Seguridad

Servicios de videollamada

GENESYS™

Interactive **Powers**

Conecta, Reinventa, Mejora...
Tus Contact Centers
Tus Canales Digitales
Tus Equipos

Servicios gestionados en AWS

Interactive Powers ofrece un entorno de servicios de alojamiento en la nube en AWS con una capa de soporte técnico que garantiza transparencia, control y eficiencia para nuestros clientes y socios. Utilizamos un servicio de monitoreo especial para controlar la mayoría de los indicadores ITSM por región, nodo o servicio, dando una garantía de tiempo de actividad del 99,99% y trazabilidad de todas nuestras operaciones en la nube. Esto permite a nuestros clientes o socios tecnológicos disponer de una experiencia segura, confiable, y eficiente al utilizar nuestra CPaaS con Genesys Cloud.

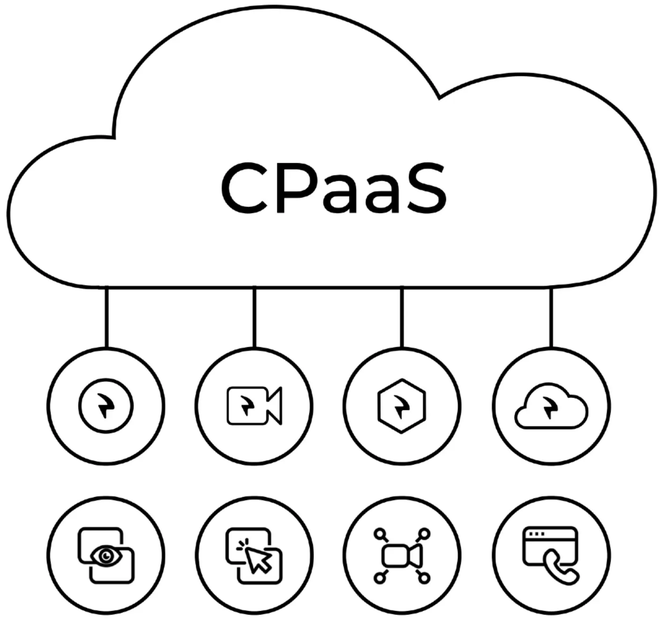
aws partner network

Standard

Technology Partner

AWS Technology Partner

Interactive Powers es uno de los primeros usuarios y socios de Amazon Web Services. Nuestra relación con Amazon nos permite ayudar a nuestros clientes a aprovechar las ventajas del ahorro de costes, la elasticidad y el rápido aprovisionamiento de la infraestructura como servicio (IaaS).



Gestionamos globalmente servicios en la nube en todas las regiones

Somos una empresa cercana en un mundo global.

Prestamos nuestros servicios CPaaS y con seguimiento local en todos los países.

powered by aws

Plataforma de canales para realizar videollamadas transaccionales con colaboración web en navegadores web modernos, dispositivos móviles y quioscos interactivos.

Video RTC

Plataforma

Saber más

powered by aws

Plataforma de grabación de videollamadas confiable y escalable que garantiza los más altos niveles de de calidad y seguridad en la nube para los Contact Centers de Genesys.

Video REC

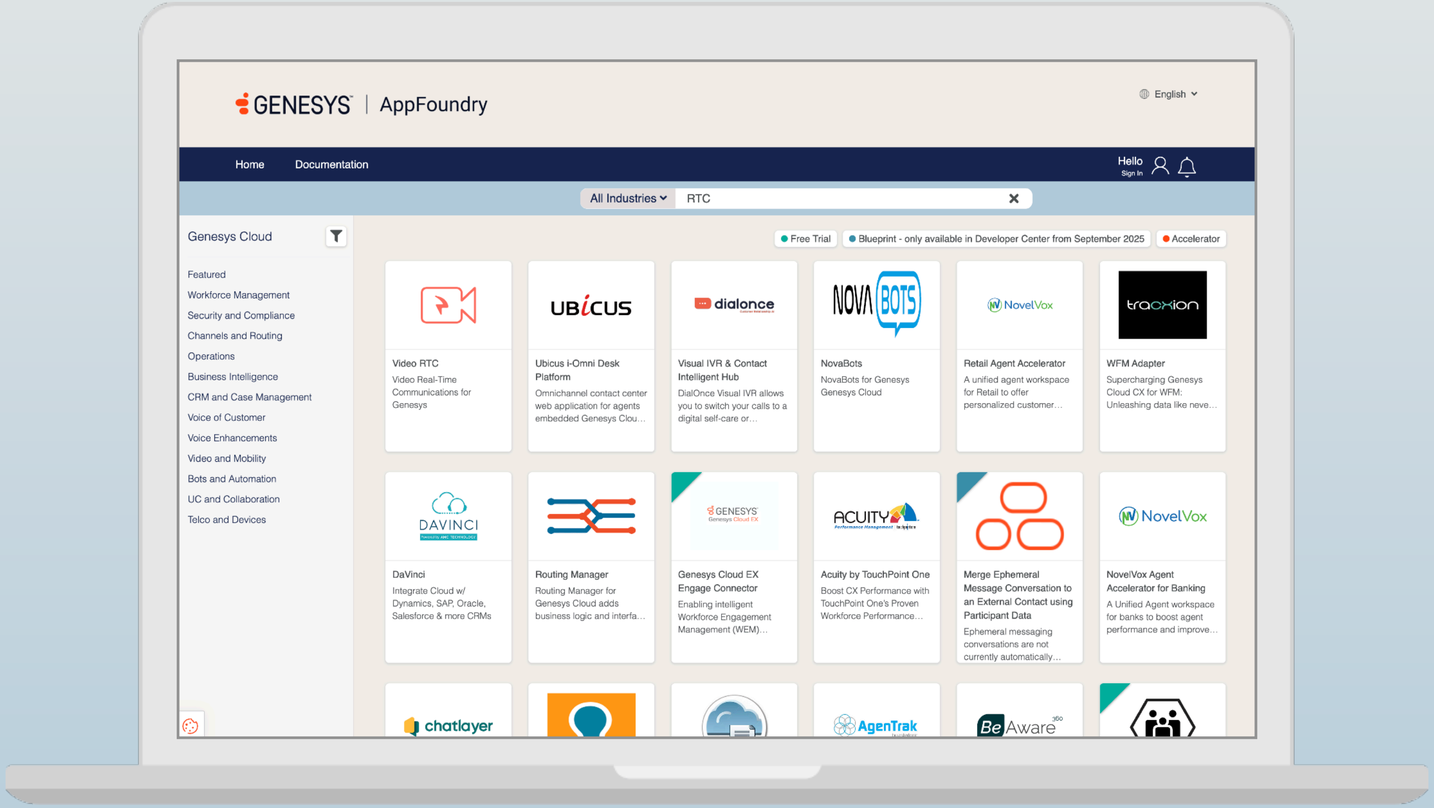
Plataforma

Saber más

powered by aws

AppFoundry Premium Partner

Video RTC is available at Genesys Marketplace since 2019!



Seguridad

Protección de los canales de vídeo

Garantizar la seguridad de las videollamadas y las grabaciones forma parte de nuestras plataformas y estándares.

Protección de los canales de voz

Garantizar la seguridad de las llamadas telefónicas y de voz, así como un proceso crítico de nuestras principales tecnologías, normas y operaciones.

Protección de la grabación y almacenamiento

La grabación y el almacenamiento también están sometidos a políticas específicas de seguridad y supervisión en la nube.

Siete principios de seguridad

Cifrado de extremo a extremo
Todas las comunicaciones en tiempo real impulsadas por nuestras plataformas están cifradas al 100% con protocolos estándar. Esto incluye tanto las conexiones WebRTC peer-to-peer como el procesamiento híbrido de transcodificación.

Dedicated STUN / TURN
Proporcionamos nuestros propios servicios STUN / TURN para cada región, lo que permite que sus comunicaciones de vídeo estén debidamente respaldadas y sean fiables. Estos servicios también pueden desplegarse como IP dedicados.

Condiciones de seguridad de AWS
Ejecutamos toda nuestra infraestructura IT sobre AWS (Amazon Web Services) asegurando las condiciones de cobertura y gestión de seguridad más altas del mercado. Puedes confiar en un 99,99% de uptime para tus servicios.

ITSM & monitoreo
Las herramientas de AWS no son suficientes para garantizar un control y supervisión perfectos de los servicios específicos de IVR, RTC, ACD y RTC, por lo que ofrecemos capacidades adicionales de ITSM y supervisión diseñadas para todas estas plataformas.

Certificados AES de 256-bit
Todos nuestros certificados de seguridad tienen una longitud mínima de 256 bits, lo que garantiza la máxima calidad para sus comunicaciones. También permitimos la activación privada y la renovación automática.

Tráfico SRTP
De acuerdo con sus recomendaciones de seguridad podemos activar el cifrado SRTP sobre SIP. Puede activarlo cuando conecte sus troncales VOIP a nuestras plataformas y servicios.

Grabación indirecta
Activar la grabación de voz o vídeo no es directamente operativo por razones de seguridad y privacidad. Así que puedes decidir qué tipo de grabación se ejecuta en tu plataforma siguiendo tus políticas de seguridad.

Privacidad

La privacidad de tus datos es nuestra prioridad

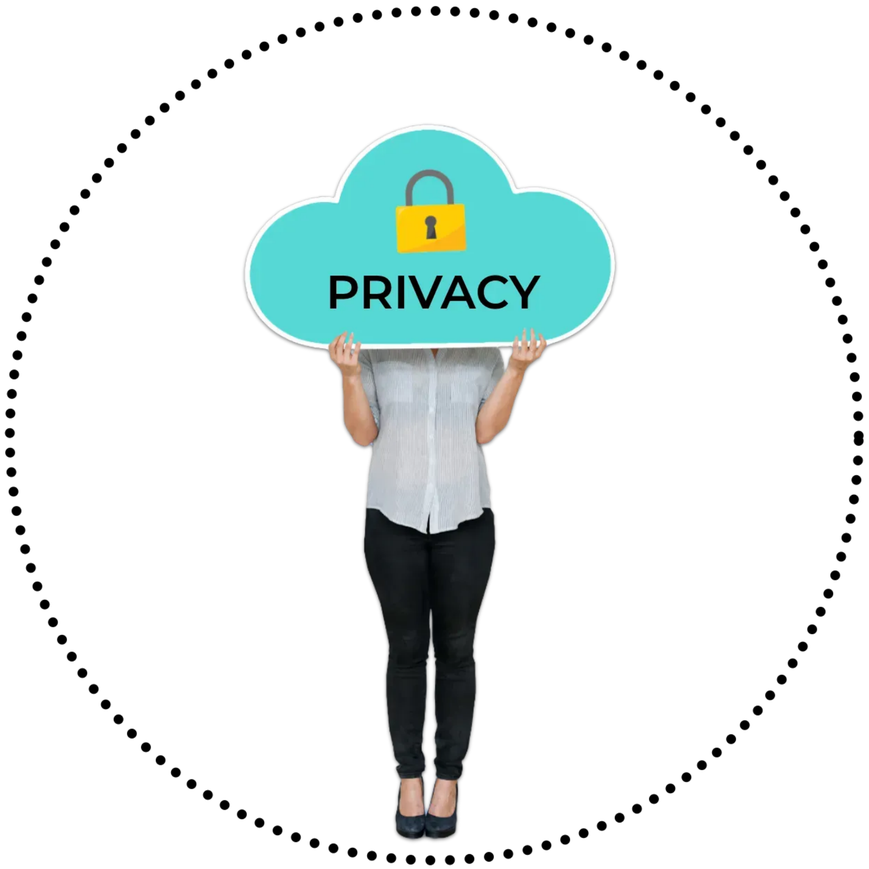
No hacemos negocio con tus datos y tus comunicaciones. Tu privacidad es absolutamente tuya.

Asignación de almacenamiento de datos

Habilitamos condiciones especiales que garantizan que tus datos estén debidamente bajo tu asignación regional.

Protección de datos paso a paso

Ofrecemos opciones específicas de activación para asignar tus llaves, cuentas y unidades de almacenamiento dedicadas.



Siete principios de protección de datos

Gestión mejorada del centro de datos
Operamos todos nuestros sistemas dentro de AWS para garantizar procesos seguros y avanzados. Utilizamos herramientas de automatización, monitoreo y gestión potentes para administrar eficazmente todos los centros de datos.

Seguridad probada de productos
Desarrollamos todos nuestros productos con severas medidas de seguridad para proteger la privacidad de sus datos. Todos los accesos utilizan nada menos que certificados de 256 bits para encriptar comunicaciones y protocolos.

Disponibilidad y resiliencia
Nuestros servicios en la nube están diseñados para ofrecer la máxima escalabilidad, disponibilidad y resistencia, con el fin de minimizar las interrupciones. Todas las soluciones cuentan con recursos regionales y supervisión.

Los datos pertenecen a nuestros clientes
Proporcionamos una Plataforma de Comunicación como Servicio (CPaaS) utilizando nodos dedicados que no comparten el acceso entre sí, salvaguardando la privacidad de sus datos y la seguridad de su negocio.

Seguridad reforzada de las aplicaciones
Nuestro objetivo de reforzar la seguridad de las aplicaciones está orientado a impedir el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de la aplicación y sus datos.

Seguridad de la red
Todos los sistemas están bajo vigilancia de nuestra seguridad de red para proteger la confidencialidad, integridad y disponibilidad. Estos controles siguen evolucionando con conocimientos específicos sobre cortafuegos, SSH, SSL, TLS, VPN...

Gestión de copias de seguridad
Todos nuestros servidores y servicios críticos están conectados a procedimientos de backup de varias semanas o meses. Todas estas operaciones se realizan en condiciones de seguridad de AWS para garantizar la restauración más rápida en cada región.

Monitoreo

Interactive Powers extiende los servicios de alojamiento de AWS con su propio sistema de monitoreo, asegurando transparencia, control y eficiencia para nuestros clientes y socios.

Nuestro servicio de monitoreo propio supervisa la mayoría de los indicadores ITSM por región, nodo y servicio, garantizando un tiempo de actividad del 99.99% y ofreciendo trazabilidad completa de todas nuestras operaciones en la nube.

Esto asegura que nuestros clientes y socios disfruten de una experiencia confiable, eficiente y transparente al utilizar nuestra CPaaS.

Servicios CheckMK

Interactive Powers dispone de paneles avanzados de monitoreo en tiempo real de acuerdo con los requisitos ITSM de cada nodo. Un servicios en la nube ofrece transaparencia para los equipos de TI y los gestores de negocios.

Estándares y Certificados AWS

Certificación ISO 27001 en seguridad de la información

> https://aws.amazon.com/es/compliance/iso-27001-faqs/

Certificación ISO 27017 (controles de seguridad para servicios en la nube)

> https://aws.amazon.com/es/compliance/iso-27017-faqs/

Certificación ISO 27018 (protección de información personal en la nube)

> https://aws.amazon.com/es/compliance/iso-27018-faqs/

SOC 1

SOC 2

SOC 3

ISAE 3402

PCI

MPAA

FISMA

ISO27001

HIPAA

DISASTER RECOVERY PLAN (DRP)

External Paper for Clients & Partners

Company Name: **Interactive Powers LLC**

Address: 50 Minorca Ave, #1406

ZIP / State / City: FL 333134 Florida / Coral Gables (Miami)

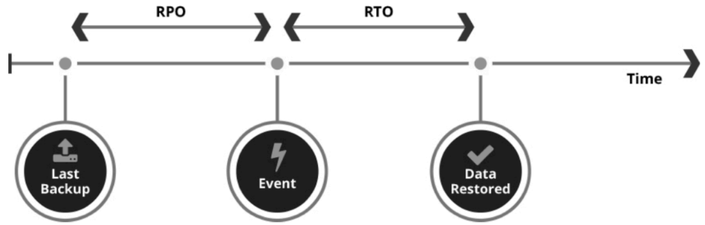
Country: United States of America

Table of Contents

Purpose....3
Versions & Changes....3
1. Introduction....4
DR Managing Staff....5
Notification Network....5
2. Scope....6
3. DR Teams & Responsibilities....7
Disaster Recovery Lead....7
Disaster Management Team....7
Network Team....7
Servers Team....7
Applications Team....8
4. Data & Backups....8
5. Restoring IT Functionality....9
6. IT Systems & Network....11
7. Severity One System....14
8. Plan Testing & Maintenance....16
Maintenance....16
Testing....16
9. Recovery Completion Form....17

7. Severity One System

When determining the right Disaster Recovery services, there are three aspects to consider:



- Source of System
- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)

Source Of System

Whether your system is onsite,

Recovery Point Objective (RPO)

How current our data is at the recovery site.

EU IVRPOWERS CPaaS

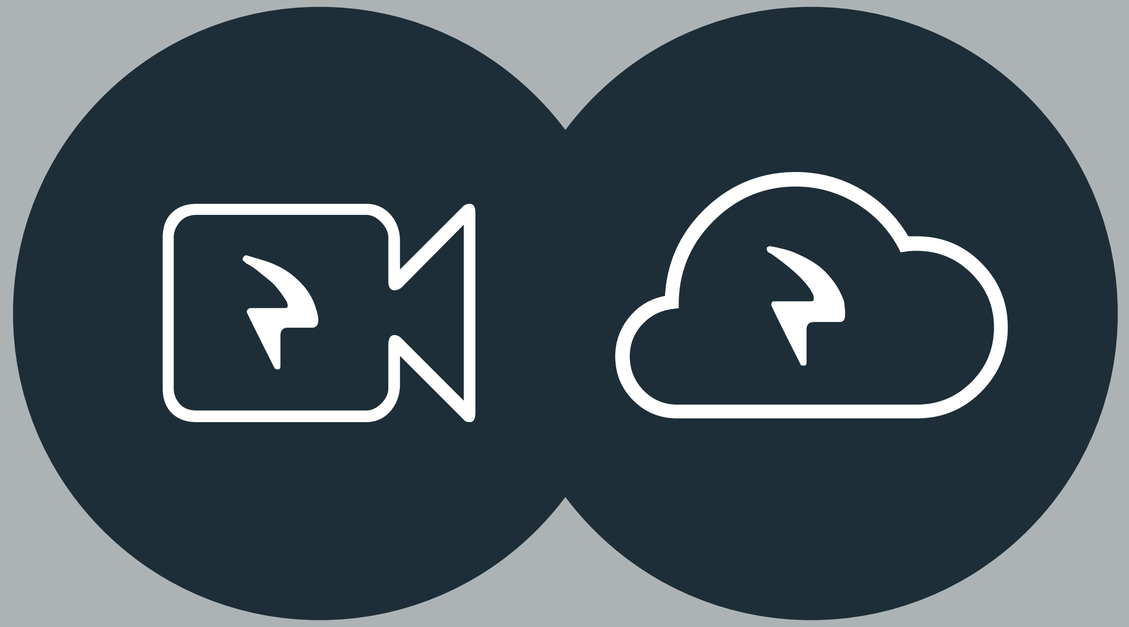
Minimun	Standard	Max. Storage	Method
1 Day	7 Days (Week)	14 Days	AWS Backup
1 Month	2 Months	1 Year	Directory Sync

US IVRPOWERS CPaaS

Minimun	Standard	Max. Storage	Method
1 Day	7 Days (Week)	14 Days	AWS Backup
1 Month	2 Months	1 Year	Directory Sync

Consultas

Aspectos de Seguridad



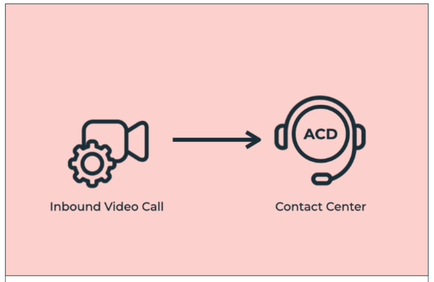
Interactive **Powers**

Video RTC

Protocolo SPLIT

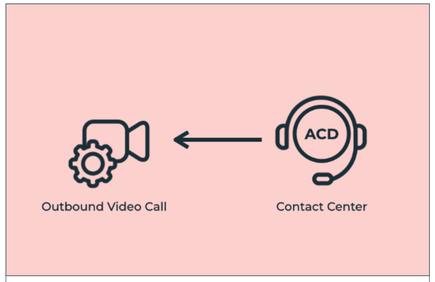
Las plataformas Video RTC operan con un protocolo especial llamado SPLIT que permite conectar canales de video comunicación transaccionales a cualquier sistema de Contact Center. Existen tres tipos de modos operativos: **SPLIT Forward** (Inbound) videollamada con distribución entrante / **SPLIT Reverse** (Outbound) videollamada de agente a usuario / **SPLIT Scheduled** (Outbound) videollamada programada con fecha de caducidad.

El protocolo SPLIT está formado por enlaces SIP / WebRTC combinando de forma sincronizada ambas tecnologías y permitiendo una conexión hibrida basada en estándares que es compatible e interoperable con la mayoría de Contact Centers y también plataformas CCaaS como Genesys Cloud.



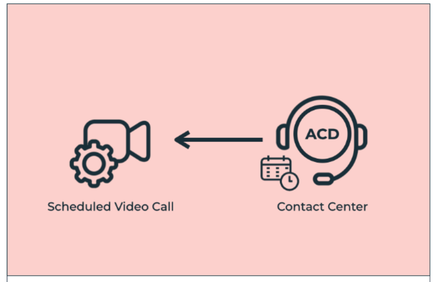
SPLIT Forward

Enrutar automáticamente las videollamadas entrantes a los agentes disponibles.



SPLIT Reverse

Realizar videollamadas salientes desde un agente hacia un usuario de Internet.



SPLIT Scheduled

Programar videollamadas desde cualquier agente para una tarea negociada a un usuario.

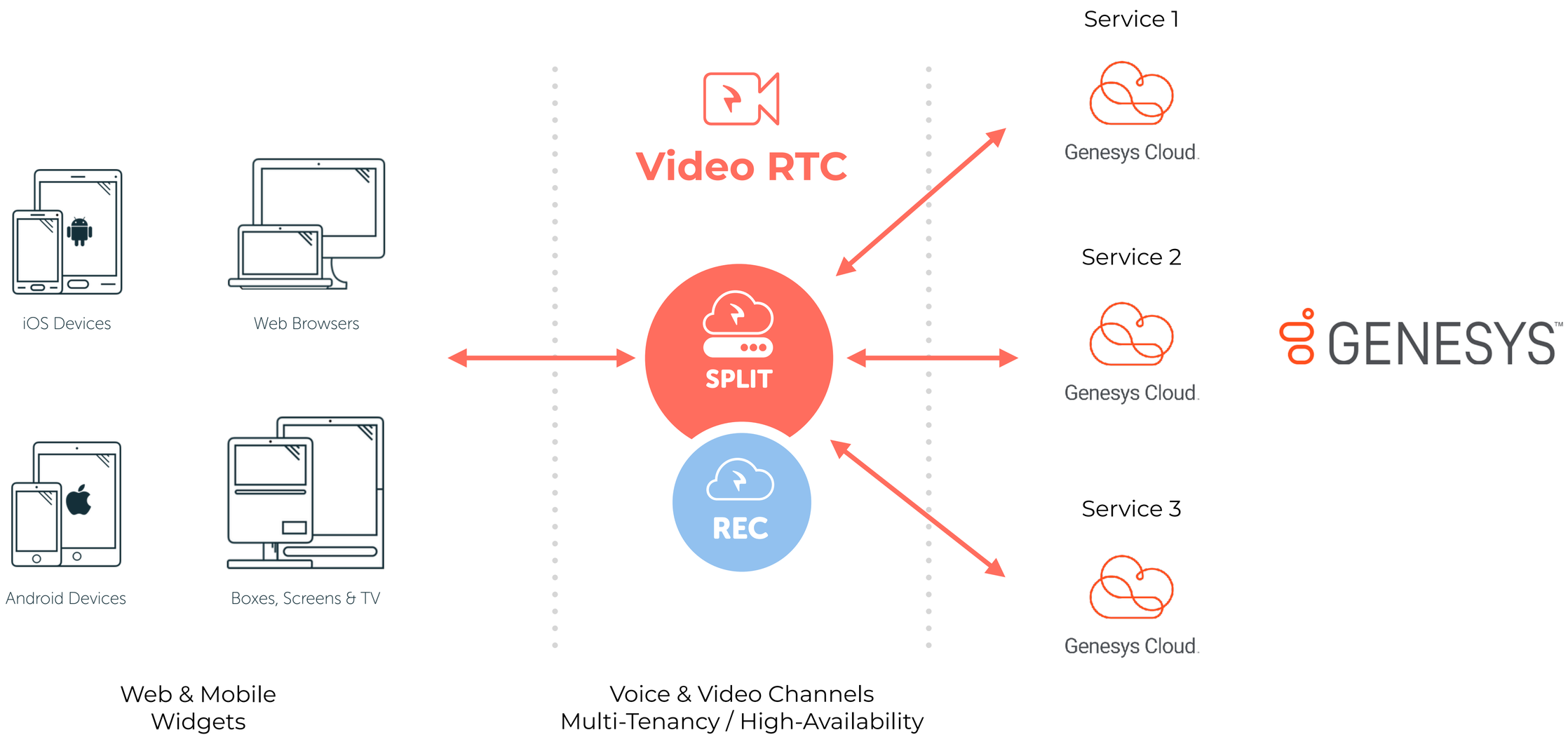

Service 1
Genesys Cloud
Video RTC
Service 2
Genesys Cloud
SPLIT
REC
Service 3
Genesys Cloud
iOS Devices
Web Browsers
Android Devices
Boxes, Screens & TV
GENESYS
Web & Mobile
Widgets
Voice & Video Channels
Multi-Tenancy / High-Availability

Diagrama: **SPLIT Reverse**

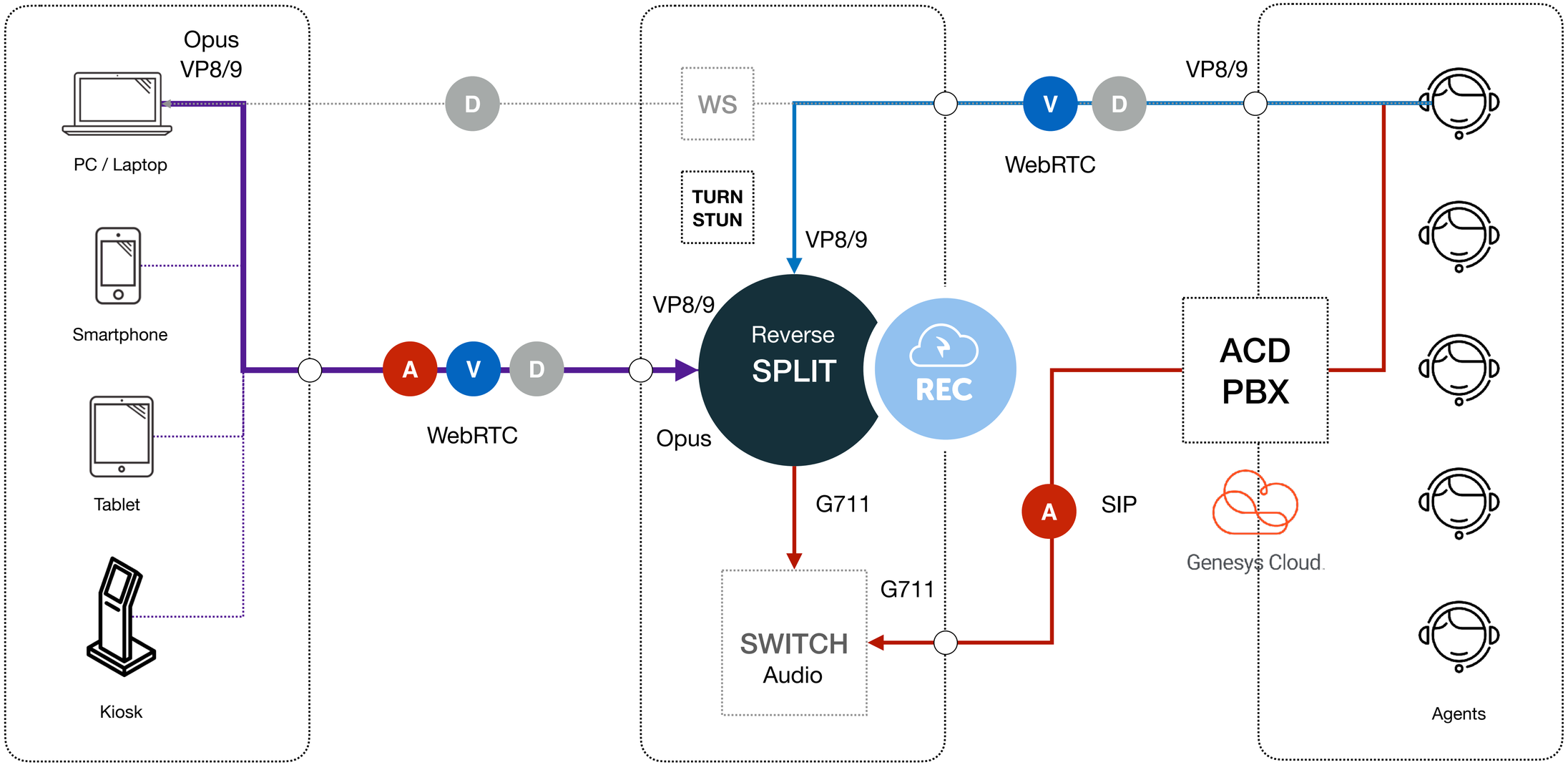
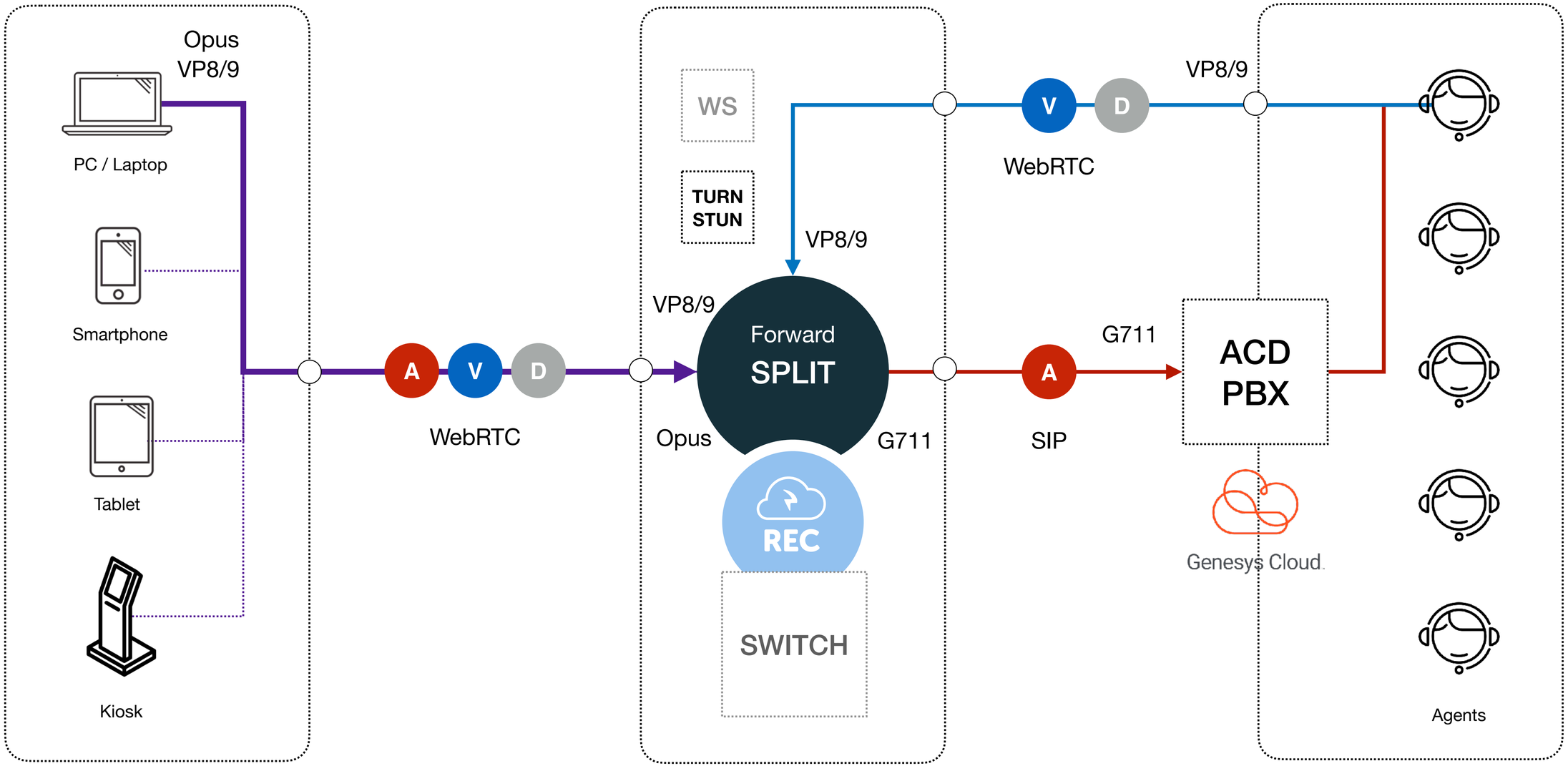


Diagrama: **SPLIT Forward**



Video RTC

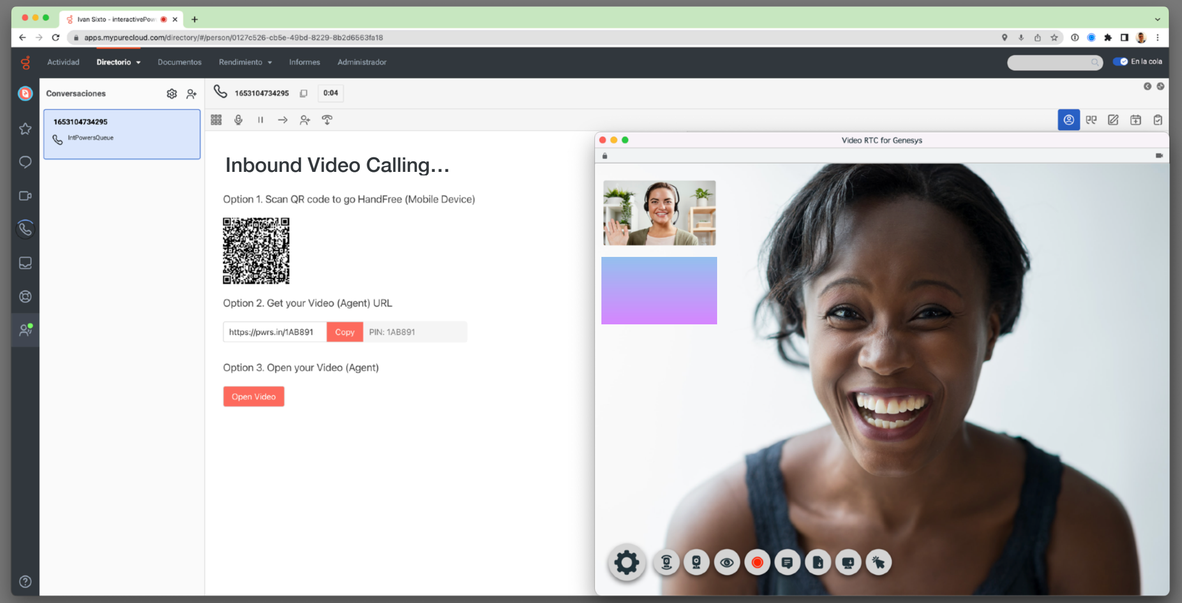
Trazabilidad SPLIT

El protocolo SPLIT opera con Genesys Cloud a través de dos tipos tecnologías: WebRTC/ JS y SIP. Las videollamadas disponen de la misma trazabilidad que las llamadas telefónicas, el protocolo SPLIT produce en Genesys Cloud los mismos registros, grabación, logs facilitando al Contact Center la obtención de reportes con el mismo nivel de detalle y formatos.

Además de la información convencionales de una llamada (telefónica), las videollamadas transaccionales SPLIT incorporan parámetros de entrada y metadatos que Genesys Cloud puede leer usando el identificador único SPLIT ID. Estos datos pueden ser utilizados para levantar información hacia un sistema de Backoffice como un CRM, ERP, o cualquier tipo de script para los agentes de atención.

High Performance Video Calls require at least the same transactional functions as Phone Calls.

GENESYS™

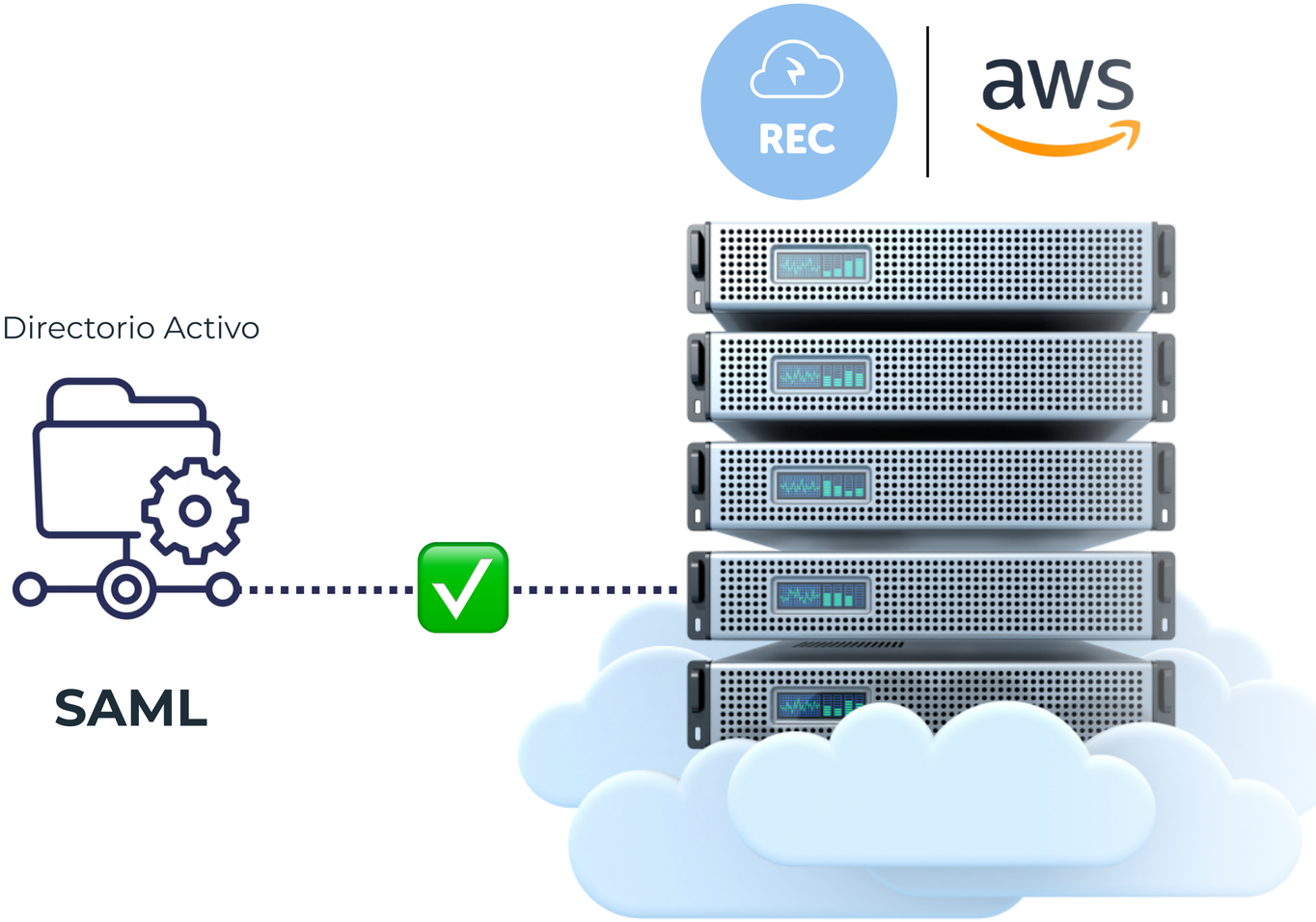


Video REC

Directorio Activo

Nuestro entorno de grabación Video REC permite conectar servicios de Directorio Activo de clientes en la configuración CPaaS estándar por regiones (EU, US,...).

Para entornos de Directorio Activo específicos del cliente, la configuración se implementa mediante el protocolo SAML 2.x. Esta autenticación separada por Directorio Activo puede mantener reglas adicionales compatibles con REC, como el filtrado por rangos de IP para los usuarios.



Cloud Ready & High Availability by Region

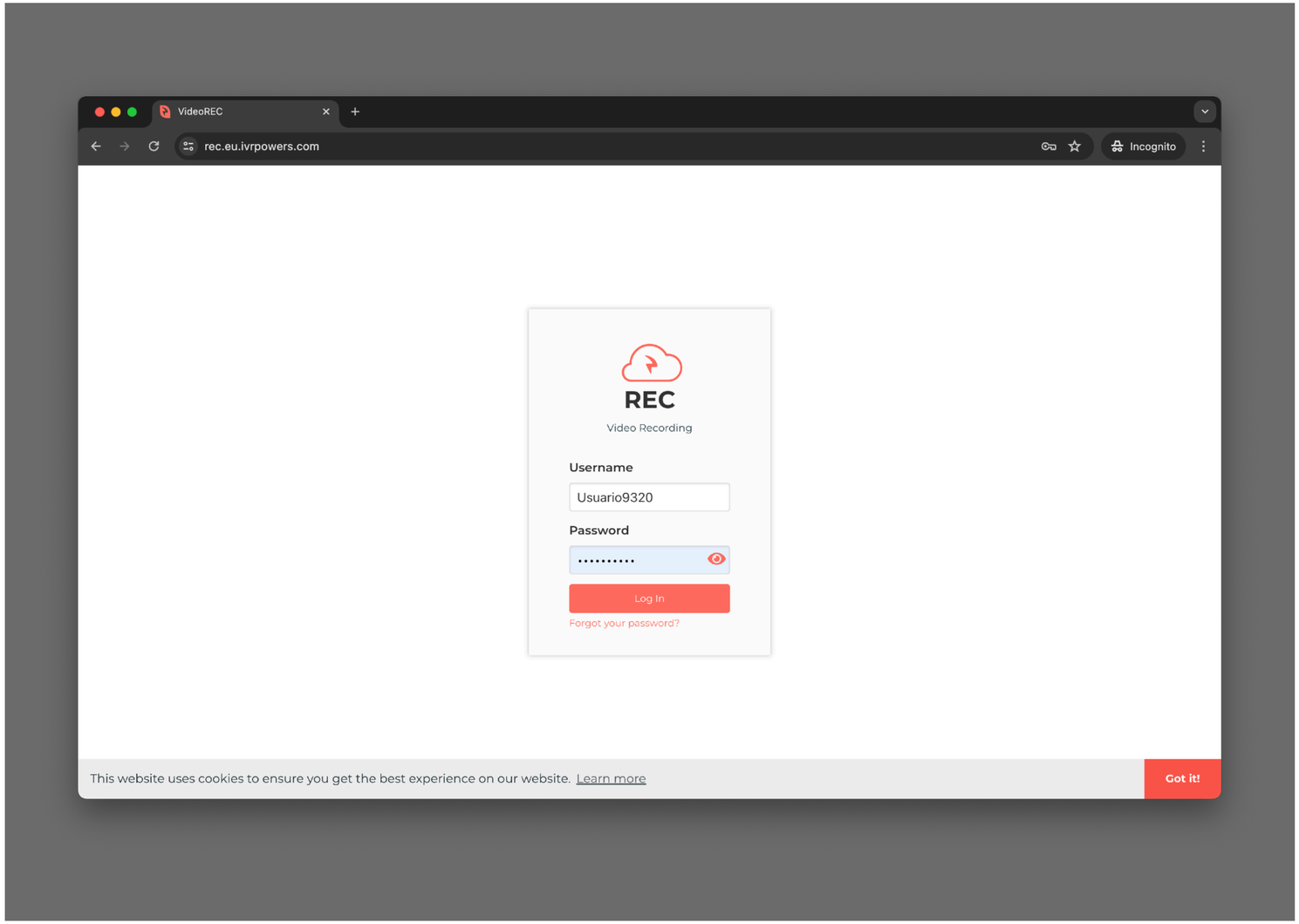
Unlimited Elastic ECS Processing Nodes Capacity

Video REC

Acceso Login

El acceso al sistema REC se realiza con cuentas nominales en cada servicio de un cliente. Este sistema dispone de una gestión de usuarios con posibilidad de actualización de contraseña mediante correo electrónico. Se pueden solicitar 1-n cuentas a las que se pueden asignar \acceso a 1-n servicios de almacenamiento de grabaciones REC / ARC; todas las cuentas de un servicio operan con la misma configuración.

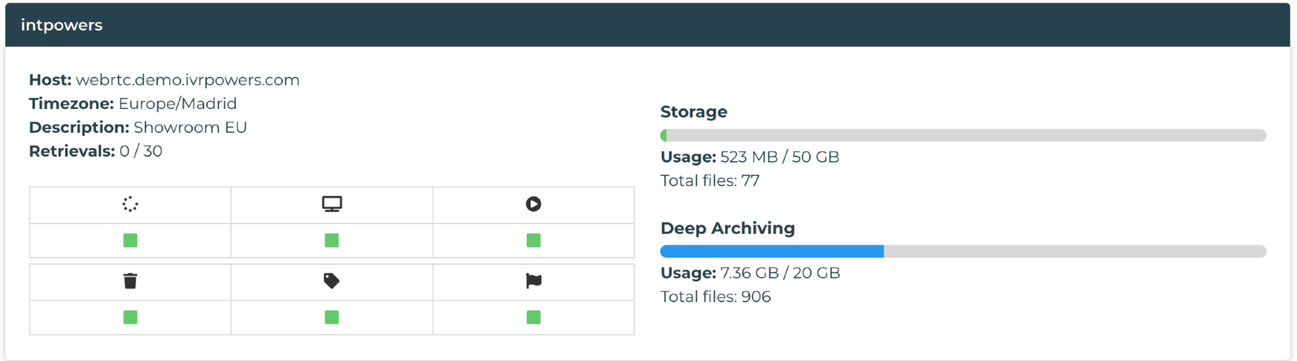
También existe interfaz de autenticación abierta o SSO / SAML externos, esta opción está disponible para directorios tipo Google, Microsoft... El entorno REC es exclusivamente de uso corporativo y reservado a un número limitado de usuarios señalados por reglas de seguridad. No se trata de un sistema que ofrece servicios a nivel de agentes. Por esas razones, la consideración de acceso está controlada por la propia configuración de seguridad de la plataforma REC.



Video REC

Permisos

Los planes de Video REC tienen diferentes permisos para el uso que cada plan de almacenamiento requiere. Cada servicio de grabación puede elegir los permisos indicados, la activación de grabación con procesamiento HD está reservado al plan tipo 3. El plan tipo 1 es limitado a conservar pistas en bruto no permite auto-procesamiento y solo mantienen grabaciones RAW sin su versión MP4. El plan 2 graba en modo SD y realiza un procesamiento automático MP4, es el más utilizado para la gestión de un Contact Centers que necesitan visualizar rápidamente las conversaciones grabadas con imagen y sonido. Por último, se puede destacar que existe un permiso especial de borrado que solo se activa a petición del cliente; por defecto no está activo. Pueden verificar, todos los permisos atribuidos de cada servicio activo en el dashboard de REC.



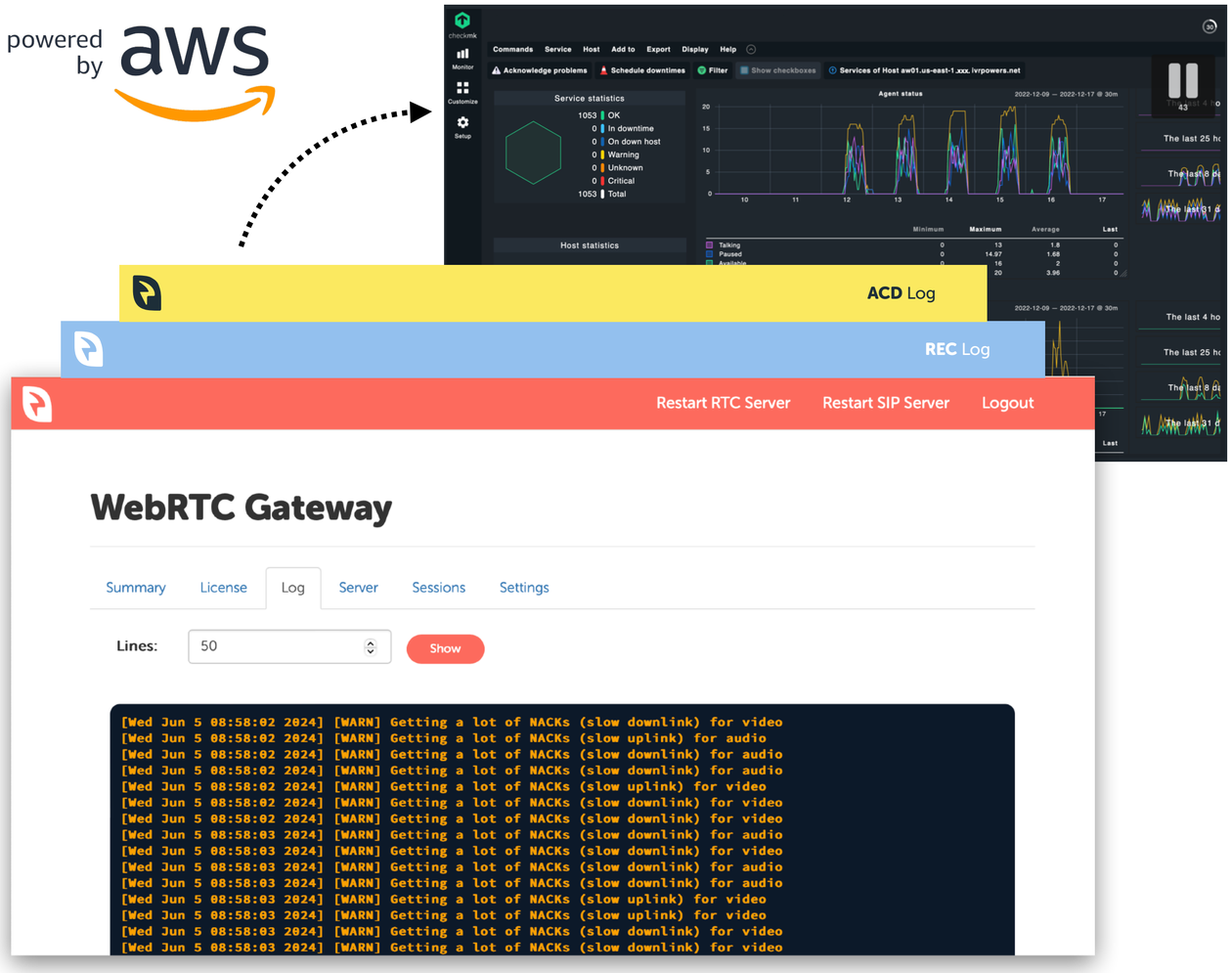
- **Auto-processing** Procesado automático MP4 de las grabaciones
- **HD Quality** Permiso procesado en HD (plan tipo 3)
- **MP4 Player** Posibilidad de previsualización MP4
- **Borrado** Autorización de borrado de registros
- **Metadata** Visualización de metadatos de videollamada
- **Flags** Marcadores de auditoria de grabaciones (Flags)

Video REC

Logs de Acceso

Todas las plataformas de Interactive Powers disponen de servicios avanzados de Logs. La orientación de los mismos es el control de eventos internos del sistema y la detección de errores, fallos, flags, acciones, avisos,... Por razones de seguridad, estos Logs no muestran contenidos de servicio, y tampoco son accesibles desde el exterior de los nodos de cada región.

El formato de Logs es específico a cada tipo de plataforma, para el caso de Video REC, no existe acceso externo, estos incluyen eventos compartidos a nivel ECS (AWS). La entrega de un registro determinado debe realizarse bajo petición para poder filtrar los eventos solicitados de un servicio (por ejemplo: el registro de login de uno o varios usuarios o cualquier traza específica). Por último, indicamos que no se permite conectar o exponer los Logs de nodos operativos a un sistema exterior de ningún cliente, si bien colaboramos en activar trazas determinadas o entregar esos datos de registro bajo requerimiento.



Video REC

Post-Processing / Exportation

Las plataformas Video REC permiten exportación programable y automática de grabaciones acorde a políticas de gestión avanzada de datos y tiempos de almacenamiento determinados.

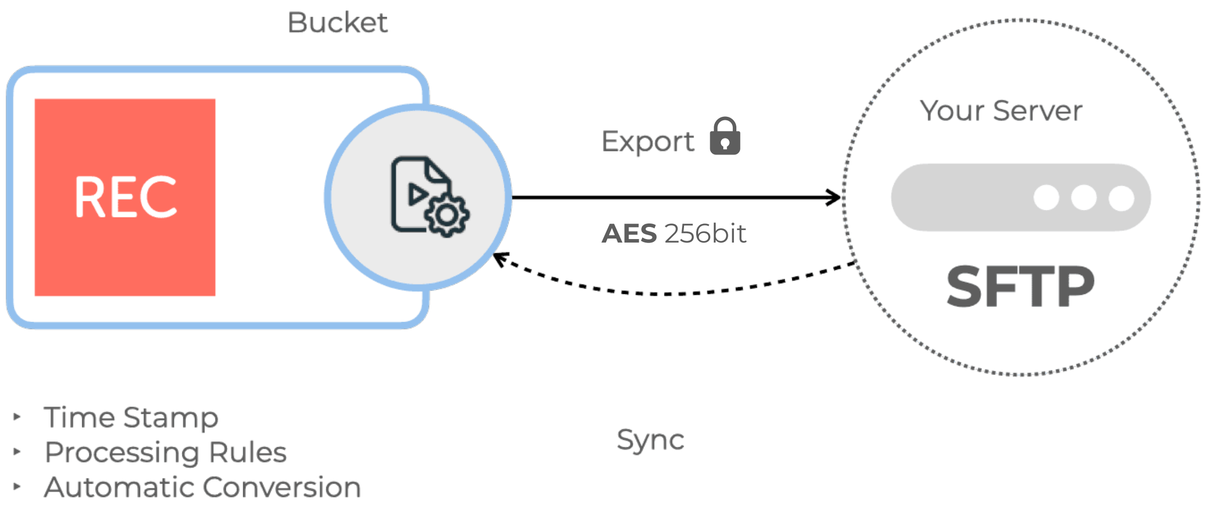
Las funciones de Post-Processing corresponden instrucciones de tipo script que se ejecutan al recibir un registro de grabación desde los sistemas Video RTC. Algunas prestaciones de esta funcionalidad de Post-Processing permite programar procesos complejos para fechas, periodos, o tiempos de almacenamiento:

- Borrado automático

- Exportación SFTP automática

- Archivo automático

- Envío automático de Copias de seguridad



SSH

amazon SFTP

Video RTC

Interfaz Usuario - Agente

El interfaz de usuario - agente es un interfaz web-responsive programado con elementos javascript, websockets y HTML5. Las funciones principales están regidas por una librería **videortc.js** que agrupa las funciones principales de comunicación para el interfaz de agente y del usuario. Además de los streams de audio/video, este interfaz incluye según el plan elegido diferentes funciones de colaboración web que permiten agregar a la comunicación cara-a-cara elementos interactivos como **Live Chat** (chat texto avanzado integrado en el canal), **File Sharing** (compartición de archivos), **Dual / Screen Sharing** (compartición de pantalla doble), **Snapshot** (captura de frames de video en alta definición). Además de las funciones anteriores existen funciones de control de las cámaras, micrófonos, altavoces, grabación... y control de presencia con identificación del agente, fondos de pantalla personalizados. Por último, el interfaz puede usar diferentes tipos de complementos o diseño para adaptarse completamente a su imagen o marca.

Video RTC

Control de Grabación

La grabación puede operarse en diferentes modos:

- Automática sin permitir parar
- Automática permitiendo parar o reanudar en Manual
- Manual permitiendo parar o reanudar

Todos estos modos permiten configurar en cada servicio una política determina de grabación acorde a cada tipo de atención. Si se utilizan varios servicios cabe destacar que cada uno puede tener una configuración diferente.

También es importante considerar que la grabación comienza cuando se establece completamente la videollamada entre el usuario y el agente. El sistema no graba el enrutamiento previo, si bien esta parte se puede grabar a través del trunk SIP de Genesys Cloud.

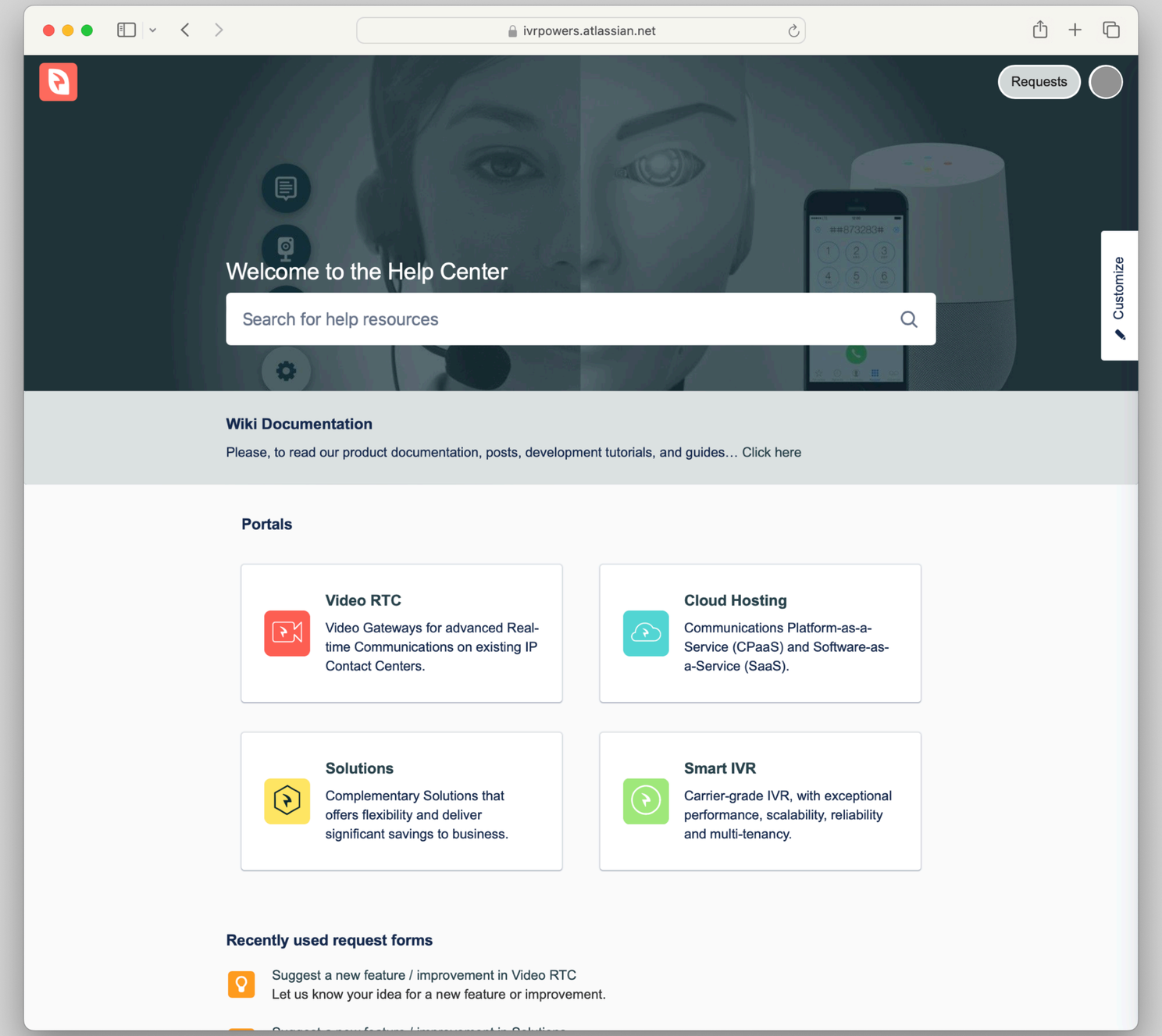
Por ultimo, cabe destacar que se puede transferir la videollamada y que la grabación tendrá varios tramos por cada transferencia realizada.

Help Center

Centro de Ayuda

Este centro de ayuda es para personal técnico especializado encargado de integraciones y/o partners tecnológicos de Interactive Powers. Las consultas pueden agregar el email de personas específicas para compartir tiempos, tareas y contenidos de resolución.

Website

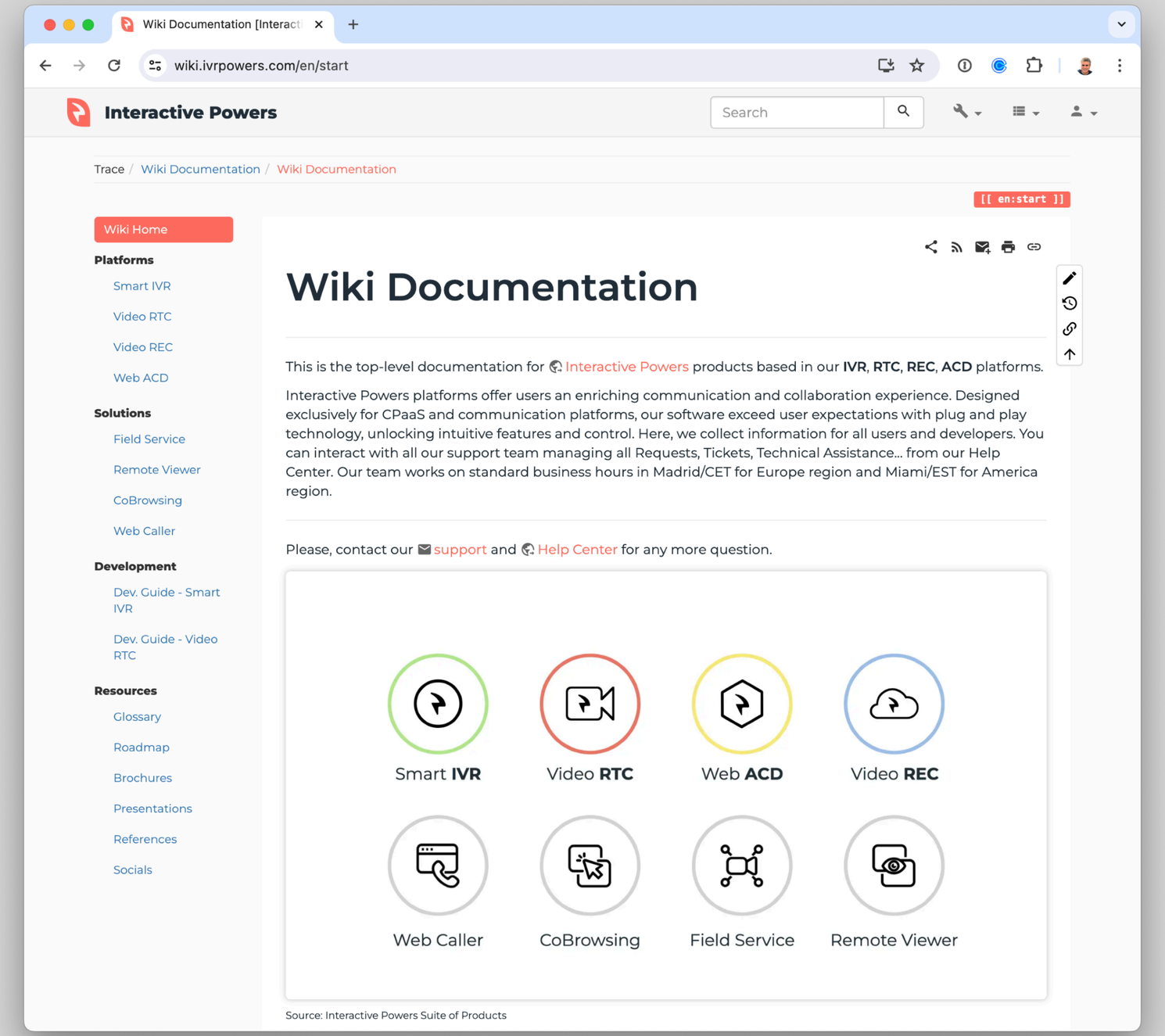


Wiki Doc

Documentación de Partners

Esta documentación esta reservada para personal técnico especializado y/o un partner tecnológico de Interactive Powers que disponen de recursos técnicos para realizar integraciones o tareas de configuración especiales con la suite de nuestros productos.

Website



Interactive **Powers**

Streamline your business communications