FAGOR ELECTRÓNICA

Flow

Manuel de Configuration de l'Interface Simulcrypt

Index page

1. INTRODUCTION

La station de tête Ikusi Flow permet de cryptes les contenus pour leur transmission de manière sûre dans le réseau coaxial ou le réseau IP d'une installation. Ikusi Flow permet la communication avec un serveur de CAS standard par le biais de l'interface simulcrypt. Le présent manuel décrit l'architecture de l'interface simulcrypt mise en place dans Ikusi Flow et son mode d'emploi.

2. DESCRIPTION DE L'INTERFACE SIMULCRYPT DANS IKUSI FLOW

Ikusi Flow permet l'interaction de la station de tête avec un système d'accès conditionnel (CAS). La station de tête n'a besoin que de connectivité avec le serveur. En utilisant le protocole DVB d'Interface Simulcrypt (ETSI TS 103 197), les clés, les messages de contrôle et les messages de gestion sont échangés entre la station de tête et le serveur CAS.

Les scramblers sont inclus dans les modules de la station de tête (plus précisément dans les modules FLOW SEC et FLOW ENC). On n'a donc pas besoin de hardware additionnel et l'installation devient moins complexe.

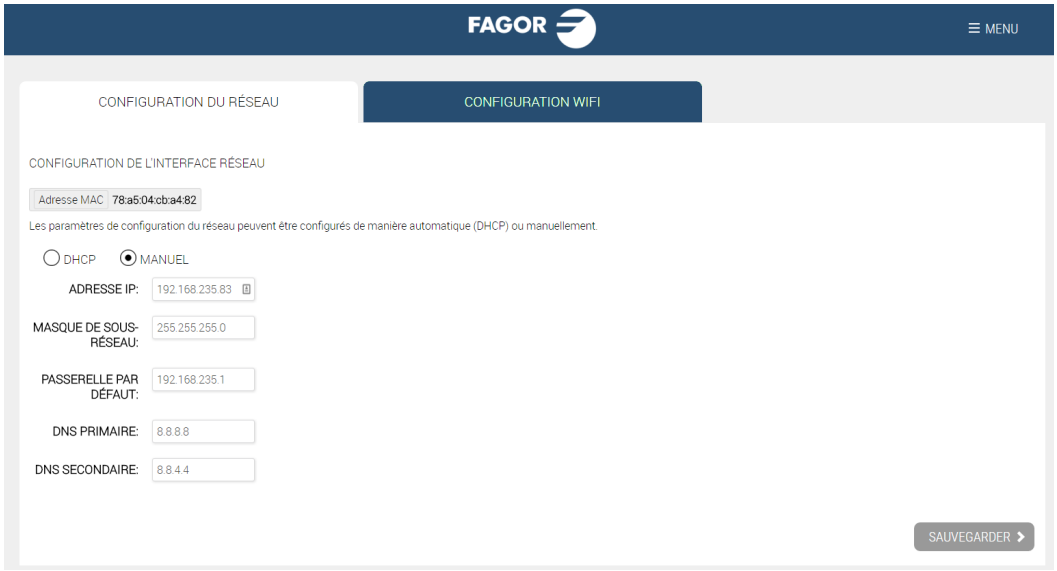
NOTE : Seuls les services traités par les modules FLOW SEC et FLOW SEC peuvent être cryptes. Dans le cas de figure du module FLOW SEC le nombre de services qui peuvent être cryptés avec chaque module est de 16, divisé en deux bloque de 8 services (un bloque pour chaque chaîne de signale associé à chaque slot common interface du module FLOW SEC).

2.1 Communication de l'Ikusi Flow avec le serveur CAS

La communication entre la station de tête Ikusi Flow et le serveur CAS se fait à travers le protocole interface simulcrypt. Ce protocole permet l'échange de messages TCP/IP entre les deux systèmes. Pour que cette communication soit possible il faut donc doter de connectivité la station de tête Ikusi Flow.

Pour cela il faut connecter le port de configuration d'Ikusi Flow à une prise réseau. Le port de cette configuration se trouve sur le module FLOW HUB et il est représenté par le symbole 

Il faut vérifier que la station de tête a les paramètres de réseau correctement configurés. Pour cette vérification il faut accéder sur MENU➞CONFIGURATION➞Réseau. L'écran suivant s'affichera :



Cliquez sur l'onglet CONFIGURATION DU RÉSEAU. Sélectionnez l'option DHCP si la configuration de réseau va être fournie automatiquement par un serveur DHCP. Dans le cas contraire, sélectionnez l'option MANUEL et introduisez la configuration (ADRESSE IP, MASQUE SE SOUS-RÉSEAU, PASSERELLE PAR DÉFAUT, DNS PRIMAIRE, DNS SECONDAIRE). Consultez l'administrateur du réseau pour obtenir ces paramètres.

NOTE : Si le serveur de CAS n'est pas situé dans la même LAN ou réseau local que l'Ikusi Flow et qu'il faut accéder au serveur par internet, assurez-vous que les dispositifs d'électronique de réseau (router, firewall, etc.) ne font pas obstacle à la communication entre la station de tête et l'extérieur. Dans certains cas, il faut que l'administrateur du réseau modifie la configuration de ces dispositifs d'électronique du réseau.

3. CONFIGURATION INITIALE

3.1 Activer les Configurations Avancées

La gestion de l'interface simulcrypt se fait en utilisant des options de la configuration avancée. Par conséquent, la première démarche consiste à activer la configuration avancée.

- Aller à MENU→CONFIGURATIONS AVANCÉES→Activer la configuration avancée.

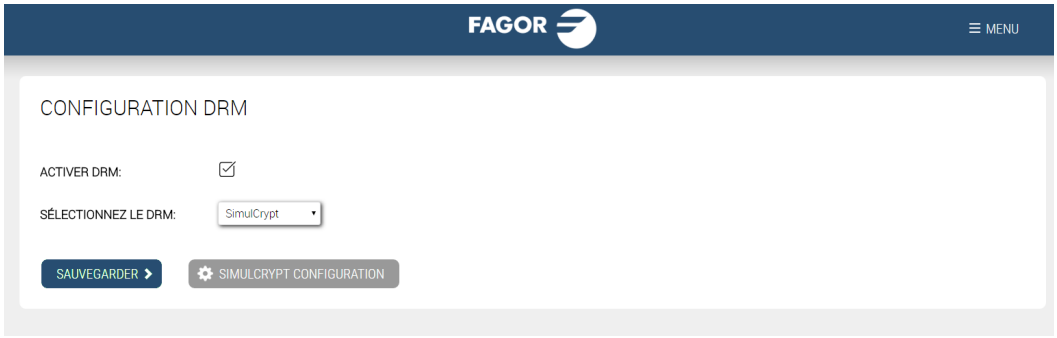
4. CONFIGURATION DE L'INTERFACE SIMULCRYPT

Nous détaillons ci-dessous la configuration de l'interface simulcrypt de l'Ikusi Flow pour réaliser l'échange de clés et de messages avec un serveur CAS externe. Une grande partie des paramètres à configurer sont fournis par le système CAS. Contactez le fabricant du CAS pour obtenir cette information.

4.1 Activation de l'interface simulcrypt

Pour activer l'interface simulcrypt, accéder à MENU→CONFIGURATIONS AVANCÉES→Configuration DRM.

Activez le checkbox ACTIVER DRM. Ensuite, déployez la liste SÉLECTIONNEZ LE DRM et choisissez SimulCrypt. Finalement, cliquez sur le bouton SAUVEGARDER.

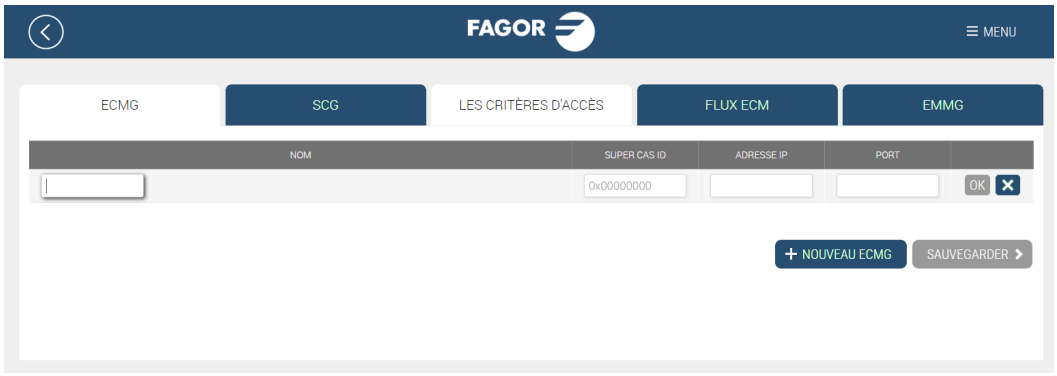


Suite à cette configuration le bouton SIMULCRIPT CONFIGURATION sera activé. Cliquez sur ce bouton pour accéder à l'écran où vous pourrez configurer le reste des paramètres (ECMG, SCG, Access Criteria, ECM Streams, EMMG).

4.2 Configuration des ECMG

Cet onglet est utilisé pour créer la connexion entre l'Ikusi Flow et le générateur des ECMs, normalement situé dans le serveur CAS externe.

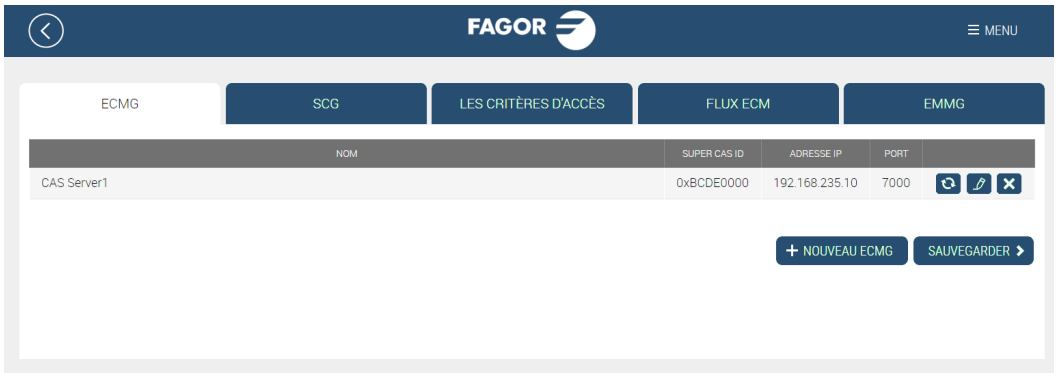
Sélectionnez l'onglet ECMG pour avoir accès à cette configuration. Cliquez sur +NOUVEAU ECMG. Une nouvelle ligne s'ajoutera correspondant au nouveau générateur d'ECM qu'on souhaite configurer.



Remplissez les paramètres du générateur d'ECM :

- NOM : c'est un champ de texte libre utilisé comme référence interne pour identifier le générateur des ECM.
- SUPERCASID : il s'agit de 8 caractères hexadécimaux qui seront fournis par le fabricant du CAS. Ils doivent être introduits sous format hexadécimal, précédés de "0x".
- ADRESSE IP : c'est l'adresse IP du serveur où se trouve le générateur des ECM.
- PORT : c'est le port du serveur externe à travers lequel on accède au générateur d'ECMs.

Une fois terminée la configuration, appuyez sur OK.



Vous pouvez modifier la configuration du générateur d'ECM lorsque vous le souhaitez en appuyant sur le bouton . De même, en cas de coupure de communication entre la station de tête et le serveur CAS, vous pouvez forcer le rafraîchissement en appuyant sur .

NOTE : Ikusi Flow permet le cryptage du signal avec plusieurs systèmes CAS en simultané. Si c'est votre cas, ajoutez autant de générateurs ECM que nécessaires.

Appuyez sur le bouton SAUVEGARDER pour enregistrer la configuration.

NOTE : Lorsque vous appuyez sur le bouton SAUVEGARDER tous les changements réalisés dans tous les onglets de la configuration simulcrypt sont enregistrés. Par conséquent, cette opération n'est strictement nécessaire que lors de la dernière modification. Quoiqu'il en soit, il est recommandé de sauvegarder à chaque fois qu'un changement est introduit dans un onglet pour éviter des oublis accidentels.

4.3 Configuration des SCG

Cet onglet s'utilise pour définir les Scrambling Control Group. Il y aura autant de SCG que de clés de cryptage utilisées dans la station de tête. Sélectionnez l'onglet SCG pour avoir accès à cette configuration.

Pour ajouter un SCG cliquez sur le bouton +NOUVEAU SCG. Une nouvelle ligne s'affichera, correspondante au nouveau Scrambling Control Group que vous souhaitez configurer.

Introduisez les paramètres du SCG ajouté :

- NOM : c'est un texte libre utilisé comme référence interne pour identifier le SCG.
- SCRAMBLING : choisissez sur la liste déroulante le système de cryptage utilisé.
- CRYPTO PERIOD : introduisez la période de validité de chaque clé, en secondes. Confirmez cette valeur avec le fabricant du CAS.

Une fois complétée la configuration, appuyez sur le bouton OK. Répétez l'opération pour ajouter autant de SCG que nécessaires.

Appuyez sur le bouton SAUVEGARDER pour enregistrer la configuration.

4.4 Configuration d'Access Criteria

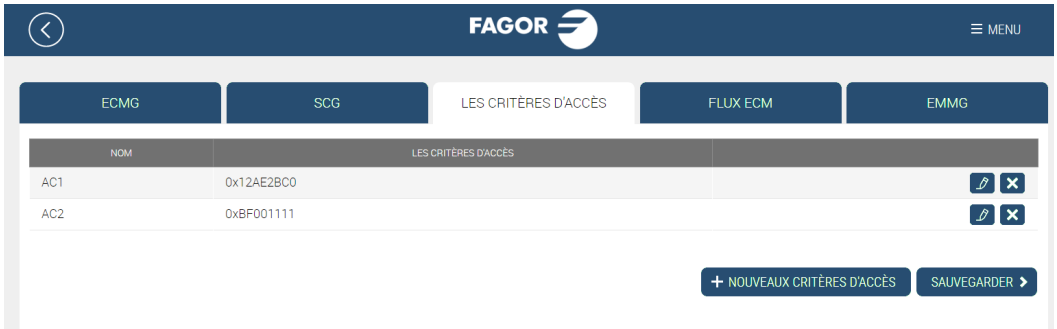
Cet onglet s'utilise pour définir les Access Criteria, s'il y en a. Cette information est fournie par le fabricant du CAS. Sélectionnez l'onglet LES CRITÈRES D'ACCÉS pour avoir accès à cette configuration.

Pour ajouter un Acess Criteria cliquez sur le bouton +NOUVEAUX CRITÈRES D'ACCÉS. Une nouvelle ligne s'affichera correspondant au nouvel Access Criteria que vous souhaitez configurer.

Introduisez les paramètres de l'Access Criteria ajouté :

- NOM : c'est un champ de texte libre utilisé comme référence pour identifier l'Access Criteria.
- LES CRITÈRES D'ACCÉS : Il s'agit de 8 caractères hexadécimaux qui seront fournis par le fabricant du CAS. Ils doivent être introduits sous format hexadécimal, précédés de "0x".

Une fois complétée la configuration, appuyez sur le bouton OK. Répétez l'opération à chaque fois que vous souhaitez ajouter un Access Criteria.



Appuyez sur le bouton SAUVEGARDER pour enregistrer la configuration.

4.5 Configuration d'ECM Streams

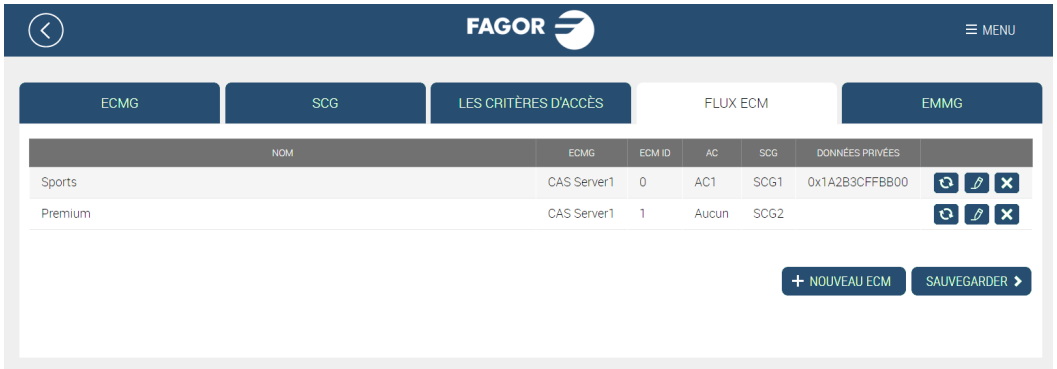
Cet onglet s'utilise pour définir quel ECM est associé à chaque SCG. Sélectionnez l'onglet ECM STREAM pour accéder à cette configuration.

Pour ajouter un ECM cliquez sur le bouton +NOUVEAU ECM. Une nouvelle ligne s'affichera correspondant au nouveau ECM que vous souhaitez configurer.

Introduisez les paramètres du ECM ajouté :

- NOM : c'est un champ de texte libre utilisé comme référence pour identifier l'ECM.
- ECMG : choisissez sur la liste déroulante le générateur du ECM chargé de fournir l'ECM. La liste montrera tous les générateurs d'ECM définis sur l'onglet ECMG.
- ECM ID : Il s'agit d'un identificateur du ECM. C'est une valeur numérique entre 0 et 65535 qui doit être unique sur le réseau de distribution. Ce champ peut être laissé vide et, dans ce cas, la station de tête elle-même en proposera un. Dans d'autres cas, le système CAS peut exiger des valeurs concrètes. Contactez le fabricant du CAS pour confirmer ce paramètre.
- AC : sélectionnez sur le menu déroulant l'Access Criteria qui doit être appliqué à l'ECM que vous êtes en train de définir. Sur le menu figurent tous les Access Criteria définis sur l'onglet LES CRITÈRES D'ACCÉS. Si l'ECM n'est associé à aucun Access Criteria, choisissez la valeur "Aucun".
- SCG : sélectionnez sur le menu déroulant le Scrambling Control Group qu'utilisera la clé de cryptage associée à l'ECM qui est en train d'être défini. Le menu affichera tous les Scrambling Control Group définis sur l'onglet SCG.
- DONNÉES PRIVÉES : il s'agit des données privées inclus dans le ca_descriptor de la PMT associées au ECM qui est en train d'être défini. Elles seront fournies par le fabricant du CAS. Elles doivent être introduites sous format hexadécimal, précédées de "0x". Dans le cas où le ca_descriptor n'inclurait pas de données personnelles, laissez le champ vide.

Une fois terminée la configuration, appuyez sur le bouton OK. Répétez l'opération chaque fois que vous ajouterez un nouveau ECM (chaque SCG doit avoir un ECM configuré pour chaque ECMG).



Appuyez sur le bouton SAUVEGARDER pour enregistrer la configuration.

4.6 Configuration des EMMG

Cet onglet s'utilise pour définir les paramètres associés au générateur d'EMM. Sélectionnez l'onglet EMMG pour avoir accès à cette configuration.

Pour ajouter un générateur d'EMM, cliquez sur le bouton +NOUVEAU EMMG. Une nouvelle ligne s'affichera correspondant au nouveau EMMG que l'on souhaite configurer.

Enregistrez les paramètres de l'EMMG ajouté :

- NOM : c'est un champ de texte libre utilisé comme référence interne pour identifier le EMMG.
- ID DU CLIENT : il s'agit de 8 hexadécimaux qui seront fournis par le fabricant du CAS. Ils doivent être introduits sous format hexadécimal, précédés de "0x".
- DONNÉES ID : il s'agit d'un identificateur de l'EMMG. Sa valeur numérique, qui oscille entre 0 et 65535, doit être unique sur le réseau de distribution. Ce champ peut être laissé vide et, dans ce cas, la station de tête en proposera un. Dans d'autres cas, le système CAS peut exiger des valeurs concrètes. Contactez le fabricant du CAS pour confirmer cette donnée.
- BANDE PASSANTE : Ikusi Flow indiquera au EMMG que cette valeur est la largeur maximale de bande qu'il peut lui fournir
- DONNÉES PRIVÉES : ce sont les données privées qui seront inclus dans le ca_descriptor de la CAT associées à l'EMM qui est en train d'être défini. Elles seront fournies par le fabricant du CAT. Elles doivent être introduites sous format hexadécimal et précédées de "0x". Si le ca_descriptor n'inclut pas de données personnelles, laissez ce champ vide.

Après la configuration, appuyez sur le bouton OK.

NOTE : Ikusi Flow permet le cryptage du signal avec plusieurs systèmes CAS simultanément. Si c'est votre cas, ajoutez autant de générateurs d'EMM que nécessaires.

NOTE : Le serveur de CAS externe se communique avec Ikusi Flow pour envoyer les EMM. Vous devrez informer au serveur de l'adresse IP où se trouve la station de tête Ikusi Flow et le port qu'il devra utiliser pour réaliser l'échange d'EMM. L'adresse IP figure dans le Rapport général d'installation (MENU➔ÉTAT➔Rapport général), dans la seccion correspondant à la Configuration du réseau. Le port utilisé pour les communications avec l'EMMG est le 9998.

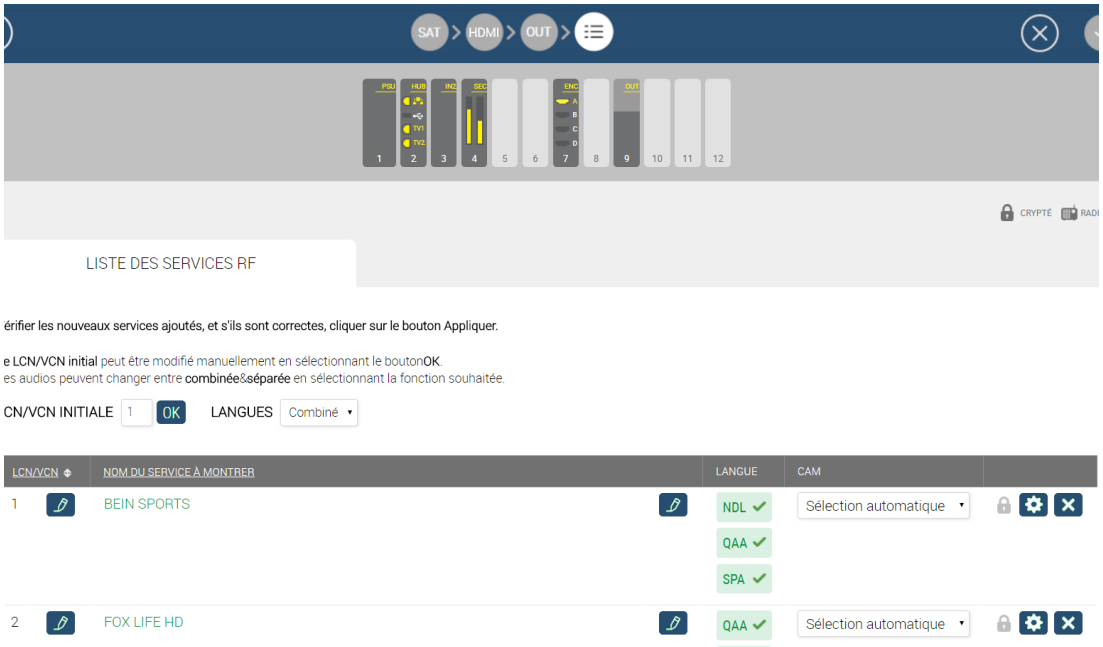
Appuyez sur le bouton SAUVEGARDER pour enregistrer la configuration.

4.7 Assignation du cryptage à chaque service

Par défaut, une fois activée l'interface simulcrypt, tous les services traités par un module FLOW SEC ou FLOW ENC seront cryptés en utilisant le premier Scrambling Control Group défini à l'onglet SCG.

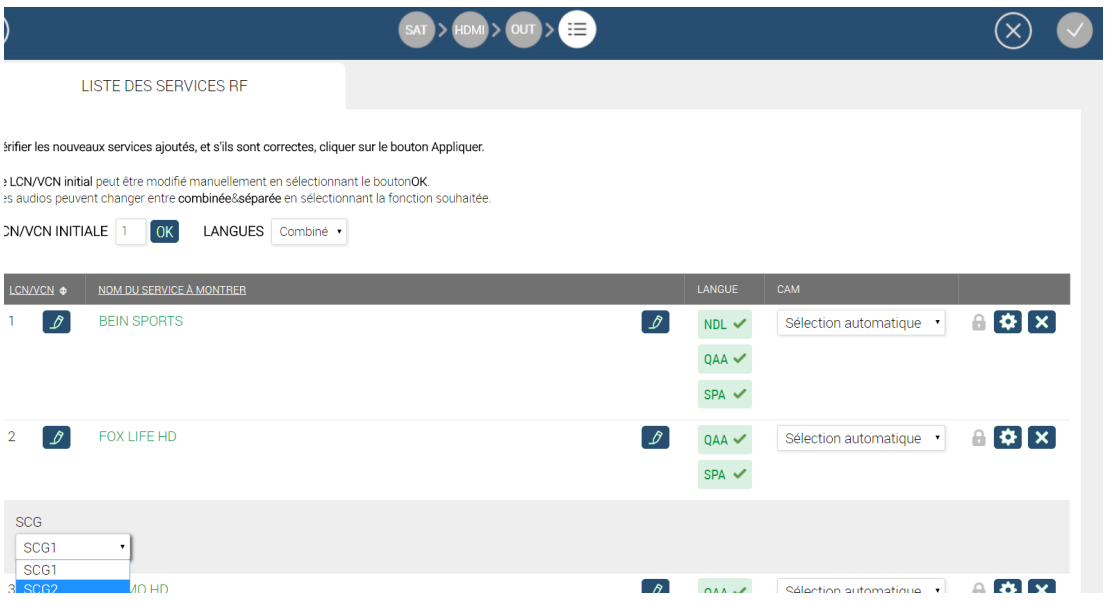
Dans le cas où il faudrait utiliser un SCG différent pour un service concret, vous devrez modifier la configuration de ce service dans l'Assistant de configuration.

Pour cela vous devrez, depuis l'écran d'accueil, appuyer sur le bouton ASSISTANT DE CONFIGURATION. Une fois ouvert, allez directement à l'étape Écran de résumé, en appuyant sur le bouton .



Sélectionnez l'option de configuration avancée correspondant au service auquel vous souhaitez passer le SCG associé.

Une nouvelle ligne s'ouvrira sur laquelle vous trouverez, entre deux paramètres, un menu déroulant où vous pourrez choisir le SCG que vous souhaitez appliquer au service.

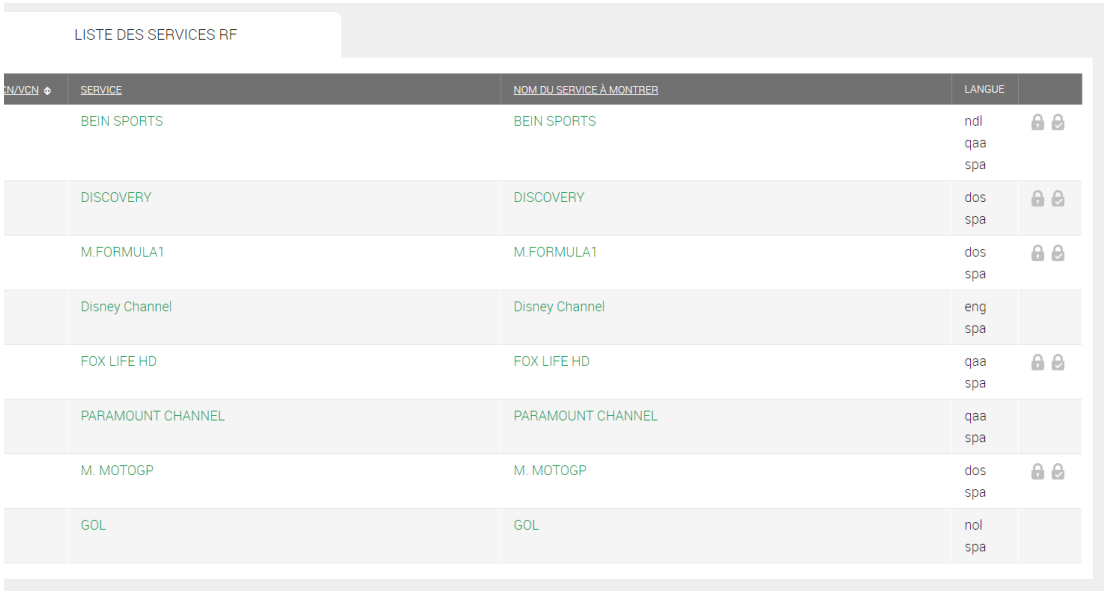


Une fois modifiée l'attribution du SCG aux services nécessaires, appuyez sur le bouton pour appliquer la nouvelle configuration.

5. VÉRIFICATION DE L'ÉTAT DE L'INTERFACE SIMULCRYPT

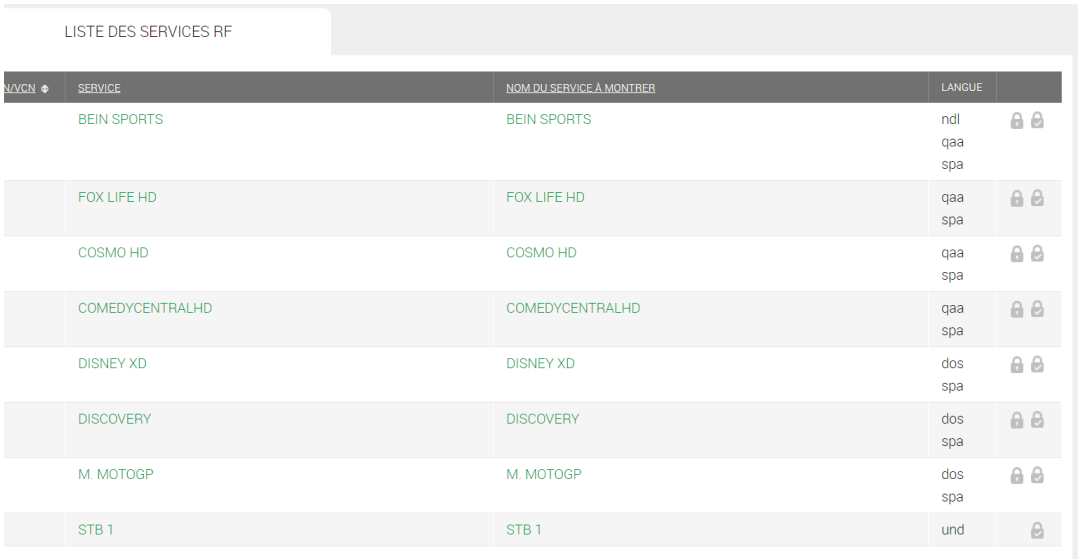
Une fois que l'interface est activée, vous pouvez vérifier son état sur l'écran d'accueil. Il y a trois manières de vérifier son activation :

- Sur la liste de services de l'écran Accueil vous pouvez vérifier que les services de télévision payants traités par les modules FLOW SEC et FLOW ENC sont protégés par un CAS à travers l'interface simulcrypt. Ils porteront l'icône .



CN/VCN	SERVICE	NOM DU SERVICE À MONTRER	LANGUE	
	BEIN SPORTS	BEIN SPORTS	ndl qaa spa	
	DISCOVERY	DISCOVERY	dos spa	
	M.FORMULA1	M.FORMULA1	dos spa	
	Disney Channel	Disney Channel	eng spa	
	FOX LIFE HD	FOX LIFE HD	qaa spa	
	PARAMOUNT CHANNEL	PARAMOUNT CHANNEL	qaa spa	
	M. MOTOGP	M. MOTOGP	dos spa	
	GOL	GOL	nol spa	

- Si vous cliquez sur un module FLOW SEC ou FLOW ENC une fenêtre d'état s'ouvrira. Parmi l'information qui s'affiche sur la fenêtre, le DRM montre que l'on utilise SimulCrypt.



N/VCN	SERVICE	NOM DU SERVICE À MONTRER	LANGUE	
	BEIN SPORTS	BEIN SPORTS	ndl qaa spa	
	FOX LIFE HD	FOX LIFE HD	qaa spa	
	COSMO HD	COSMO HD	qaa spa	
	COMEDYCENTRALHD	COMEDYCENTRALHD	qaa spa	
	DISNEY XD	DISNEY XD	dos spa	
	DISCOVERY	DISCOVERY	dos spa	
	M. MOTOGP	M. MOTOGP	dos spa	
	STB 1	STB 1	und	

- L'apperçu général d'état indique si l'interface simulcrypt est utilisée sur chaque module FLOW SEC ou FLOW ENC. Pour obtenir le rapport accédez sur MENU→ÉTAT→Aperçu général. Une fenêtre s'ouvrira portant l'information complète de la station de tête détaillée. Sur chaque carré consacré à chaque module FLOW SEC ou FLOW ENC, dans le champ DRM, un texte s'affichera indiquant que SimulCrypt est utilisé.

méro du slot	5
méro de série	4311SB009316
sion hardware	0
sion du firmware	2.2.1+d20170327
npérature	40°C
ures de fonctionnement	535h
M	SimulCrypt
M 1 Inséré	oui
M 1 Utilisé	oui
M 1 Niveau d'utilisation	60%
M 1 Fabricant	SmarDTV
M 1 Modèle	Movistar+ Pro CAM
M 1 Services	FOX LIFE HD M. MOTOGP M.FORMULA1
M 2 Inséré	oui
M 2 Utilisé	oui
M 2 Niveau d'utilisation	40%
M 2 Fabricant	SmarDTV
M 2 Modèle	Movistar+ Pro CAM
M 2 Services	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