FAGOR ELECTRÓNICA

Flow

Manual de configuración Interfaz Simulcrypt

Índice pág

1. INTRODUCCIÓN

La cabecera Ikusi Flow permite encriptar los contenidos para que sean transmitidos de manera segura dentro de la red coaxial o de la red IP de una instalación. Ikusi Flow ofrece la capacidad de comunicarse con un servidor de CAS estándar a través de la interfaz simulcrypt. En este manual se describe cómo es la arquitectura de la interfaz simulcrypt implementada en Ikusi Flow y cómo se usa.

2. DESCRIPCIÓN DE LA INTERFAZ SIMULCRYPT EN IKUSI FLOW

Ikusi Flow permite la interoperación de la cabecera con un sistema de acceso condicional (CAS). La cabecera solo necesita conectividad con el servidor de CAS. Usando el protocolo DVB de Interfaz Simulcrypt (ETSI TS 103 197), las claves, los mensajes de control y los mensajes de gestión son intercambiados entre la cabecera y el servidor de CAS.

Los scramblers están incluídos en los propios módulos de la cabecera (concretamente en los módulos FLOW SEC y FLOW ENC). De esta a manera, no se necesita hardware adicional, reduciendo la complejidad de la instalación.

NOTA: Solo los servicios que sean procesados por los módulos FLOW SEC y FLOW ENC pueden encriptarse. En el caso de los módulos FLOW SEC, el número máximo de servicios que pueden encriptarse con cada módulo es 16, divididos en 2 bloques de 8 servicios (un bloque por cada cadena de señal asociada a cada slot common interface del FLOW SEC).

2.1 Comunicación de Ikusi Flow con servidor de CAS

La comunicación entre la cabecera Ikusi Flow y el servidor de CAS se hace a través del protocolo interfaz simulcrypt. Este protocolo permite el intercambio de mensajes TCP/IP entre ambos sistemas. Por lo tanto, para que esta comunicación sea posible se debe dotar de conectividad a la cabecera Ikusi Flow.

Para ello, se debe conectar el puerto de configuración de Ikusi Flow a una toma de red. El puerto de configuración se encuentra en el módulo FLOW HUB y está identificado con el símbolo 

Debe asegurarse de que la cabecera tenga configurados correctamente los parámetros de red. Para ello, ir a MENÚ→CONFIGURACIÓN→Red. Aparecerá una pantalla como la siguiente:

Haga click en la pestaña CONFIGURACIÓN DE RED. Seleccione la opción DHCP si la configuración de red va a ser proporcionada automáticamente por un servidor DHCP. En caso contrario, seleccione la opción MANUAL e introduzca la configuración

(DIRECCIÓN IP, MÁSCARA DE RED, GATEWAY POR DEFECTO, DNS PRIMARIO, DNS SECUNDARIO). Consulte con el gestor de la red para obtener dichos parámetros.

NOTA: En caso de que el servidor de CAS no esté situado en la misma LAN que Ikusi Flow, sino que haya que acceder a éste a través de internet, asegúrese de que los dispositivos de electrónica de red (router, firewall, etc) no impiden la comunicación de la cabecera con el exterior. En algunos casos, es necesario que el gestor de la red modifique la configuración de dichos dispositivos de electrónica de red.

3. CONFIGURACIÓN INICIAL

3.1 Activar Configuraciones Avanzadas

La gestión de la interfaz simulcrypt se realiza usando opciones de la configuración avanzada. Por lo tanto, el primer paso consiste en activar la configuración avanzada.

- ir a MENÚ→CONFIGURACIONES AVANZADAS→Activar configuraciones avanzadas

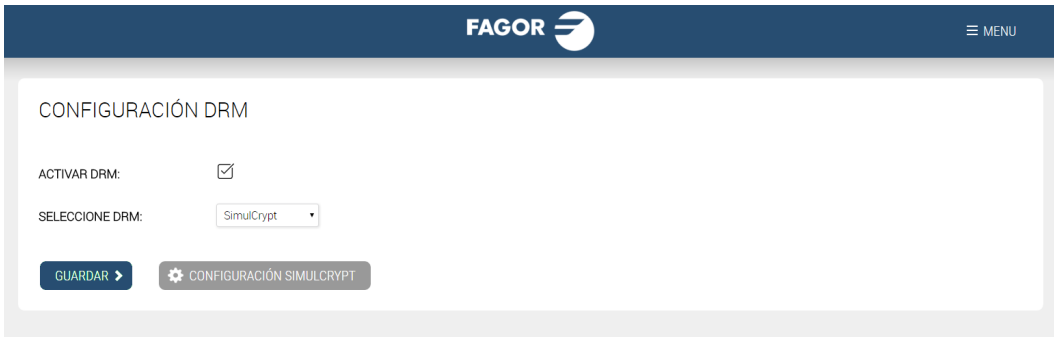
4. CONFIGURACIÓN DE LA INTERFAZ SIMULCRYPT

A continuación se detalla cómo realizar la configuración de la interfaz simulcrypt de Ikusi Flow para realizar el intercambio de claves y mensajes con un servidor de CAS externo. Gran parte de los parámetros que deben ser configurados son proporcionados por el sistema de CAS. Póngase en contacto con el fabricante del CAS para obtener dicha información.

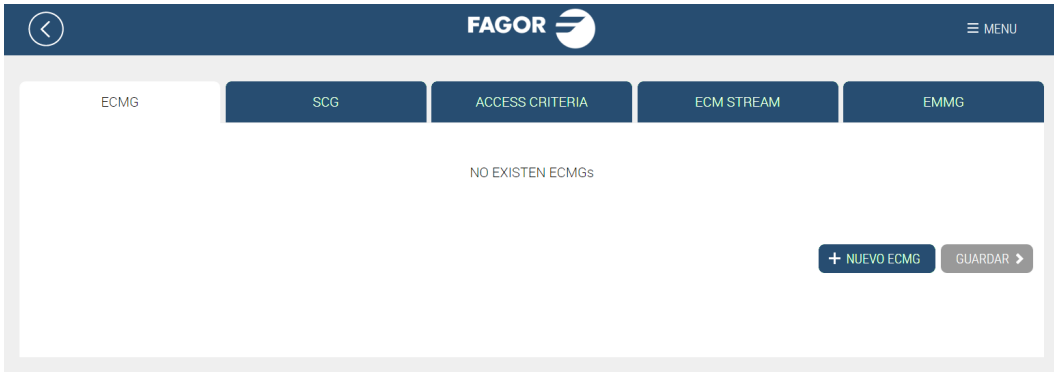
4.1 Activación de la interfaz simulcrypt

Para activar la interfaz simulcrypt, ir a MENÚ→CONFIGURACIÓN AVANZADAS→Configuración DRM

Active el checkbox ACTIVAR DRM. Después, despliegue la lista SELECCIONE DRM y elija SimulCrypt. Finalmente, pulse el botón GUARDAR



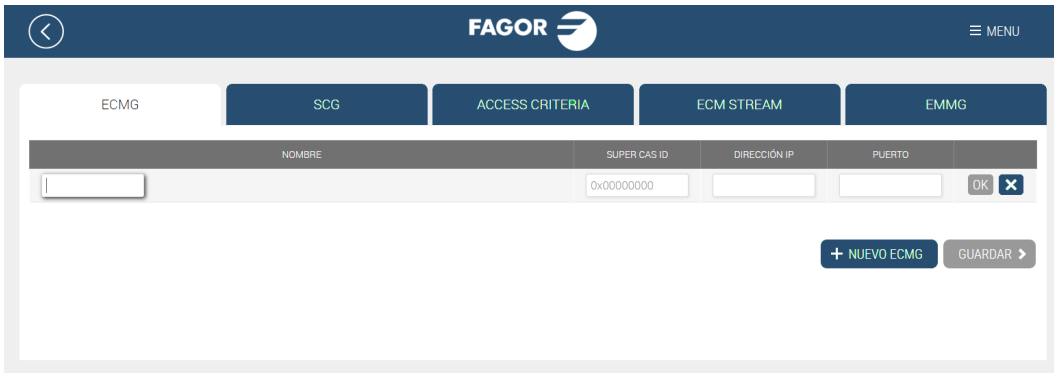
Tras ello, el botón CONFIGURACIÓN SIMULCRYPT se habilitará. Haga click sobre él para acceder a la pantalla donde podrá configurar el resto de parámetros (ECMG, SCG, Access Criteria, ECM Streams, EMMG).



4.2 Configuración de ECMGs

Está pestaña se usa para crear la conexión entre Ikusi Flow y el generador de ECMs, normalmente situado en el servidor de CAS externo.

Seleccione la pestaña ECMG para tener acceso a esta configuración. Haga click en el botón + NUEVO ECMG. Se añadirá una fila correspondiente al nuevo generador de ECM que se desea configurar.



Rellene los parámetros del generador de ECMs:

- NOMBRE: es un campo de texto libre usado como referencia interna para identificar el generador de ECMs
- SUPERCASID: son 8 caracteres hexadecimales que serán proporcionados por el fabricante del CAS. Deben ser introducidos en formato hexadecimal, precedidos de "0x"
- DIRECCIÓN IP: es la dirección IP del servidor donde esté el generador de ECMs
- PUERTO: es el puerto del servidor externo a través del que se accede al generador de ECMs

Tras completar la configuración, pulse el botón OK.

Puede modificar la configuración del generador de ECMs cuando desee, pulsando el botón . Además, en caso de corte de comunicación entre la cabecera y el servidor de CAS, puede forzar el refresco de la comunicación pulsando .

NOTA: Ikusi Flow permite el encriptado de la señal con varios sistemas de CAS simultáneamente. Si ese es su caso, añada tantos generadores de ECM como sean necesarios.

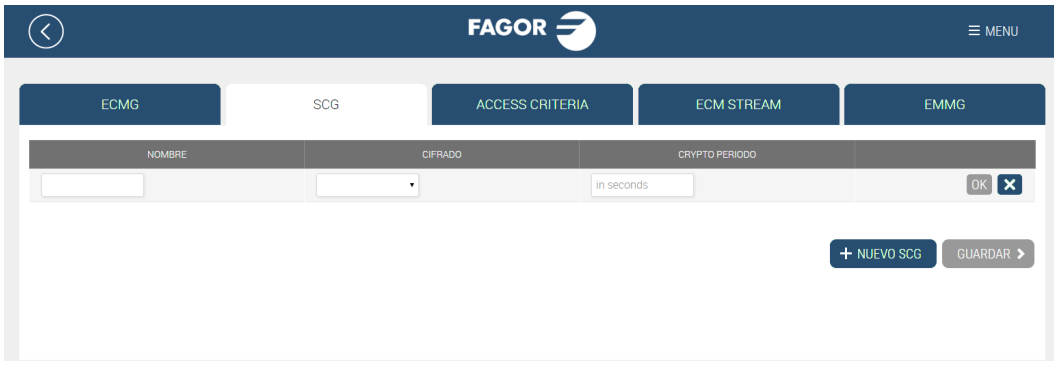
Pulse el botón GUARDAR para almacenar la configuración.

NOTA: Al pulsar el botón GUARDAR se salvan todos los cambios de todas las pestañas de la configuración simulcrypt. Por lo tanto, sólo es estrictamente necesario hacerlo en la última que se modifique. Aún así, se recomienda hacerlo cada vez que se haga un cambio en cualquiera de las pestañas, para evitar olvidos accidentales.

4.3 Configuración de SCGs

Está pestaña se usa definir los Scrambling Control Group. Existirán tantos SCGs como claves de encriptado distintas usadas en la cabecera. Seleccione la pestaña SCG para tener acceso a esta configuración.

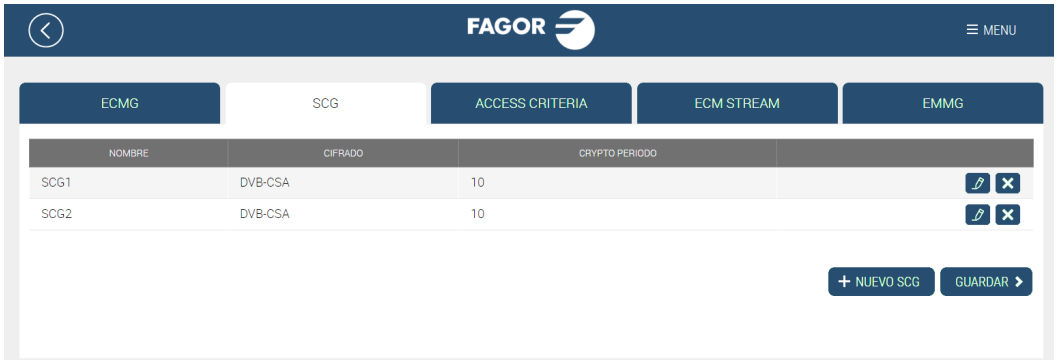
Para añadir un SCG haga click en el botón + NUEVO SCG. Aparecerá una fila correspondiente al nuevo Scrambling Control Group que se desea configurar.



Rellene los parámetros del SCG añadido:

- NOMBRE: es un campo de texto libre usado como referencia interna para identificar el SCG
- CIFRADO: elija en la lista desplegable el sistema de encriptado utilizado.
- CRYPTO PERIOD: introduzca el periodo de validez de cada clave, en segundos. Confirme dicho valor con el fabricante del CAS.

Tras completar la configuración, pulse el botón OK. Repita la operación para añadir tantos SCGs como sean necesarios.

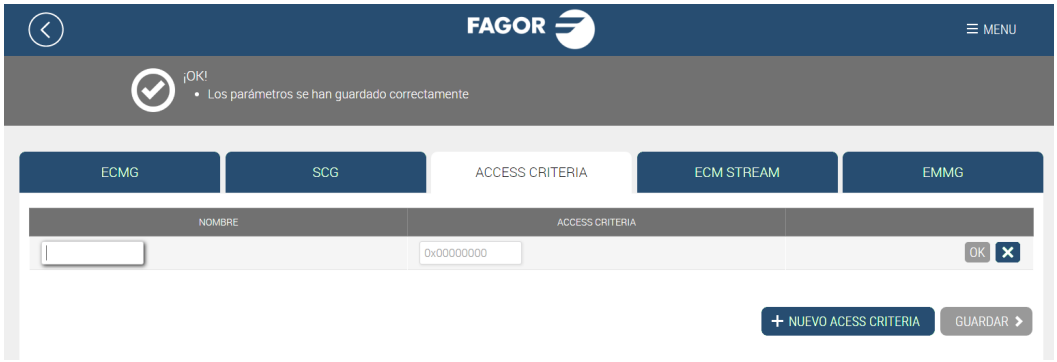


Pulse el botón GUARDAR para almacenar la configuración.

4.4 Configuración de Access Criteria

Está pestaña se usa definir los Access Criteria, en caso de que existan. Esta información es proporcionada por el fabricante del CAS. Seleccione la pestaña ACCESS CRITERIA para tener acceso a esta configuración.

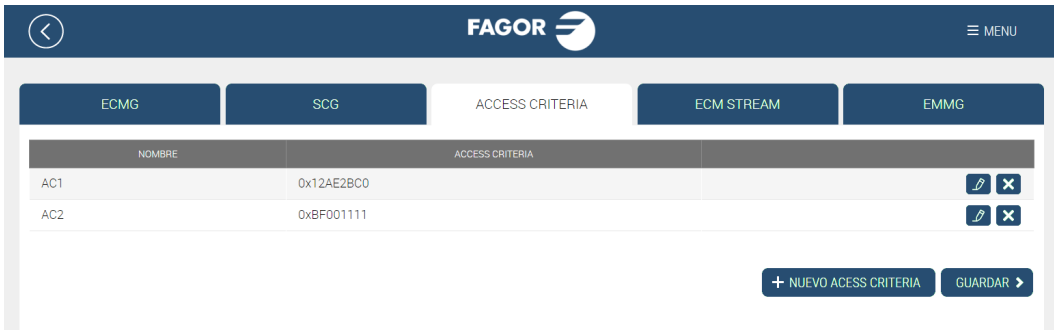
Para añadir un Access Criteria haga click en el botón + NUEVO ACCESS CRITERA. Aparecerá una fila correspondiente al nuevo Access Criteria que se desea configurar.



Rellene los parámetros del Access Criteria añadido:

- NOMBRE: es un campo de texto libre usado como referencia interna para identificar el Access Criteria
- ACCESS CRITERIA: Son 8 caracteres hexadecimales que serán proporcionados por el fabricante del CAS. Deben ser introducidos en formato hexadecimal, precedidos de "0x"

Tras completar la configuración, pulse el botón OK. Repita la operación para añadir tantos Access Criteria como sean necesarios.



Pulse el botón GUARDAR para almacenar la configuración.

4.5 Configuración de ECM Streams

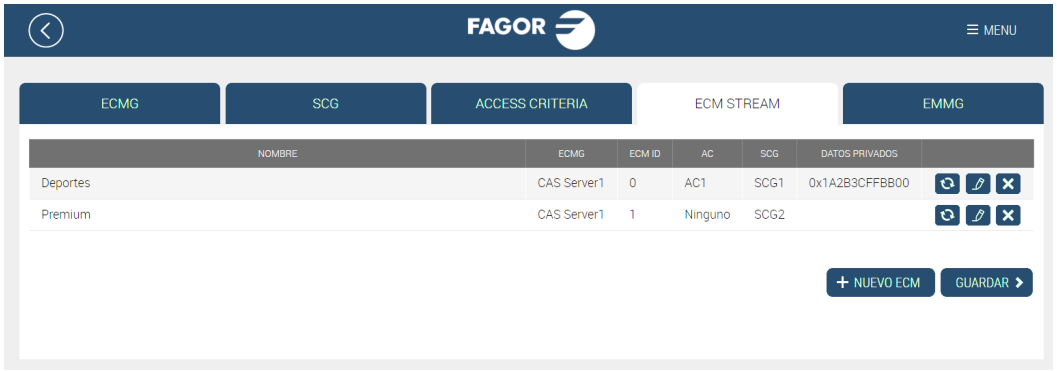
Está pestaña se usa definir qué ECM estará relacionado con cada SCG. Seleccione la pestaña ECM STREAM para tener acceso a esta configuración.

Para añadir un ECM haga click en el botón + NUEVO ECM. Aparecerá una fila correspondiente al nuevo ECM que se desea configurar.

Rellene los parámetros del ECM añadido:

- NOMBRE: es un campo de texto libre usado como referencia interna para identificar el ECM.
- ECMG: seleccione en la lista desplegable el generador de ECM encargado de porporcionar el ECM. En la lista aparecerán todos los generadores de ECM definidos en la pestaña ECMG.
- ECM ID: es un identificador del ECM. Es un valor numérico entre 0 y 65535 que debe ser único en la red de distribución. Este campo se puede dejar vacío, y en ese caso la propia cabecerá propondrá uno. En otros casos, el sistema de CAS puede exigir unos valores concretos. Póngase en contacto con el fabricante del CAS para confirmar este punto.
- AC: seleccione en la lista desplegable el Access Criteria que se debe aplicar al ECM que se está definiendo En la lista aparecerán todos los Access Criteria definidos en la pestaña ACCESS CRITERIA. Si el ECM no está ligado a ningún Access Criteria, seleccione el valor “Ninguno”.
- SCG: seleccione en la lista desplegable el Scrambling Control Group que utilizará la clave de encriptado asociada al ECM que se está definiendo En la lista aparecerán todos los Scrambling Control Group definidos en la pestaña SCG.
- DATOS PRIVADOS: son los datos privados que se incluirán en el ca_descriptor de la PMT asociados al ECM que se está definiendo. Serán proporcionados por el fabricante del CAS. Deben ser introducidos en formato hexadecimal, precedidos de “0x”. En caso de que el ca_descriptor no incluya datos privados, deje el campo vacío.

Tras completar la configuración, pulse el botón OK. Repita la operación para añadir tantos ECMs como sean necesarios (cada SCG debe tener configurado al menos un ECM por cada ECMG).



Pulse el botón GUARDAR para almacenar la configuración.

4.6 Configuración de EMMGs

Está pestaña se usa para definir los parámetros asociados al generador de EMMs. Seleccione la pestaña EMMG para tener acceso a esta configuración.

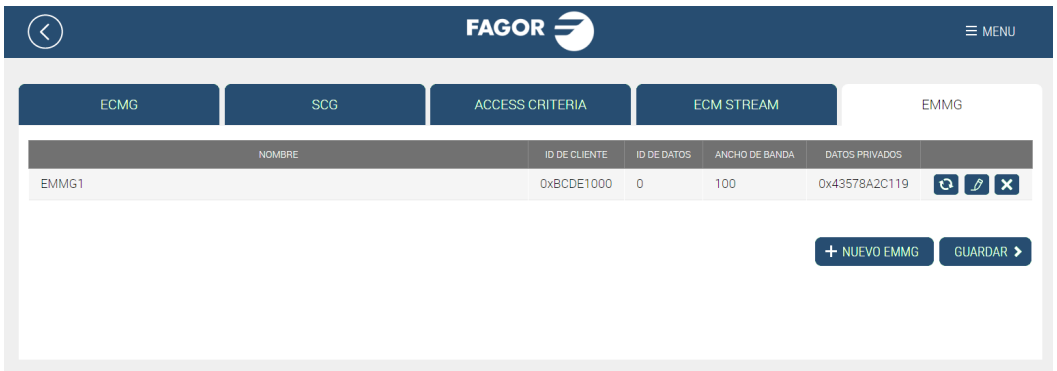
Para añadir un generador de EMMs haga click en el botón + NUEVO EMMG. Aparecerá una fila correspondiente al nuevo EMMG que se desea configurar.

Rellene los parámetros del EMMG añadido:

- NOMBRE: es un campo de texto libre usado como referencia interna para identificar el EMMG
- ID DE CLIENTE: son 8 caracteres hexadecimales que serán proporcionados por el fabricante del CAS. Deben ser introducidos en formato hexadecimal, precedidos de "0x"
- ID DE DATOS: es un identificador del EMMG. Es un valor numérico entre 0 y 65535 que debe ser único en la red de distribución. Este campo se puede dejar vacío, y en ese caso la propia cabecera propondrá uno. En otros casos, el sistema de CAS puede exigir unos valores concretos. Póngase en contacto con el fabricante del CAS para confirmar este punto
- ANCHO DE BANDA: Ikusi Flow indicará al EMMG que ese valor es el máximo ancho de banda que puede recibir de él
- DATOS PRIVADOS: son los datos privados que se incluirán en el ca_descriptor de la CAT asociados al EMM que se está definiendo. Serán proporcionados por el fabricante del CAS. Deben ser introducidos en formato hexadecimal, precedidos de "0x". En caso de que el ca_descriptor no incluya datos privados, deje el campo vacío.

Tras completar la configuración, pulse el botón OK.

NOTA: Ikusi Flow permite el encriptado de la señal con varios sistemas de CAS simultáneamente. Si ese es su caso, añada tantos generadores de EMM como sean necesarios.



NOTA: El servidor de CAS externo se comunicará con Ikusi Flow para enviar los EMMs. Para ello, deberá informar a dicho servidor de en qué dirección IP se encuentra la cabecera Ikusi Flow y qué puerto deberá usar para realizar el intercambio de EMMs. La dirección IP la podrá encontrar en el Informe General de Instalación (MENÚ→ESTADO→Informe general), en el apartado correspondiente a Configuración de red. El puerto utilizado para las comunicaciones con el EMMG es el 9998.

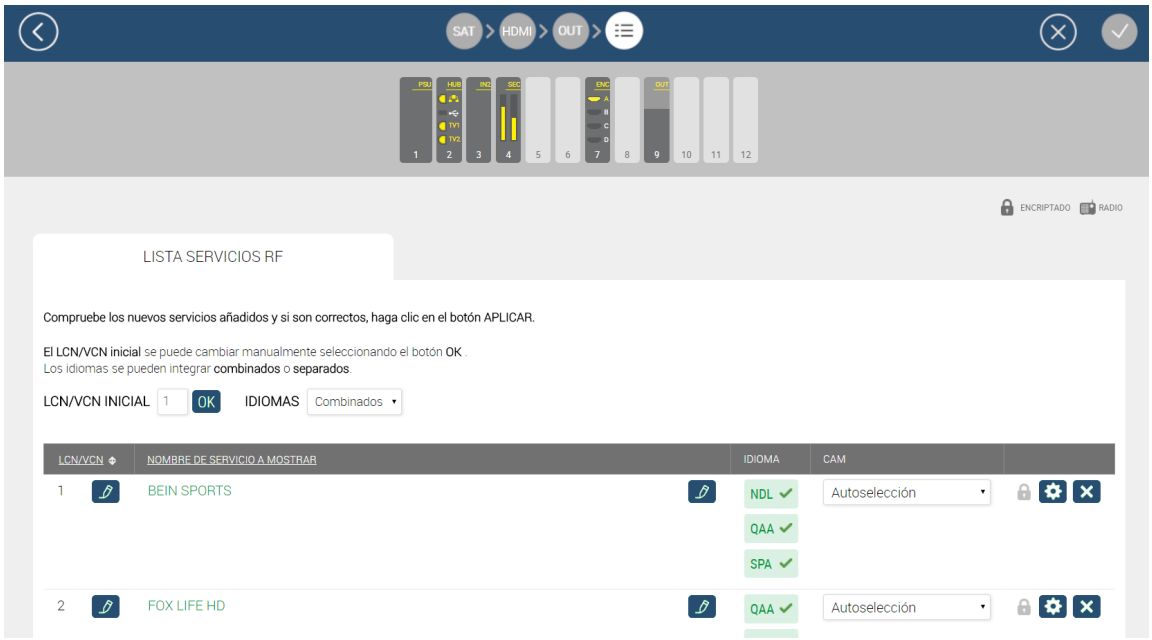
Pulse el botón GUARDAR para almacenar la configuración.

4.7 Asignación de encriptado en cada servicio

Por defecto, tras activar la interfaz simulcrypt, todos los servicios que sean procesados por un módulo FLOW SEC o FLOW ENC serán encriptados usando el primer Scrambling Control Group que se haya definido en la pestaña SCG.

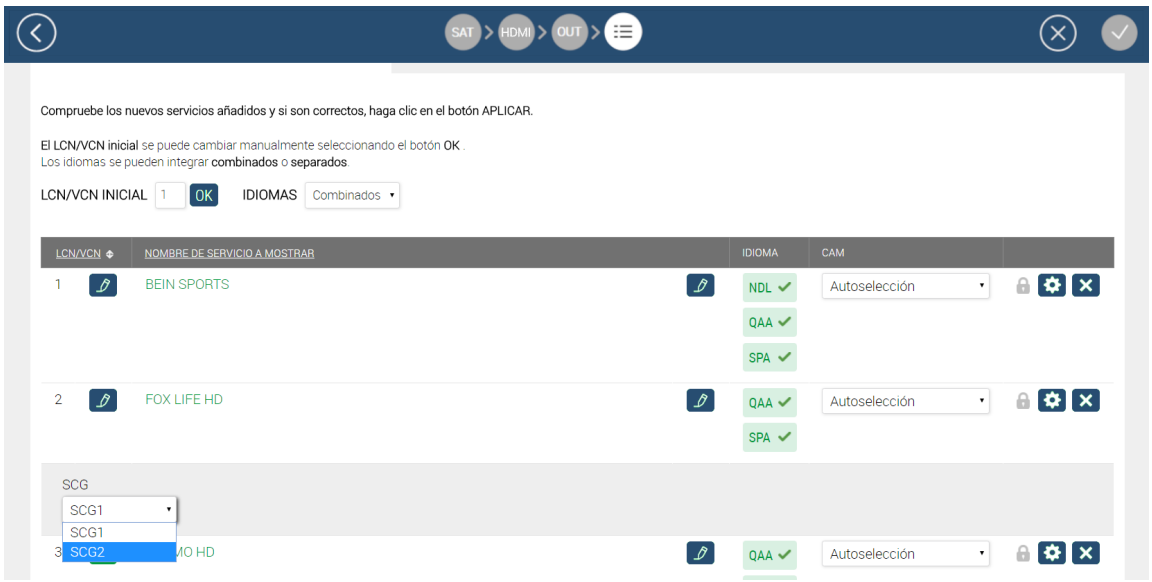
En caso de que deba utilizarse un SCG distinto para un servicio concreto, deberá modificar la configuración de dicho servicio en el Asistente de Configuración.

Para ello, desde la pantalla Inicio pulse el botón ASISTENTE DE CONFIGURACIÓN. Dentro del Asistente, ir directamente al paso Pantalla de resumen, pulsando el botón .



Seleccione el botón de configuración avanzada correspondiente al servicio al que desea cambiar el SCG asociado.

Se abrirá una fila donde, entre otros parámetros, encontrará una lista desplegable donde podrá elegir el SCG que desea aplicar al servicio.

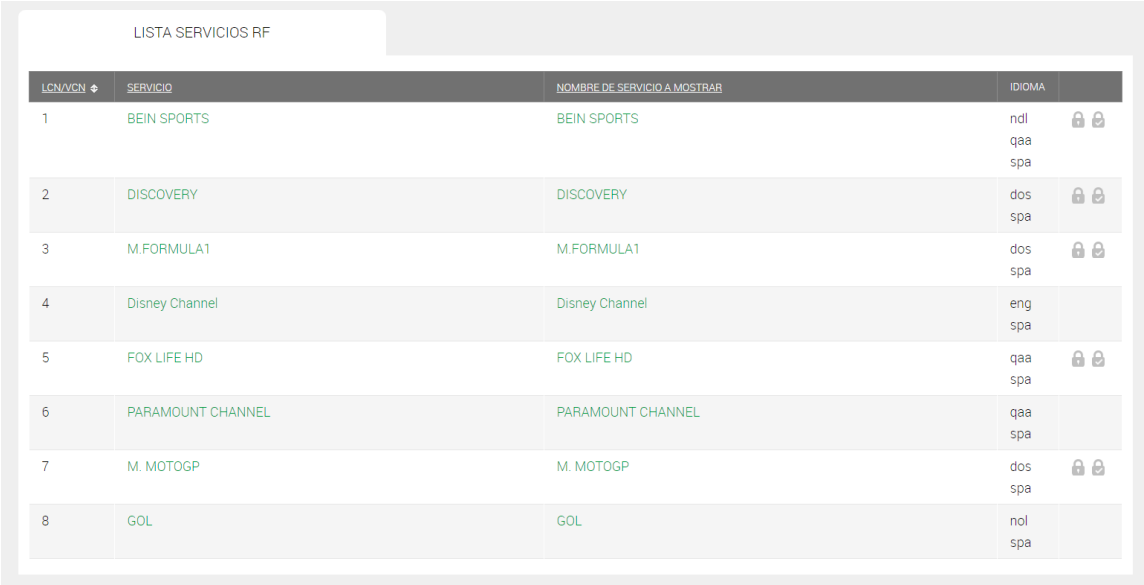


Una vez modificada la asignación de SCGs en los servicios que sea necesarios, pulse el botón para aplicar la nueva configuración.

5. COMPROBACIÓN DEL ESTADO DE LA INTEFAZ SIMULCRYPT

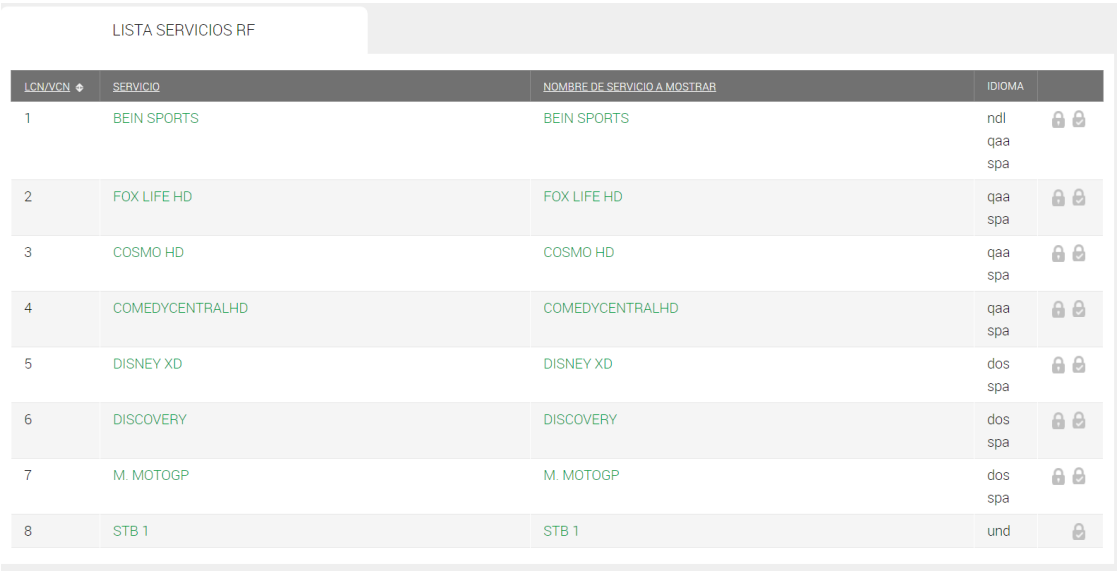
Una vez que la interfaz simulcrypt ha sido activada, puede comprobar su estado en la pantalla Inicio. Hay tres maneras de comprobar que ha sido activada:

- En la lista de servicios de la pantalla Inicio puede comprobar que los servicios procesados por los módulos FLOW SEC y FLOW ENC están siendo protegidos a través de la interfaz simulcrypt. Aparecerán marcados el icono .



LCN/VCN	SERVICIO	NOMBRE DE SERVICIO A MOSTRAR	IDIOMA
1	BEIN SPORTS	BEIN SPORTS	ndl qaa spa
2	DISCOVERY	DISCOVERY	dos spa
3	M.FORMULA1	M.FORMULA1	dos spa
4	Disney Channel	Disney Channel	eng spa
5	FOX LIFE HD	FOX LIFE HD	qaa spa
6	PARAMOUNT CHANNEL	PARAMOUNT CHANNEL	qaa spa
7	M. MOTOGP	M. MOTOGP	dos spa
8	GOL	GOL	nol spa

- Al hacer click sobre un módulo FLOW SEC o FLOW ENC se abrirá una ventana de estado. Entre la información que aparece en la ventana, en el apartado DRM se puede ver que se está usando SimulCrypt.



LCN/VCN	SERVICIO	NOMBRE DE SERVICIO A MOSTRAR	IDIOMA
1	BEIN SPORTS	BEIN SPORTS	ndl qaa spa
2	FOX LIFE HD	FOX LIFE HD	qaa spa
3	COSMO HD	COSMO HD	qaa spa
4	COMEDYCENTRALHD	COMEDYCENTRALHD	qaa spa
5	DISNEY XD	DISNEY XD	dos spa
6	DISCOVERY	DISCOVERY	dos spa
7	M. MOTOGP	M. MOTOGP	dos spa
8	STB 1	STB 1	und

- En el informe general de estado se indica si se está usando la interfaz simulcrypt en cada módulo FLOW SEC o FLOW ENC. Para obtener el informe ir a MENÚ→ESTADO→Informe general. Se abrirá una ventana con la información completa de la cabecera en detalle. En cada cuadro dedicado a cada módulo FLOW SEC o FLOW ENC, en el campo DRM, aparecerá un texto indicando que se está usando SimulCrypt.

EC	
º de slot	5
º de serie	4311SB009316
ersión de hardware	0
ersión de firmware	2.2.1+d20170327
emperatura	40ºC
iempo de uso	531h
RM	SimulCrypt
AM 1 Insertado	sí
AM 1 En uso	sí
AM 1 Nivel de uso	60%
AM 1 Fabricante	SmarDTV
AM 1 Modelo	Movistar+ Pro CAM
AM 1 Servicios	FOX LIFE HD M. MOTOGP M.FORMULA1
AM 2 Insertado	sí
AM 2 En uso	sí
AM 2 Nivel de uso	40%
AM 2 Fabricante	SmarDTV
AM 2 Modelo	Movistar+ Pro CAM
AM 2 Servicios	BEIN SPORTS DISCOVERY

FAGOR ELECTRÓNICA | IKUSI

Fagor Multimedia Solutions SL.
Araba hiribidea, 34
E-20500 Mondragón - Guipúzcoa
Tel: +34 943 71 25 26
e-mail: rf.sales@fagorelectronica.es
www.fagorelectronica.com

Donostia Ibilbidea, 28
E-20115 Astigarraga - Guipúzcoa
Tel:+34 943 44 89 44
e-mail: support@fagormultimedia.com
www.fagormultimedia.com

MONDRAGON
HUMANITY AT WORK
Finance
Industry
Retail
Knowledge