloud based, SmartVideo/Genesys has no access to the recordings. End User/Customer will apply their own retention policies. It should include how long files are stored, when they are archived or removed. This can all be administered by the End User/Customer Genesys Cloud/SmartVideo Administrator.

Network requirement

There are two types of traffic, Media Streams over UDP and controlling traffic between videoengager cloud and recording deployment on premise.

For the networking use following table to allow traffic to on-premise solution:

Service	**Protocol**	**From**	**Port(s)**
Media Server (control)	tpc	videome.leadsecure.com	https [443]
Media Server (stream)	udp	Internet (customer facing)	55000:65535

Recording Processor (control)	tcp	videome.leadsecure.com	https [443]

6. User Data stored in VideoEngager cloud

VideoEngager stores basic information for the customer sessions and VideoCalls. Complete data samples and schema are in a separate document, here we provide an outline of the data.

Call Data Record

Information about the call includes contains:

- Start time
- Duration
- Talk time
- Agent Email
- Agent Name (if available)

Session Data Record

Information for every session agent and customer contains:

- IP Address
- User Agent (Browser information or Mobile App version)
- Session start
- Session Duration