

VERSATILE

ONE PLATFORM FOR ALL YOUR NEEDS

Flow

Simulcrypt Interface
configuration guide

Index	pages
1. INTRODUCTION	3
2. IKUSI FLOW SIMULCRYPT INTERFACE DESCRIPTION	3
2.1 Communication with CAS server	3
3. INITIAL CONFIGURATION	4
3.1 Enable advanced configuration	4
4. SIMULCRYPT INTERFACE CONFIGURATION	4
4.1 Enable simulcrypt interface	4
4.2 ECMGs configuration	5
4.3 SCGs configuration	6
4.4 Access Criteria configuration	6
4.5 ECM streams configuration	7
4.6 EMMGs configuration	8
4.7 Encryption allocation to each service	10
5. SIMULCRYPT INTERFACE STATUS CHECKING	11

1. INTRODUCTION

Ikusi Flow headend allows to encrypt contents in order to be securely transmitted in coaxial or IPTV distribution networks. Ikusi Flow includes the ability of communication with a standard CAS server through the simulcrypt interface. In this guide the simulcrypt interface implemented in Ikusi Flow and how it is used is described.

2. IKUSI FLOW SIMULCRYPT INTERFACE DESCRIPTION


Ikusi Flow allows the interoperation of the headend with a conditional access system (CAS). The headend only requires a connection with the CAS server. Using DVB Simulcrypt Interface Protocol (ETSI TS 103 197), keys, control messages and management messages are exchanged between Ikusi Flow and the CAS server.

The scramblers are included in the Ikusi Flow modules (specifically, in the FLOW SEC and FLOW ENC modules). Therefore, no additional hardware is needed, reducing the installation complexity.

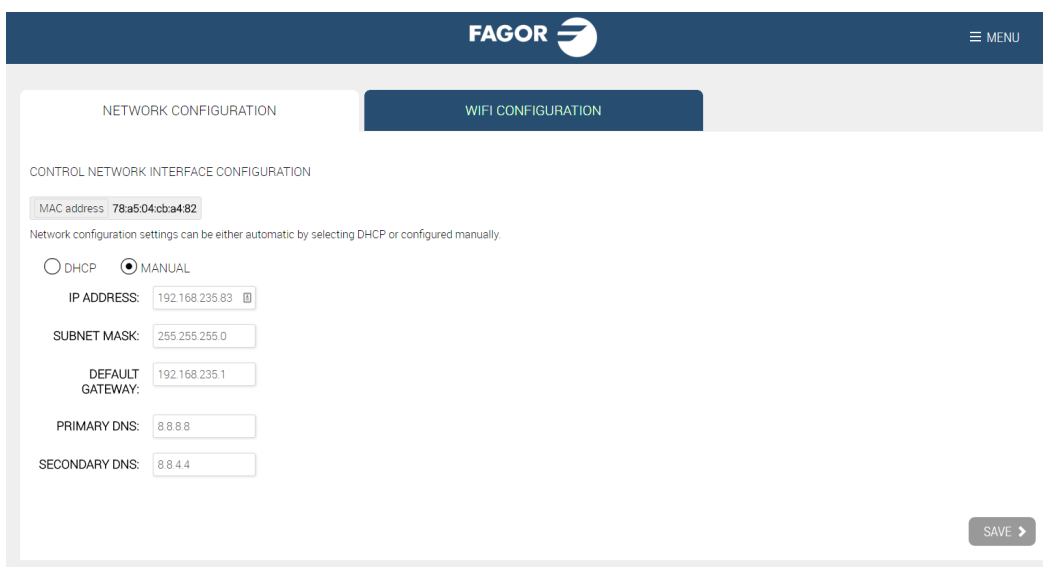
NOTE: Only contents that are managed by the FLOW SEC and FLOW ENC modules can be encrypted. In the case of FLOW SEC modules, the maximum number of services that can be encrypted with each module is 16, divided in 2 blocks of 8 services (one block for each signal chain associated to each common interface slot of the FLOW SEC).

2.1 Communication with CAS server

The communication between the Ikusi Flow headend and the CAS server is done through simulcrypt interface protocol. This protocol allows the interchange of TCP/IP messages between both systems. Therefore, to make this communication possible, the Ikusi Flow headend must be provided with connectivity.

To do that, the configuration port of Ikusi Flow must be connected to a network socket. The configuration port is located in the FLOW HUB module and it is identified with  label.

You must confirm that the network parameters of the headend are properly configured. For that, go to MENU→CONFIGURATION→Network. The following window will open:



The screenshot shows the FAGOR network configuration interface. At the top, there is a dark blue header with the FAGOR logo and a 'MENU' button. Below the header, there are two tabs: 'NETWORK CONFIGURATION' (selected) and 'WIFI CONFIGURATION'. Under the 'NETWORK CONFIGURATION' tab, the section is titled 'CONTROL NETWORK INTERFACE CONFIGURATION'. It shows a 'MAC address' field with the value '78a5:04cba482'. Below this, there is a note: 'Network configuration settings can be either automatic by selecting DHCP or configured manually'. There are two radio buttons: 'DHCP' (unselected) and 'MANUAL' (selected). Below the radio buttons, there are several input fields: 'IP ADDRESS' (192.168.235.83), 'SUBNET MASK' (255.255.255.0), 'DEFAULT GATEWAY' (192.168.235.1), 'PRIMARY DNS' (8.8.8.8), and 'SECONDARY DNS' (8.8.4.4). At the bottom right, there is a 'SAVE' button with a right-pointing arrow.

Click on NETWORK CONFIGURATION tab. Select DHCP option when the network settings are provided automatically by a DHCP server. In other case, select MANUAL option and enter the network parameters (IP ADDRESS, SUBNET MASK, DEFAULT GATEWAY, PRIMARY DNS, SECONDARY DNS). Consult network manager to get those parameters.

NOTE: In the case the CAS server is not located in the same LAN than the headend, but it must be acceded through internet, confirm that the electronic network devices (router, firewall, etc) do not impede the communication of the headend with the outside of the LAN. In some cases, the network manager must modify the configuration of those network electronic devices.

3. INITIAL CONFIGURATION

3.1 Enable advanced configuration

The management of the simulcrypt interface is performed using options of the advanced configuration. Therefore, the first step consists in enabling advanced configuration.

- Go to MENU→ADVANCED CONFIGURATION→DRM Configuration

4. SIMULCRYPT INTERFACE CONFIGURATION

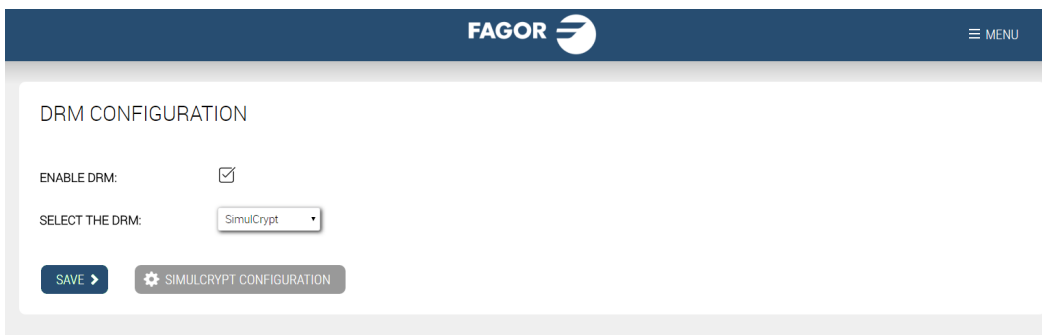
Below is detailed how simulcrypt inteface of Ikusi Flow should be configured to perform the interchange of keys and messasges with an external CAS server. Much of the parameters that must be configured are provided by the CAS system. Contact with the CAS vendor to obtain that information.

4.1 Enable simulcrypt interface

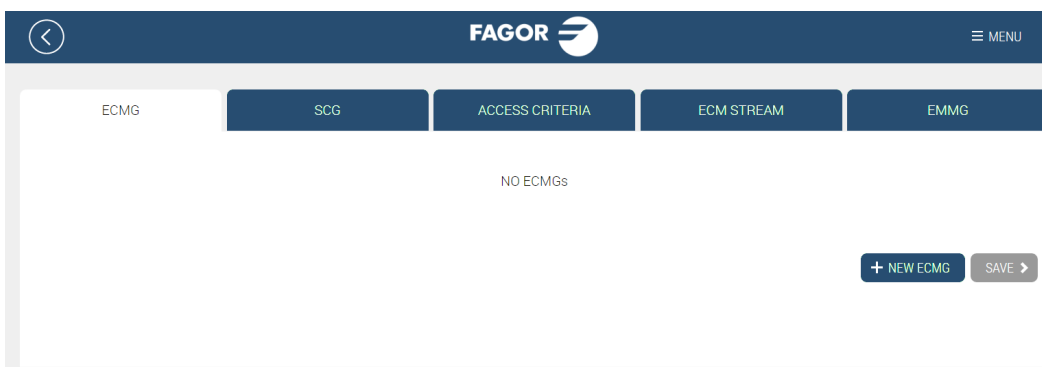
To enable the simulcrypt interface, go to MENU→ADVANCED CONFIGURATION→DRM Configuration



Check ENABLE DRM box. After that, open SELECT DRM list and choose SimulCrypt. Finally, push SAVE button.



After that, SIMULCRYPT CONFIGURATION button will be enabled. Click on it to access to the screen where you could configure the rest of the parameters (ECMG, SCG, Access Criteria, ECM Streams, EMMG).



4.2 ECMGs configuration

This tab is used to create the connection between Ikusi Flow and the ECM generator, generally located in the external CAS server.



Select ECMG tab to access to this configuration. Click on + NEW ECMG. A row will be added, corresponding to the new ECM generator that you want to configure.

Fill in the parameters of the ECM generator:

- **NAME:** is a free text field, used as internal reference to identify the ECM generator.
- **SUPERCASID:** are 8 hexadecimal characters that will be provided by the CAS vendor. They must be introduced in hexadecimal format, preceded by "0x".
- **IP ADDRESS:** is the IP address of the server where the ECM generator is located.
- **PORT:** is the port of the external server, through which the ECM generator is accessed.

After finishing the configuration, push OK button.

NAME	SUPER CAS ID	IP ADDRESS	PORT
CAS Server1	0xBCDE0000	192.168.235.10	7000

You can modify the configuration of the ECM generator when you want, pushing  button. In addition, in case of communication loss between the headend and the CAS server, you can force the refresh of the communication pushing .

NOTE: Ikusi Flow allows the signal encryption with several CAS systems simultaneously. If that is your case, add as many ECM generators as you need.

Push SAVE button to store the configuration.

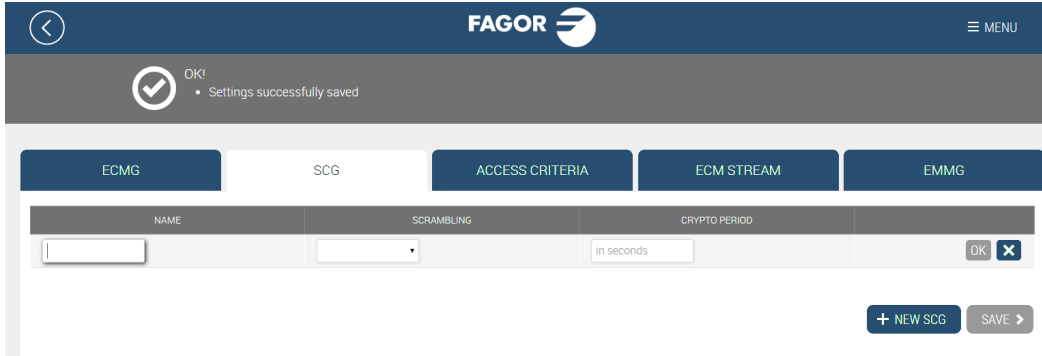
NOTE: Pushing SAVE button all the changes of every tab of the simulcrypt configuration are saved. Therefore, only is strictly necessary to do it in the last tab you modify. However, it is recommended to do it every time a change in any tab was done, in order to avoid accidental oblivions.

4.3 SCGs configuration

This tab is used to define the Scrambling Control Groups. They will be as many SCGs as different encryption keys used in the headend. Select SCG tab to access to this configuration.



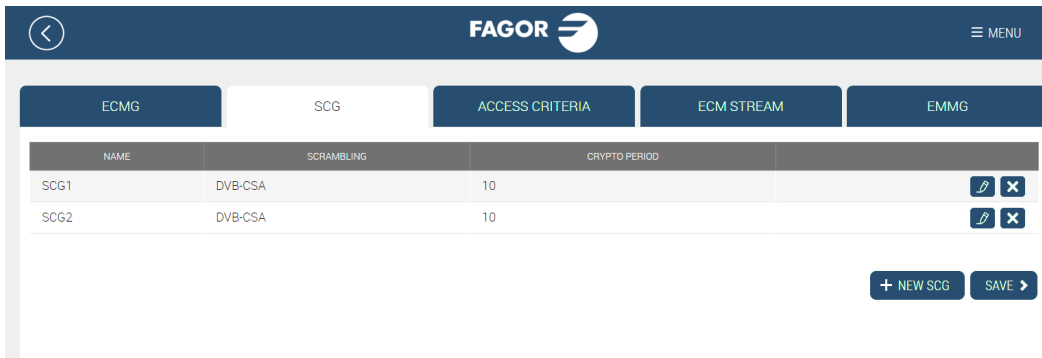
To add a SCG, click on + NEW SCG button. A row will be added, corresponding to the new Scrambling Control Group that you want to configure.



Fill in the parameters of the added SCG:

- **NAME:** is a free text field, used as internal reference to identify the SCG.
- **SCRAMBLING:** choose in the dropdown list the encryption system that you want to use.
- **CRYPTO PERIOD:** enter the period of validity of each key, in seconds. Confirm this value with the CAS vendor.

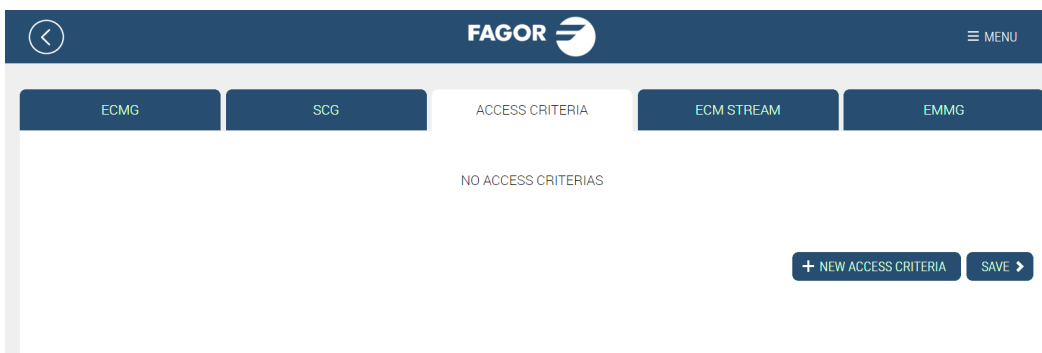
After finishing the configuration, push OK button. Repeat the same process to add as many SCGs as they are needed.



Push SAVE button to store the configuration.

4.4 Access Criteria configuration

This tab is used to define the Access Criteria, in the case there were any. This information is provided by the CAS vendor. Select ACCESS CRITERIA tab to access to this configuration.



To add an Access Criteria, click on + NEW ACCESS CRITERIA button. A row will be added, corresponding to the new Access Criteria that you want to configure.

Fill in the parameters of the added Access Criteria:

- **NAME:** is a free text field, used as internal reference to identify the Access Criteria.
- **ACCESS CRITERIA:** are 8 hexadecimal characters that will be provided by the CAS vendor. They must be introduced in hexadecimal format, preceded by "0x".

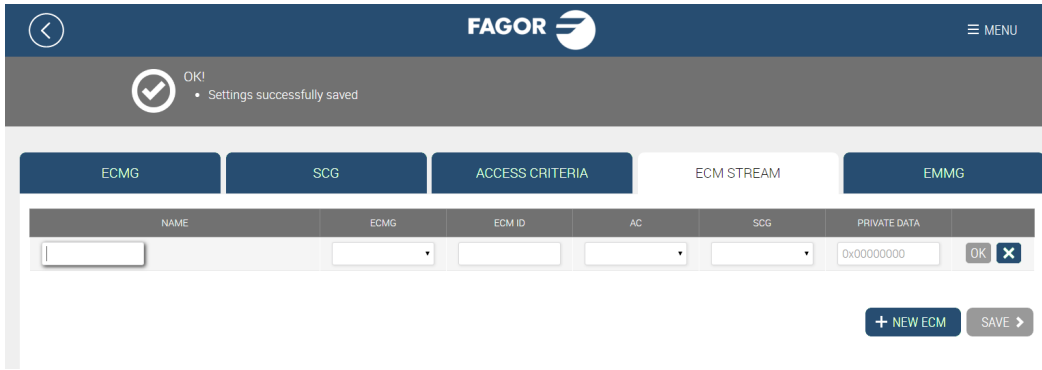
After finishing the configuration, push OK button. Repeat the same process to add as many Access Criteria as they are needed.

Push SAVE button to store the configuration.

4.5 ECM Streams configuration

This tab is used to define which ECM will be associated with each SCG. Select ECM STREAM tab to access to this configuration.

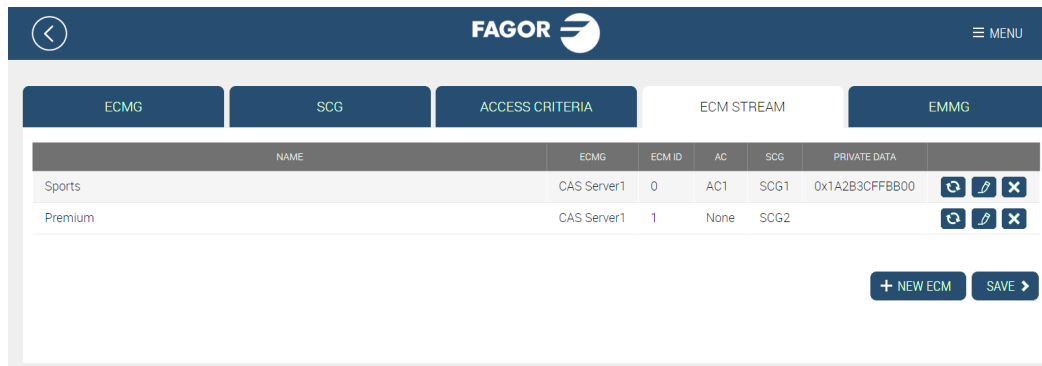
To add an ECM, click on + NEW ECM button. A row will be added, corresponding to the new ECM that you want to configure.



Fill in the parameters of the added ECM:

- **NAME:** is a free text field, used as internal reference to identify the ECM.
- **ECMG:** select in the dropdown list the ECM generator in charge of provide the ECM. All the ECM generators defined in ECMG tab will appear in the list.
- **ECM ID:** is an identifier of the ECM. It is a numeric value, between 0 and 65535, and it must be unique in the distribution network. This field can be leave void, and in that case, the headend itself will assign one. In other cases, the CAS system can require some specific values. Contact with the CAS vendor to confirm this point.
- **AC:** select in the dropdown list the Access Criteria that must be applied to the ECM that is being defined. All the Access Criteria defined in ACCESS CRITERIA tab will appear in the list. If the ECM is not linked to any Access Criteria, select "None" value.
- **SCG:** select in the dropdown list the Scrambling Control Group that will used the encryption key associated to the ECM that is being defined. All the Scrambling Control Groups defined in SCG tab will appear in the list.
- **PRIVATE DATA:** are the private data that will be included in the ca_descriptor of the PMT associated to the ECM that is being defined. They will be provided by the CAS vendor. They must be introduced in hexadecimal format, preceded by "0x". In the case the ca_descriptor doesn't include private data, leave the field void.

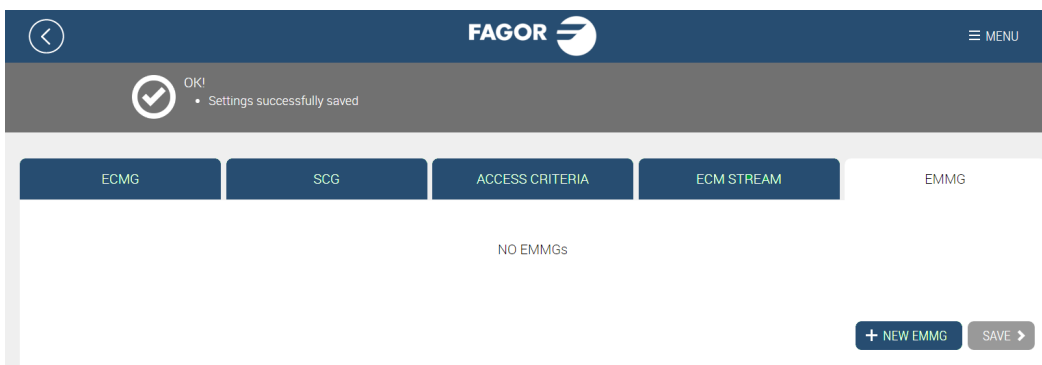
After finishing the configuration, push OK button. Repeat the same process to add as many ECM they are needed (each SCG must have at least one ECM for each ECMG).



Push SAVE button to store the configuration.

4.6 EMMGs configuration

This tab is used to define the parameters associated to the EMM generator. Select EMMG tab to access to this configuration.



To add an EMM generator, click on + NEW EMMG button. A row will be added, corresponding to the new EMMG that you want to configure.

Fill in the parameters of the added EMMG:

- **NAME:** is a free text field, used as internal reference to identify the EMMG.
- **CLIENT ID:** are 8 hexadecimal characters that will be provided by the CAS vendor. They must be introduced in hexadecimal format, preceded by "0x".
- **DATA ID:** is an identifier of the EMMG. It is a numeric value, between 0 and 65535, and it must be unique in the distribution network. This field can be left void, and in that case, the headend itself will assign one. In other cases, the CAS system can require some specific values. Contact with the CAS vendor to confirm this point.
- **BANDWIDTH:** is the maximum bandwidth that the Ikusi Flow instructs the EMMG to send.
- **PRIVATE DATA :** are the private data that will be included in the ca_descriptor of the CAT associated to the EMM that is being defined. They will be provided by the CAS vendor. They must be introduced in hexadecimal format, preceded by "0x". In the case the ca_descriptor doesn't include private data, leave the field void.

After finishing the configuration, push OK button.

NOTE: Ikusi Flow allows the signal encryption with several CAS systems simultaneously. If that is your case, add as many EMM generators as you need.

NOTE: The external CAS server will communicate with Ikusi Flow to send the EMMs. To do that, you should inform to that server in which IP address Ikusi Flow is located and which port it should use to perform the interchange of EMMs. You can find the IP address in the Installation Overview Report (MENU→STATUS→Overview), in the section corresponding to Network Configuration. The port used in the communication with the EMMG is 9998.

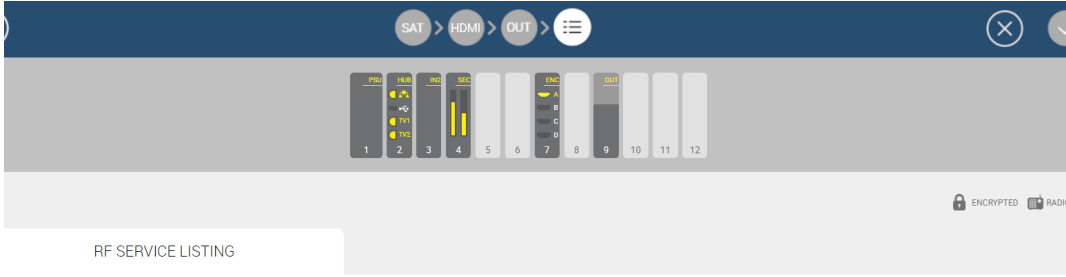
Push SAVE button to store the configuration.

4.7 Encryption allocation to each service

By default, after enabling the simulcrypt interface, all services that are managed by a FLOW SEC or FLOW ENC module will be encrypted, using the first Scrambling Control Group defined in the SCG tab.

In the case that a different SCG must be used in a specific service, you should modify the configuration of that service in the Service Wizard.

To do that, from Home screen push SERVICE WIZARD button. After the Wizard starts, go directly to the Summary screen, pushing  button.




Check the new services added, and if correct, click APPLY button.

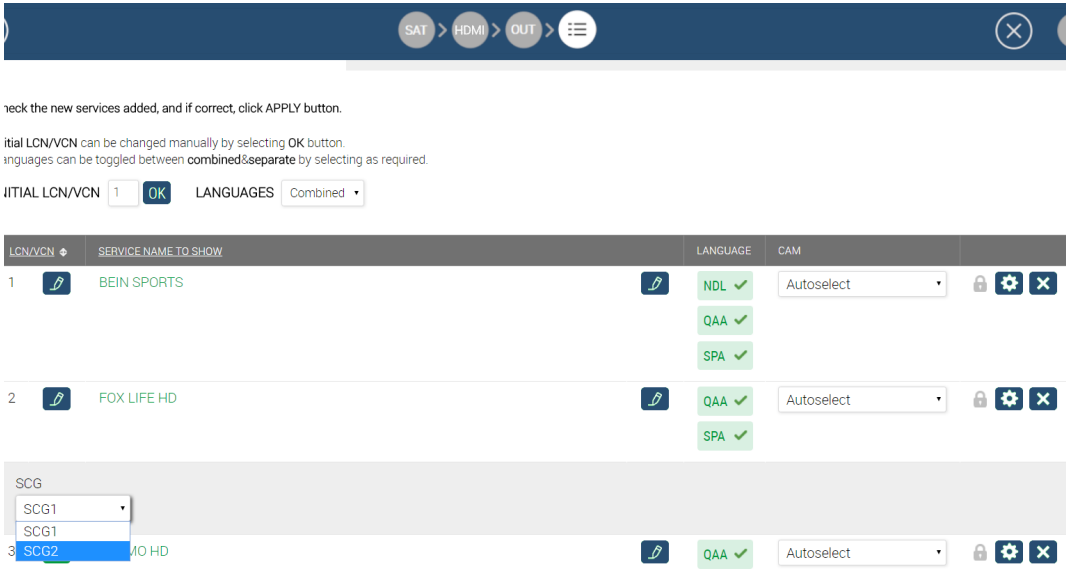
Initial LCN/VCN can be changed manually by selecting OK button.
Languages can be toggled between **combined** & **separate** by selecting as required.


INITIAL LCN/VCN LANGUAGES

LCN/VCN	SERVICE NAME TO SHOW	LANGUAGE	CAM
1	BEIN SPORTS	NDL ✓ QAA ✓ SPA ✓	Autoselect
2	FOX LIFE HD	QAA ✓	Autoselect

Select advanced configuration button  corresponding to the service that wants to change the associated SCG.


A row will open, where, among other parameters, you will find a dropdown list to choose the SCG that you want to apply to the service.


















Once the SCG assignment is modified in the desired service, push  button to apply the new configuration.

5. SIMULCRYPT INTERFACE STATUS CHECKING

Once the simulcrypt interface has been enabled, you can check its status in Home screen. There are three methods to check it has been enabled:

- In Home Screen, in service listing you can check that services processed by FLOW SEC and FLOW ENC modules are being protected with a DRM. They will be labelled with  icon.

RF SERVICE LISTING				
SVCN	SERVICE	SERVICE_NAME_TO_SHOW	LANGUAGE	
	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	

- Clicking over a FLOW SEC or FLOW ENC module a status screen will open. Among the information shown in this window, in the DRM section you could see that SimulCrypt is being used.


MODULE INFORMATION

SLOT NUMBER	5
SERIAL NUMBER	4311SB009316
HARDWARE VERSION	0
FIRMWARE VERSION	2.2.1+d20170327
TEMPERATURE	41°C
DRM	SimulCrypt

CAM 1



SEC

 REBOOT

- In the installation overview report appears if simulcrypt interface is being used in each FLOW SEC or FLOW ENC module. To obtain this report go to MENU→STATUS→Overview. A window with the whole information of the headend in detail will open. In each box dedicated to each FLOW SEC or FLOW ENC, in the DRM field, appears a text indicating SimulCrypt is being used.

Port number	5
Serial number	4311SB009316
Firmware version	0
Software version	2.2.1+d20170327
Temperature	41°C
Operating hours	533h
IM	SimulCrypt
IM 1 Inserted	yes
IM 1 In use	yes
IM 1 Use level	60%
IM 1 Manufacturer	SmarDTV
IM 1 Model	Movistar+ Pro CAM
IM 1 Services	FOX LIFE HD M. MOTOGP M.FORMULA1
IM 2 Inserted	yes
IM 2 In use	yes
IM 2 Use level	40%
IM 2 Manufacturer	SmarDTV
IM 2 Model	Movistar+ Pro CAM
IM 2 Services	BEIN SPORTS DISCOVERY



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

