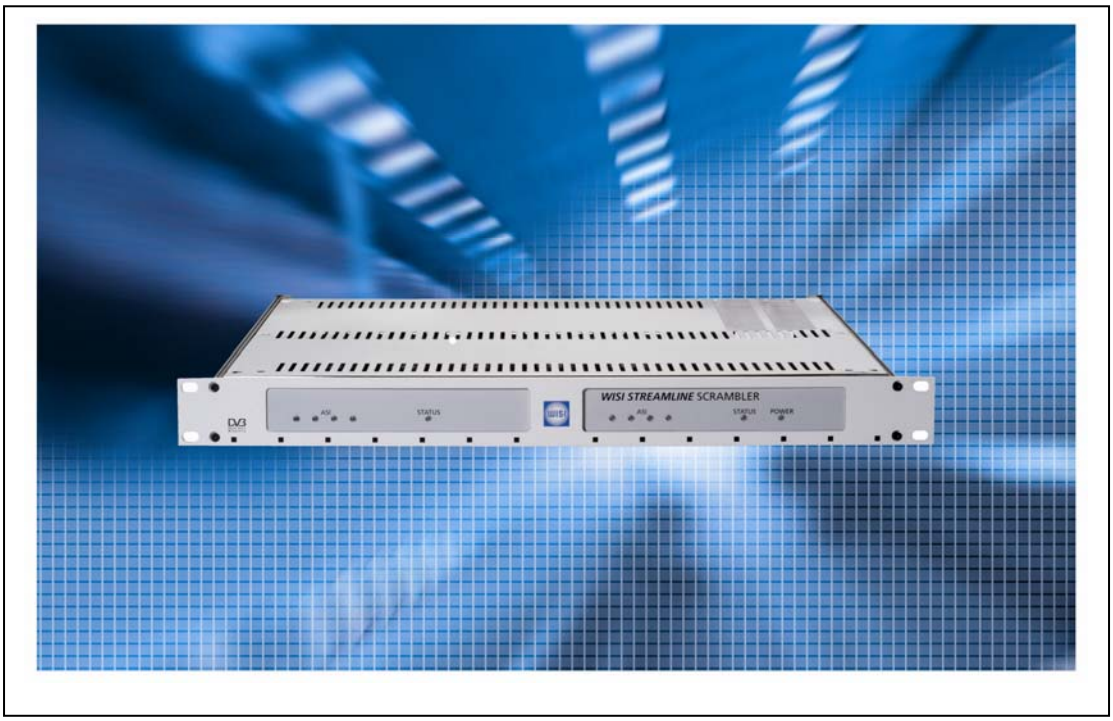
Operation Manual

OT 32 (Dual-) DVB-Scrambler



044 137

Index

SAFETY AND INSTALLATION NOTES PLEASE OBSERVE!

Caution
The mains voltage must match the rated input voltage of the unit (180-265 VAC; 50/60 Hz).

Connecting cable — Lay the cable so that no- one can trip over it.
— Lay the cable with a downward loop so that any water condensing on it can drip on the floor instead of running into the unit.

Selecting the installation location
Excessive temperatures will reduce the operating lifetime of the unit. DO not install the unit directly above or in the vicinity of radiators or heating systems where it would be subjected to thermal radiation or oil vapours.

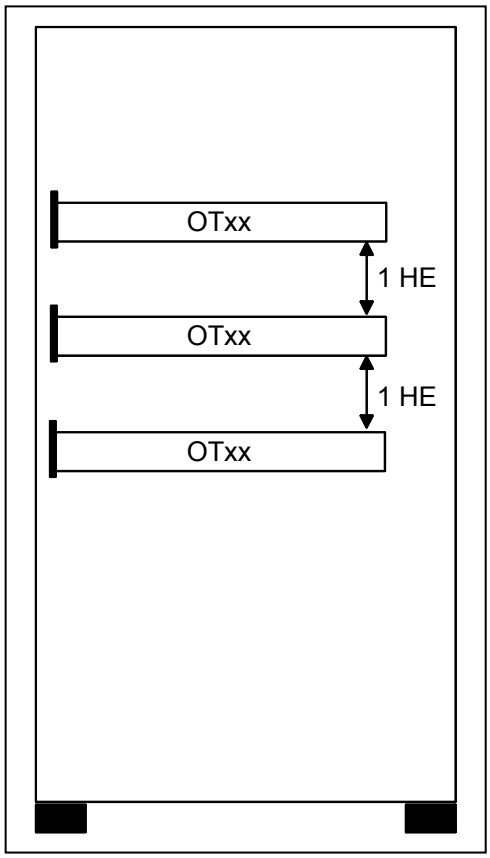
Ventilation slots
Do not cover the ventilation slots.

Moisture
Water dripping or splashing onto the unit will damage it. If there is condensation on the unit, wait until this has evaporated before switching the unit on.

Caution – danger!
In accordance with EN 50 083-1, the antenna system must comply with the safety requirements with respect to grounding, potential equalisation, etc.

Service work

Service work may be carried out only by qualified personnel. Always disconnect the power supply voltage before starting any such work.



1. Overview

1.1 System Introduction

OT 32 Scrambler is the equipment that scrambles selected programs of transport stream (TS) under the control of CAS, allows the only authorized user to receive and watch the programs. Thereby system operator can realize management of conditional charge. The equipment implements compatibleness with many CA systems by adopting universal scrambling arithmetic of DVB standard and data protocol of TCP standard.

1.2 Function Introduction

OT 32 (Dual-) DVB-Scrambler main functions:

- Stand alone Scrambler for DVB transport-stream signals
- Scrambling to selected programs or transport stream (SPTS/MPTS)
- Injecting of ECM and EMM from the CAS system into the transportstream
- Corrected PCR-jitter caused by injecting the EMM/ECM datas
- Compliant with DVB standard CAS systems
- Complicant with DVB Simulcrypt, supporting up to 4 CAS
- Effective input data rate 1-70 Mbps
- Packet length 188 and 204 supported
- Injection of EMM ECM data through Ethernet
- Common scrambling Algorithm used
- Generation of scrambling Control Word (CW)
- Managing of PSI/SI information related to CA
- TCP and UDP protocol supported
- Configuration via Webinterface and command line over TCP/IP
- SNMPv2c network management
- Expandibility to dual-scrambler

1.3 Front and rear panel

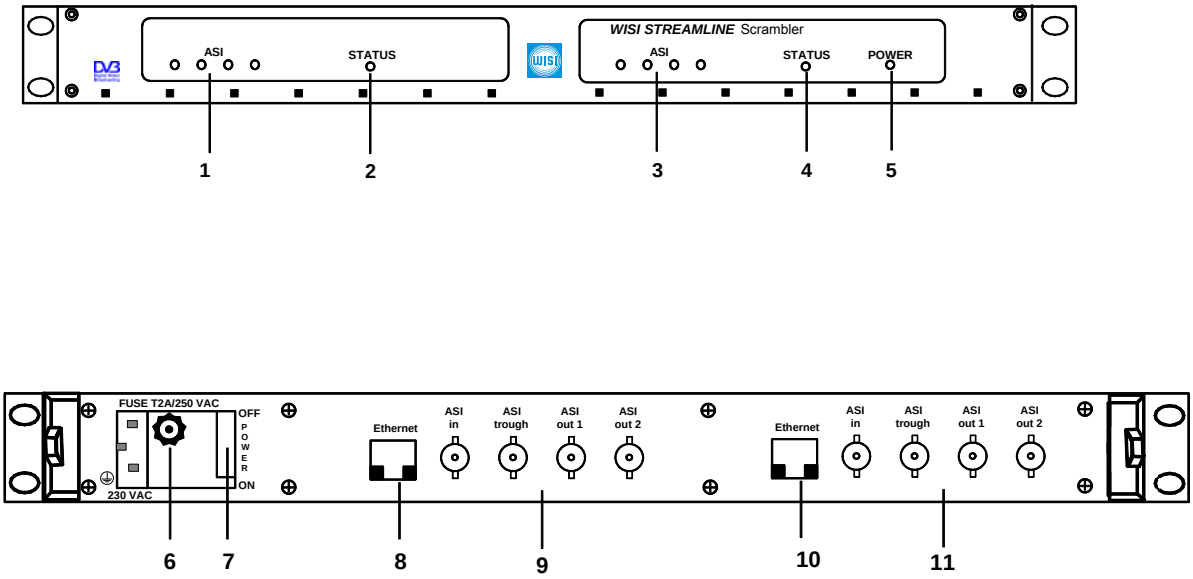


Figure 2-1 Stand-alone scrambler back panel interface

1,3	ASI interface LEDs	2, 4	STATUS LED
5	POWER LED	6	FUSE T2A/250 VAC
7	POWER ON/OFF.	8,10	100 Base/T.
9,11	ASI Interface		

2. Basic configuration of the device

For general every day administrative purposes the device supports:

- HTML web browser interface

For configuration of a brand new device a proprietary interface called "BCMD" = "broadcast command" interface is supported. For uploading new firmware and FPGA code, the TFTP interface is supported.

2.1 Configuring a brand new device

Generally the administrator will assign a fixed IP address to the scrambler. In the default state of the scrambler, there is no fix IP address defined.

2.2 Using the scrcmd tool to configure the IP address

This chapter describes the proposed method to configure a new device.

Attention: The method requests all scramblers in the network to return their current MAC address and IP address

However, its not necessary to compute the IP address to configure the scrambler first time. The scrambler supports a proprietary interface (called "BCMD" interface), that allows configuration using UDP broadcasts. The scrambler automatically activates the BCMD interface whenever there's no fix IP address defined.
The detection and enumeration of scramblers present in the network is done with a command line utility for Windows and Linux provided with the scrambler:

Enumerate all scramblers.!!

The tool will broadcast messages into the network, requesting all scramblers to return their current MAC address and IP address

scrcmd -enum

The return will look like this. The example shows two scramblers on the network:

[00] 00:11:22:33::44:55 169.254.1.85
[01] AA:BB:CC:DD::EE:FF 169.254.1.1

Please note: This list will also include devices which already have a fixed IP address assigned, if the BCMD interface is still enabled.

Set the IP address of a scrambler and reboot it.

The command reconfigures the IP address of the scrambler identified by the MAC address 00:11[...] to 172.29.0.130.

scrcmd -mac=00:11:22:33:44:55 -ip=172.29.0.130 -mask=255.255.0.0 –reboot

Identify the physical scrambler visually by its MAC address

The command causes the scrambler owning the MAC address 00:11[...] to flash its front panel LED red/green for some seconds:

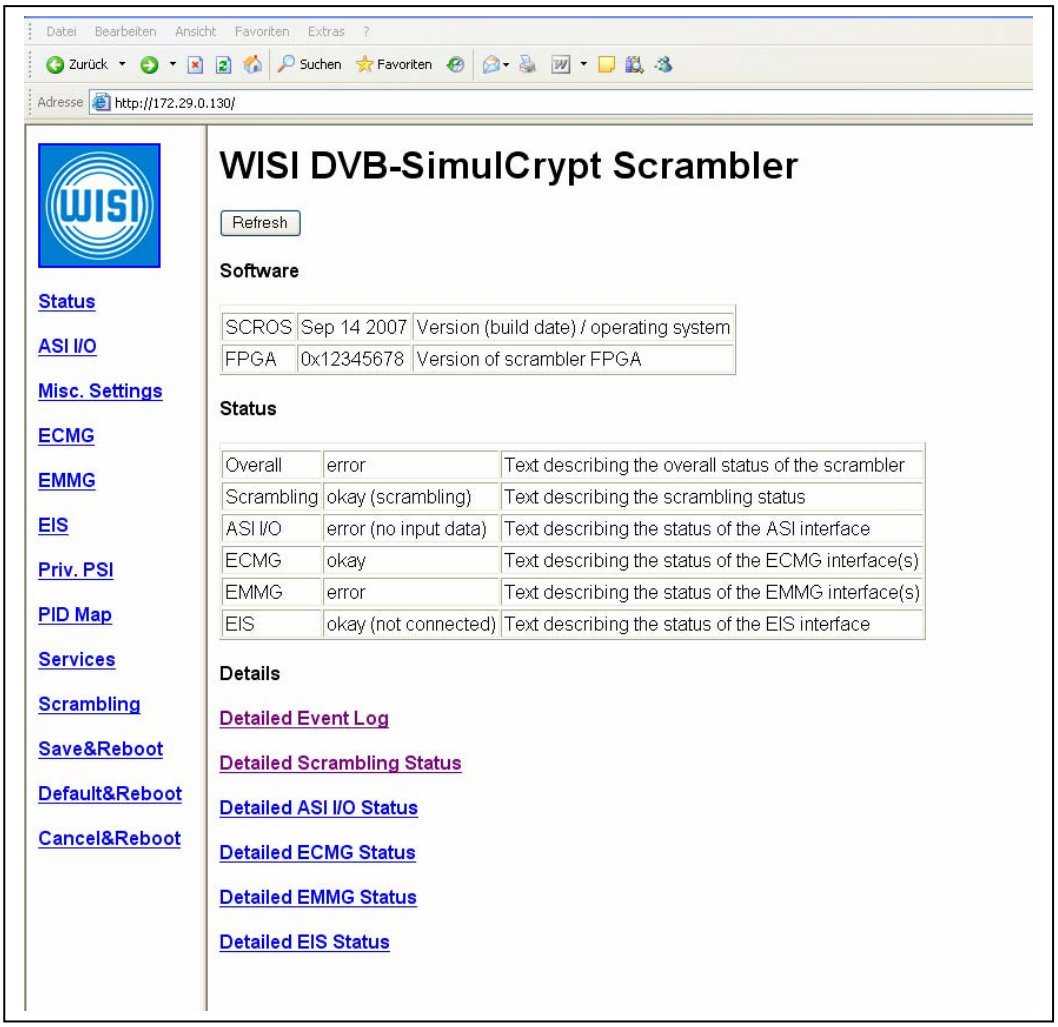
scrcmd -mac=00:11:22:33:44:55 –flash

3. Scrambling configuration (web browser interface)

The HTTP Interface consists of a menu frame on the left hand side and a parameter frame on the right hand side.
To open the HTML interface, open a web browser and enter the URL (replace 172.29.0.130 by the IP address of your device):

http://172.29.0.130

This will automatically open the "Status View" page shown below. The Status page is the index page of the HTML interface. It will automatically show if you access the scrambler, or if you click on Status. This page shows version numbers and an overall description of the scrambler status. The example below shows the scrambler in an erroneous state, because thereis no transport stream present on the ASI input connector:



To setup the scrambler you step through almost every menu item (in the menu bar on the left hand side) from top to bottom and modify the settings according to your DVB headend setup. When you are done with the setup you click on "Save&Reboot" to store the settings permanently and restart the scrambler, which will – after the restart - be working as configured.

To make modifications to settings, click into the corresponding edit box, alter the value and then click on the "Submit" button located on the upper left corner of the HTML page. The scrambler will then process the modifications. It will possibly limit some values automatically, so they remain in the allowed operating range.
The status pages, like shown above, do not have a "Submit" button, but a button named "Refresh". You click on this button, to refresh the contents of the status variables.
The scrambler presents information to the administrator mainly using tables. These tables either have 3 or 6 columns. The first column contains a short name of the parameter presented in this row. The last column usually contains a short description of the parameter, it may be empty, if there is no description available. In between the short parameter name and the description is the data field, that contains the content of the parameter. Some tables present only one data column, other present 4 data columns to the administrator.

3.1 Input fields

Each input field has a specific data format:

Numeric input fields: The scrambler accepts both hexadecimal numbers (Starting with "0x") and decimal numbers in numeric data fields. Numeric input fields are for example used to define port numbers. Acceptable numbers are for example:

0x201
513
0xFFFFFF00

The scrambler will present the number in numeric fields either as decimal or as hexadecimal values, depending on whatever is suitable for this input field. For example: Port numbers are usually decimal, while the CAS-ID is presented as a hex value. Independent of the preferred presentation, you can always enter hex. or dec. values in numeric input fields.

IP address input field: The scrambler accepts an IP address in the format "a.b.c.d" here. For example:

172.29.0.130

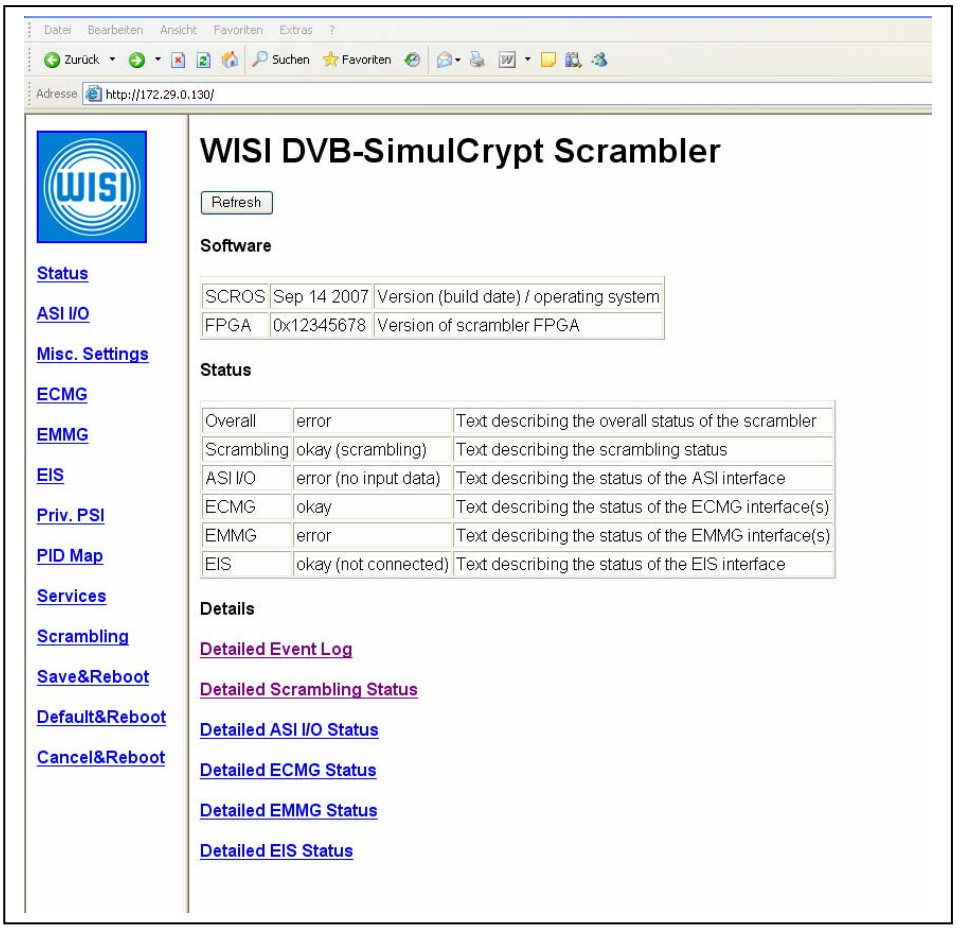
Hexadecimal string input fields: The scrambler accepts a string of characters "0..9" and "A..F" and "a..f." **without** a leading "0x". While numeric input fields only accept values, that fit into 32Bit variables (or less), the hexadecimal string input fields accept a much longer string of hexadecimal values. The hexadecimal string input fields are (for example) used to define "access criteria" and private data to be inserted into the CAT (for example). Example:

A076B300005F

String input fields: The scrambler accepts a string of characters. String input fields are for example used for naming Scrambling Control Groups.
Although many values take effect immediately, some values can only be applied after a reboot and some will take effect only after a transponder scan.

3.2 Status Page

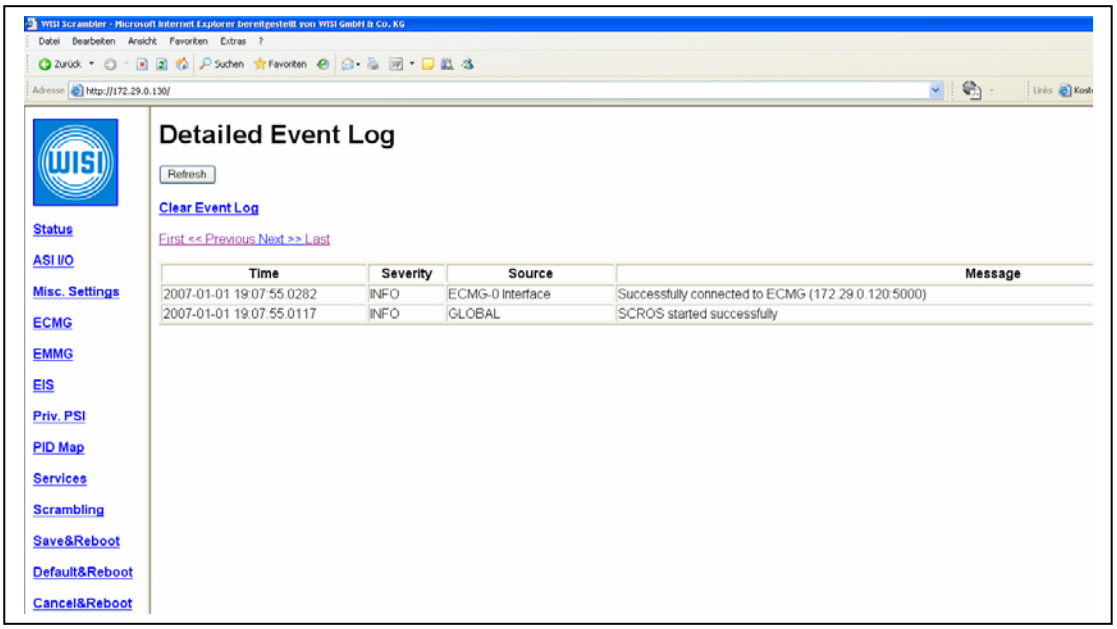
The Status page is the index page of the HTML interface. It will automatically show if you access the scrambler, or if you click on Status in the menu bar on the left hand side. This page shows version numbers and an overall description of the scrambler status. The example below shows the scrambler in an erroneous state, because there is no transport stream present on the ASI input connector:



The Status page contains links that lead to status pages of some functional units of the scrambler. For example: The ECMG parameter page has its associated ECMG status page. These detailed status pages are described elsewhere in this document.
The first table on the status page contains the versions of the scrambler software:
· SCROS: Build date of the operating system. The build date is used as the "version number".
· FPGA: Version number of the FPGA code.

3.3 Detailed Event Log

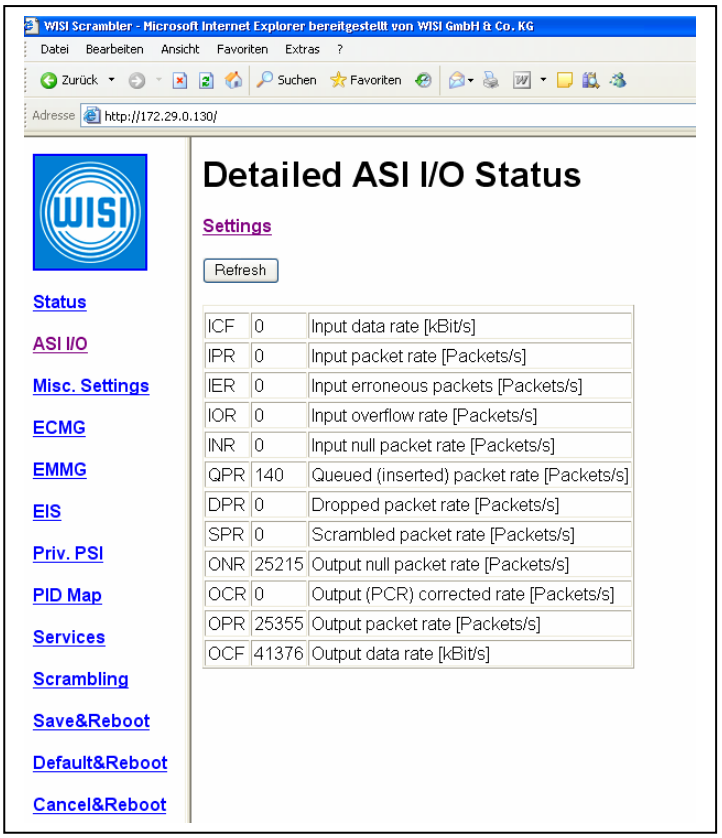
The detailed event log is accessed by clicking on "Status" in the menu bar on the left hand side and then on the link "Detailed Event Log". The "Event log" is a table, storing:
· The time when an event occurred
· The severity (INFO = informational, ERROR = error condition)
· The functional unit of the scrambler that caused the event.
· A message describing the event.
The "Detailed Event Log" consists of multiple pages. You navigate this pages by clicking on "First", "Previous", "Next" or "Last". In the case of the event log, clicking on "First" shows the oldest, and "Last" the latest events.



3.4 ASI I/O Settings Page

The ASI I/O Settings page lets you configure the data rate and data format of the output transport stream.

3.5 ASI I/O Status Page



The ASI I/O Status Pages shows the status of the ASI input and output. The content will be updated when you press “Refresh”.

- **Input data rate**: Detected data rate on the ASI input.

- **Input packet rate**: Number of transport stream packets per second arriving on the ASI input.

- **Input erroneous packet**: Number of transport stream packets containing errors per second arriving on the ASI input.

- **Input overflow rate**: Number of times, the input fifo of the scrambler overflowed.

- **Input null packet rate**: Number of null transport stream packets (PID 0x1FFF) per second arriving on the ASI input.

- **Queued (inserted) packet rate**: Number of transport stream packets inserted into the transport stream by the scrambler. This value includes ECM, EMM, PAT, CAT and PMT transport stream packets being inserted.

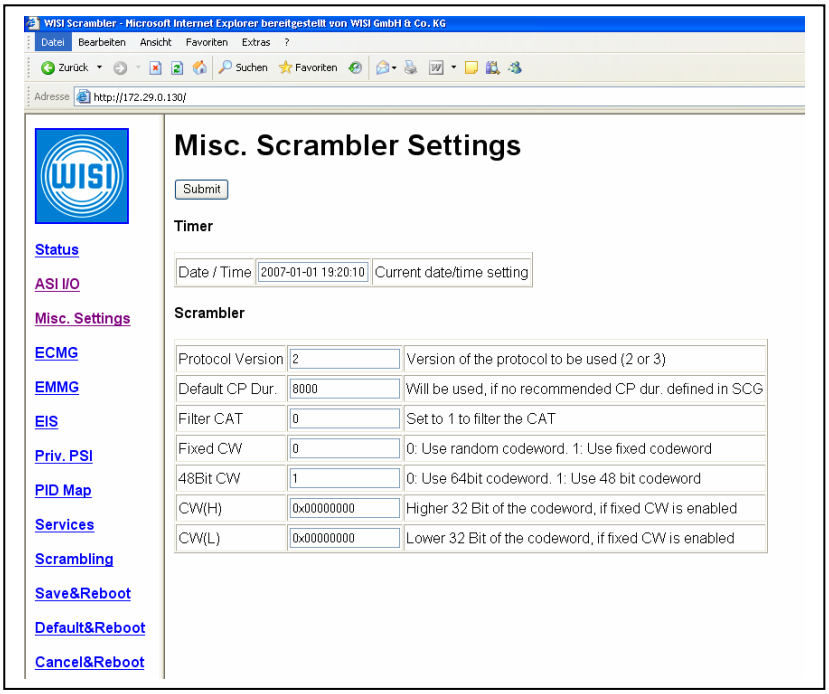
- **Dropped packet rate**: Number of transport stream packets, that the scrambler removes on the input side. The scrambler drops PAT, CAT and PMT and all packets arriving on reserved ECM / EMM PID´s.

- **Scrambled packet rate**: Number of transport stream packets, that were scrambled by the scrambler per second.

- **Output null packet rate**: Number of null packets generated by the scrambler per second to meet the output data rate.

- **Output data rate**: The data rate being output on the ASI.
  Please note: The "Input null packet rate" has to be bigger than the "Queued (inserted) packet rate". If the "Queued (inserted) packet rate" is bigger than the "Input null packet rate" for an extended amount of time, the resulting output transport stream becomes erroneous.
  Also, if the "Output null packet rate" is 0 or very low for extended periods, this also indicates an scrambler overload.

3.6 Misc. Settings Page



This page lets you setup miscellaneous settings:

- **Date/Time**: Enter the current date and time here. The format is YYYY-MM-DD HH:MM:SS. You have to set the current date and time only, if you plan to use activation times in Scrambling Control Groups.

- **Protocol Version**: Selects the ECMG protocol to be used (2 or 3).

- **Default CP Duration**: The scrambler supports different crypto period (CP) durations for every Scrambling Control Group. If you don't specify a CP duration for a Scrambling Control Group, the scrambler will automatically use the value specified here. The minimum value is 8000 (= 8 seconds) crypto period duration.

- **Filter CAT**: If 0, the scrambler will take the original CAT present in the input transport stream and append its own CA descriptors. If the value is 1 (nonzero), the scrambler will ignore the content of the original CAT and generate a new one, containing only CA descriptors generated by the scrambler.

- **Fixed CW**: If 0, the scrambler will use random codewords (CW) to scramble the content. If 1 (nonzero), the scrambler will use a fixed CW as defined below. The value

1 should only be used for debugging purposes of course!

- **48Bit CW**: If 0, the scrambler will use 64 Bit codewords to scramble the content. If 1 (nonzero), the scrambler will use 48Bit codewords. Some CAS only support the 48Bit mode.
- **CW(H):** This is the high dword of the fixed codeword to be used, if Fixed CW is 1.
- **CW(L):** This is the low dword of the fixed codeword to be used, if Fixed CW is 1.

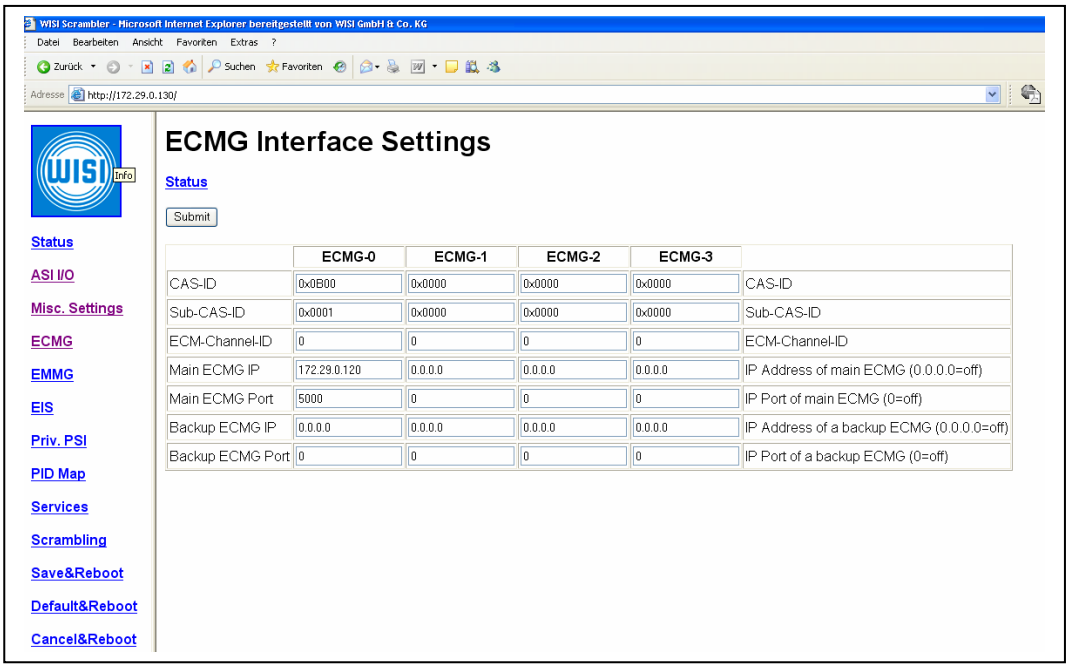
3.7 ECMG Settings Page

The scrambler supports up to 4 different ECMGs in parallel. Depending on your application you have one up to eight ECMGs attached. If one is connected only, you are running your system with one CAS and without backup. If you have eight ECMGs attached, you are running your system with four CAS and one backup for every CAS.

Every of the four columns is used to configure the main and backup IP addresses and ports of one CAS. If you set the IP address to 0.0.0.0 or the port to 0, you disable the associated CAS.

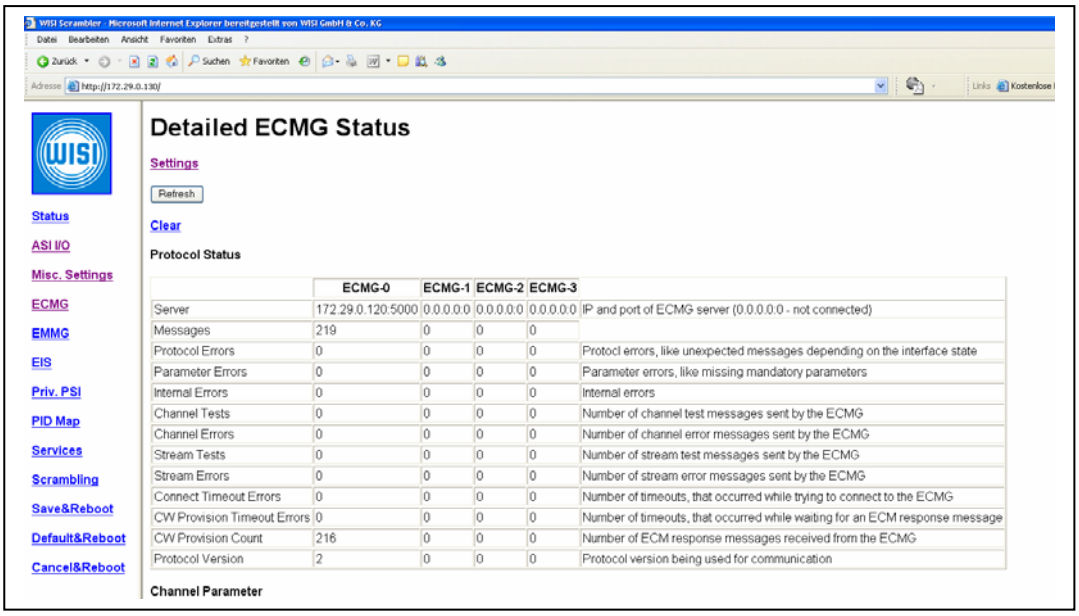
The CAS-ID and Sub-CAS-ID depend on the CAS you are using in your environment.

The following example shows one CAS with both main and backup ECMGs activated (Row ECMG-0). All other CAS are disabled. The main ECMG is accessed on port 5000 of 10.0.0.70, the backup ECMG is accessed on port 6000 of 10.0.0.70. Of course its possible to have different IP addresses for main and backup ECMG.



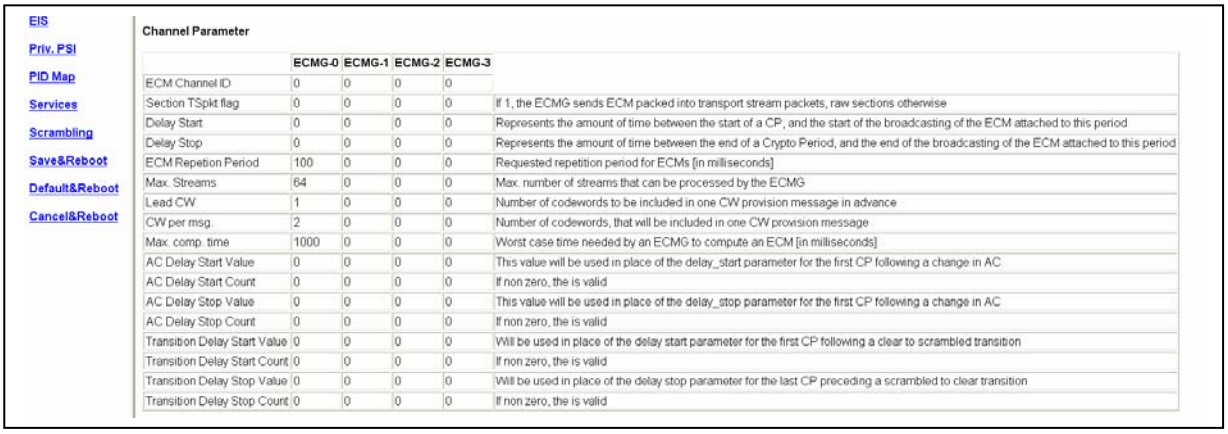
3.8 ECMG Status Page

The ECMG Status Page consists of two parts. The upper part lets you verify the connection and communication between ECMG and the scrambler.



	ECMG-0	ECMG-1	ECMG-2	ECMG-3	
Server	172.29.0.120:5000	0.0.0.0:0	0.0.0.0:0	0.0.0.0:0	IP and port of ECMG server (0.0.0.0:0 - not connected)
Messages	219	0	0	0	
Protocol Errors	0	0	0	0	Protocl errors, like unexpected messages depending on the interface state
Parameter Errors	0	0	0	0	Parameter errors, like missing mandatory parameters
Internal Errors	0	0	0	0	Internal errors
Channel Tests	0	0	0	0	Number of channel test messages sent by the ECMG
Channel Errors	0	0	0	0	Number of channel error messages sent by the ECMG
Stream Tests	0	0	0	0	Number of stream test messages sent by the ECMG
Stream Errors	0	0	0	0	Number of stream error messages sent by the ECMG
Connect Timeout Errors	0	0	0	0	Number of timeouts, that occurred while trying to connect to the ECMG
CW Provision Timeout Errors	0	0	0	0	Number of timeouts, that occurred while waiting for an ECM response message
CW Provision Count	216	0	0	0	Number of ECM response messages received from the ECMG
Protocol Version	2	0	0	0	Protocol version being used for communication

Use the scrollbar of your browser to reach the bottom part of the ECMG Status. The bottom part informs you about the DVB SimulCrypt parameters that the scrambler and ECMG agreed on using. See the DVB SimulCrypt specification for a detailed description of the meaning of each parameter.



	ECMG-0	ECMG-1	ECMG-2	ECMG-3	
ECM Channel ID	0	0	0	0	
Section TSpkt flag	0	0	0	0	If 1, the ECMG sends ECM packed into transport stream packets, raw sections otherwise
Delay Start	0	0	0	0	Represents the amount of time between the start of a CP, and the start of the broadcasting of the ECM attached to this period
Delay Stop	0	0	0	0	Represents the amount of time between the end of a Crypto Period, and the end of the broadcasting of the ECM attached to this period
ECM Repetion Period	100	0	0	0	Requested repetition period for ECMs [in milliseconds]
Max. Streams	64	0	0	0	Max. number of streams that can be processed by the ECMG
Lead CW	1	0	0	0	Number of codewords to be included in one CW provision message in advance
CW per msg.	2	0	0	0	Number of codewords, that will be included in one CW provision message
Max. comp. time	1000	0	0	0	Worst case time needed by an ECMG to compute an ECM [in milliseconds]
AC Delay Start Value	0	0	0	0	This value will be used in place of the delay_start parameter for the first CP following a change in AC
AC Delay Start Count	0	0	0	0	If non zero, the is valid
AC Delay Stop Value	0	0	0	0	This value will be used in place of the delay_stop parameter for the first CP following a change in AC
AC Delay Stop Count	0	0	0	0	If non zero, the is valid
Transition Delay Start Value	0	0	0	0	Will be used in place of the delay start parameter for the first CP following a clear to scrambled transition
Transition Delay Start Count	0	0	0	0	If non zero, the is valid
Transition Delay Stop Value	0	0	0	0	Will be used in place of the delay stop parameter for the last CP preceding a scrambled to clear transition
Transition Delay Stop Count	0	0	0	0	If non zero, the is valid

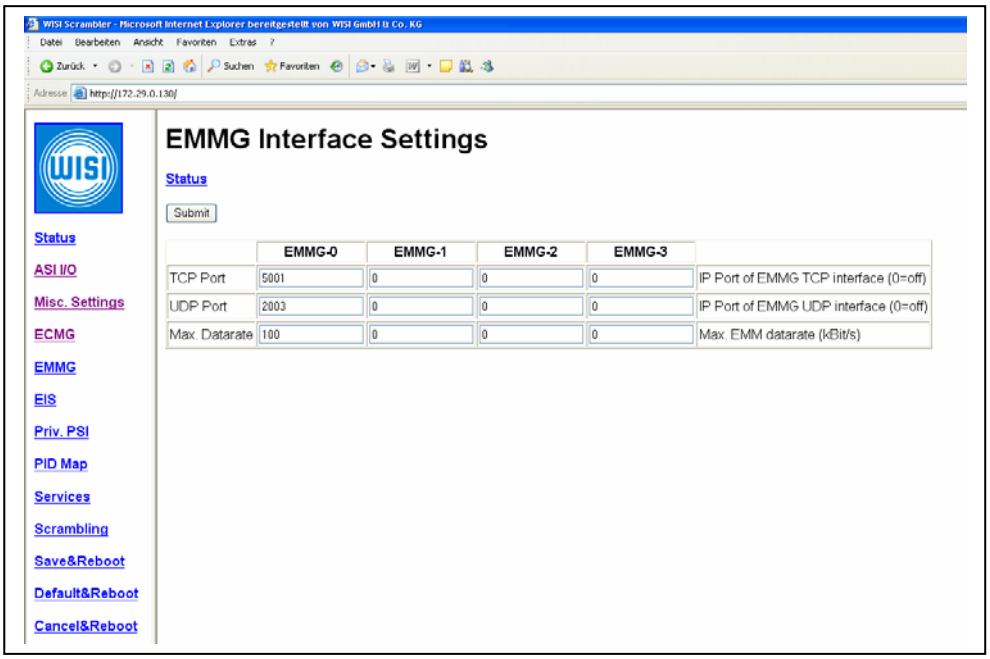
3.9 EMMG Settings Page

The scrambler is capable of being connected to four EMMGs. You define the ports to listen to EMMG requests on this page. For each of the four EMMGs there are two ports to be defined:

- The TCP Port
- The UDP Port

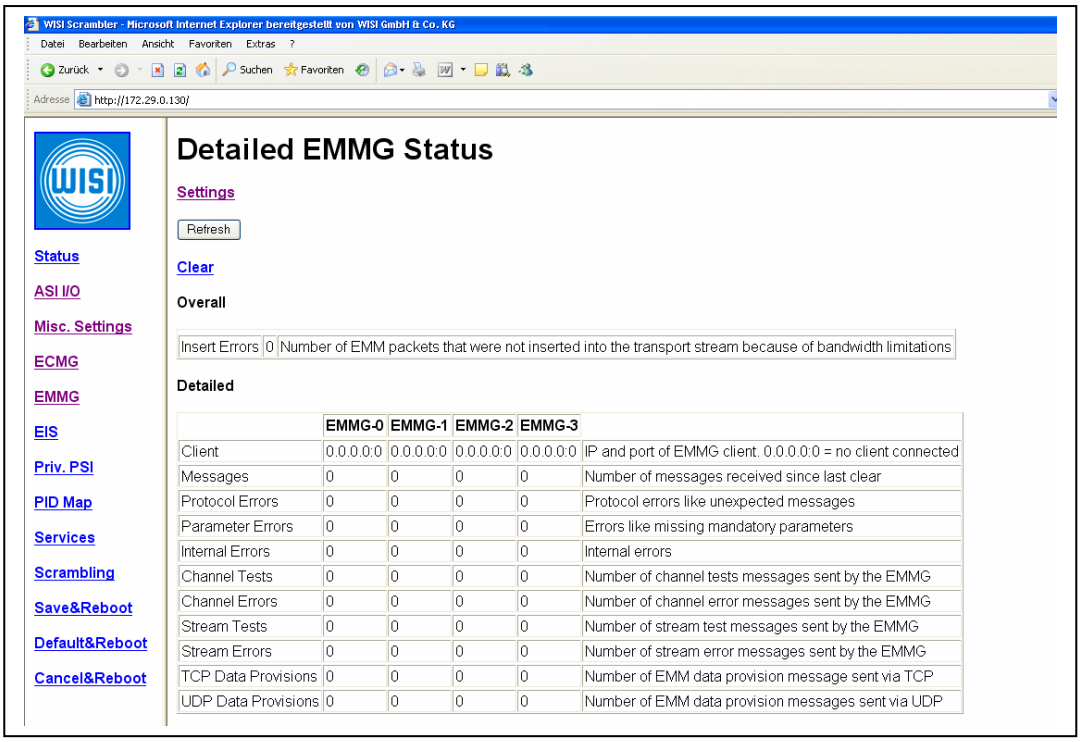
To deactivate an EMMG interface, set the associated TCP Port to 0. The UDP interface does not work without the TCP interface activated, while the TCP interface is capable of working alone.

The example shows a configuration, that lets the scrambler listen on port TCP port 5001 for EMMG requests, like EMM provisions. It will also accept EMM provisions on UDP port 2003.
The data rate parameter sets the max. amount of data being granted for the EMM data stream. Please note: The actual amount of data rate available for EMMs and ECMs depends on the ASI I/O settings. For example: Its possible to grant 1MBit/s EMM rate here, but there is no chance for the scrambler to pack these EMM packets into a physical transport stream being attached to the scrambler at the desired rate. It's the responsibility of the headend administrator to ensure, that there are enough null packets in the transportstream to meet this setting here.



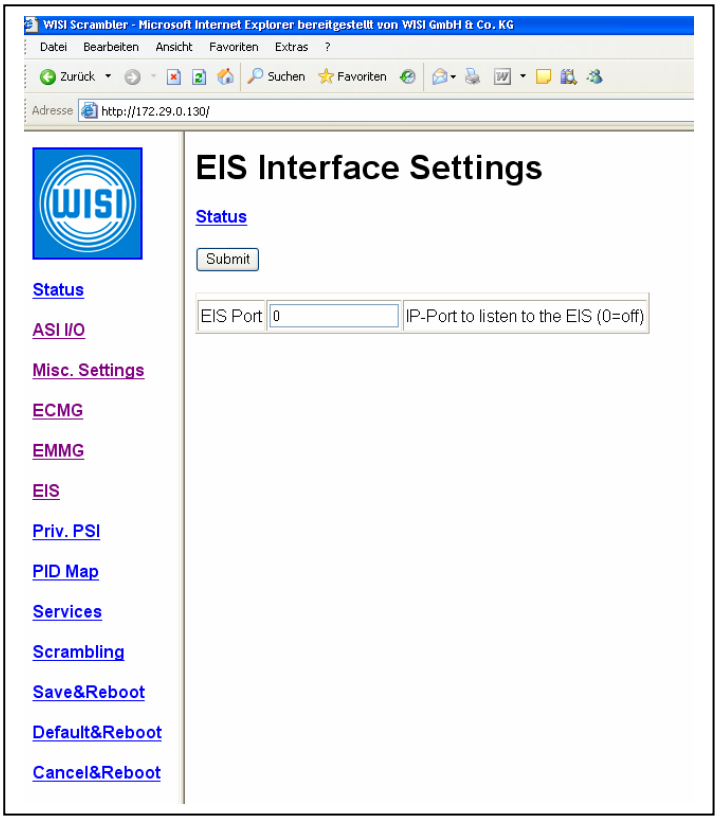
3.10 Detailed EMMG Status Page

The "Detailed EMMG Status" Page lets you verify the connection with the EMMG. If there is an EMMG connected to the scrambler, the "Client" row will show the IP and source-port of the connected EMMG. "0.0.0.0.0:0" means, that there is no EMMG connected.
The rest of the entries count messages and errors. In the case of an error free connection, you will see "Messages" and "TCP Data provisions" and / or "UDP Data provisions" increase, while all other values of a column remain 0 (or do not increase).



3.11 EIS Settings Page

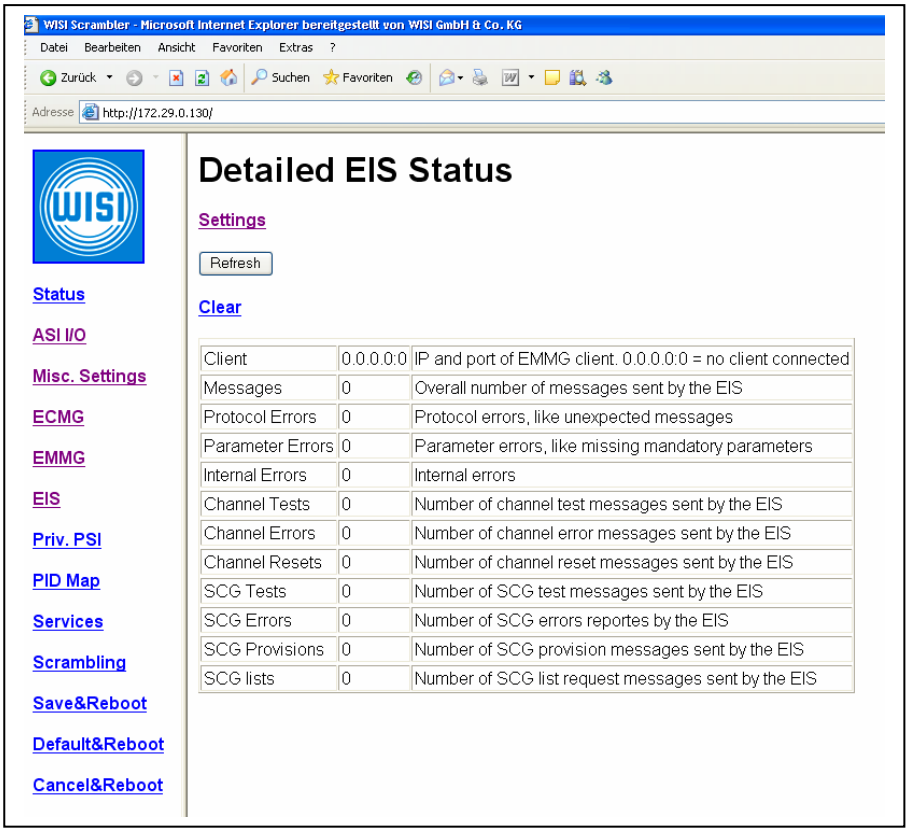
The EIS is an (external) software component that defines Scrambling Control Groups. It connects to the scrambler using TCP/IP. The scrambler will listen on the specific port for message of the EIS. If you want to disable the EIS interface, set the value to 0.



It is possible to verify the Scrambling Control Groups that were defined by an EIS, by clicking on "Scrambling" in the menu bar.

3.12 Detailed EIS Status Page

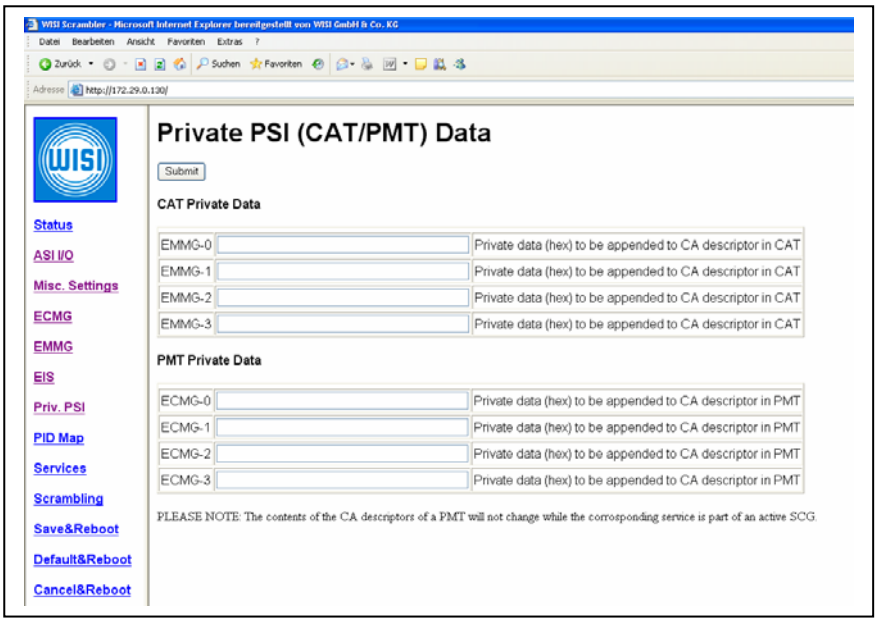
The EIS status page lets you check the communication between the EIS and the scrambler.



Client	0.0.0.0:0	IP and port of EMMG client. 0.0.0.0:0 = no client connected
Messages	0	Overall number of messages sent by the EIS
Protocol Errors	0	Protocol errors, like unexpected messages
Parameter Errors	0	Parameter errors, like missing mandatory parameters
Internal Errors	0	Internal errors
Channel Tests	0	Number of channel test messages sent by the EIS
Channel Errors	0	Number of channel error messages sent by the EIS
Channel Resets	0	Number of channel reset messages sent by the EIS
SCG Tests	0	Number of SCG test messages sent by the EIS
SCG Errors	0	Number of SCG errors reportes by the EIS
SCG Provisions	0	Number of SCG provision messages sent by the EIS
SCG lists	0	Number of SCG list request messages sent by the EIS

3.13 Private PSI (CAT/PMT) Data Page

The scrambler inserts private PSI data into the CA descriptors. Enter the hexadecimal string of the private PSI data to be inserted into the edit boxes, then press the "Submit" button.

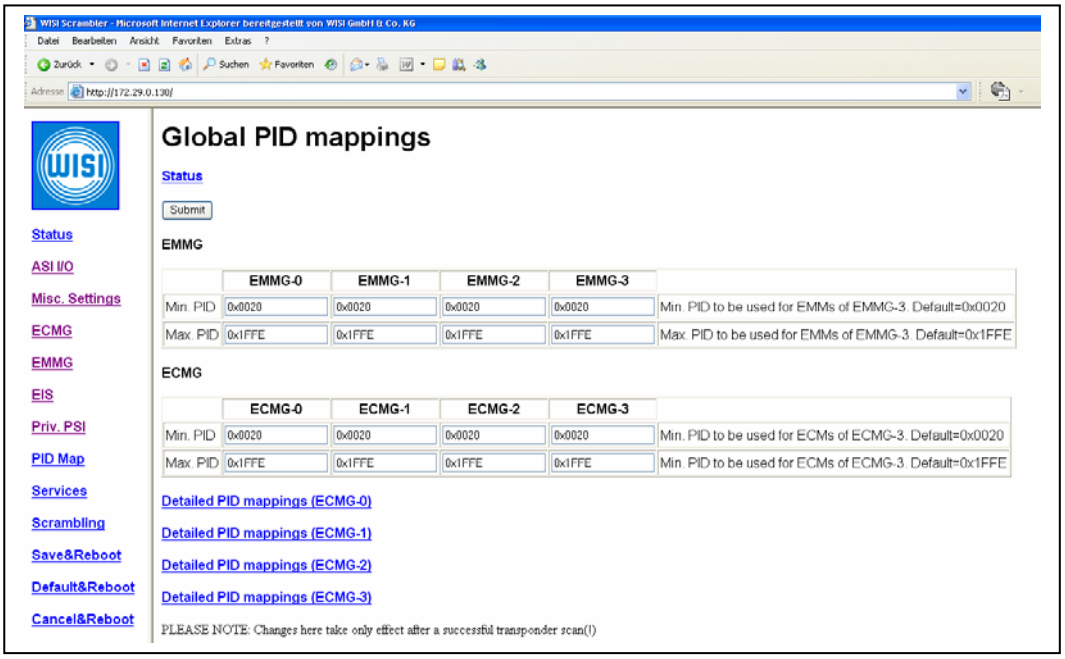


The content of the CA descriptors of the CAT will change immediately (within 500ms). The contents of the CA descriptors in a PMT will only change when the corresponding services switches from clear to scrambled. If you use Save&Reboot after the whole setup, you can be sure, that your private data will be used.
Please note: There is no need for private PSI data, if your head end conforms to the DVB head end standard.
ATTENTION! You have to take care by yourself, that the size of the PMT section containing your private data and all CA descriptors does not exceed the maximum size when using private data.

3.14 Global PID mappings Page

This page enables the administrator to define PID ranges to be used for placing ECM and EMM PID´s. The scrambler supports up to 4 ECM generators and up to 256 Scrambling Control Groups. Therefore the scrambler needs up to 1024 (free) PID´s to be used as ECM PID´s.

The PID´s will be automatically assigned by the scrambler after a successful scan. The scrambler tries to allocate the PID´s in the given ranges, taking PIDs into account, that are already in use. The scrambler analyzes the PAT, CAT and PMT´s during the scanning to find PID´s, that cannot be used as ECM or EMM PID´s.

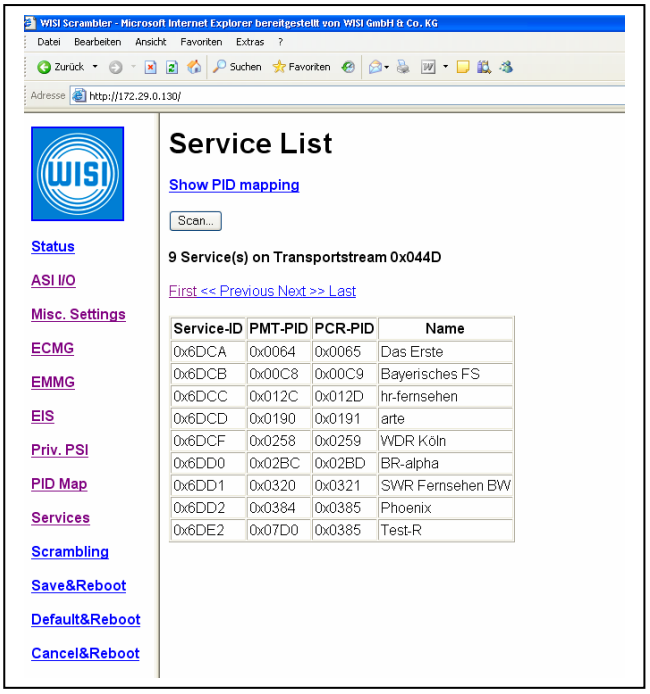


3.15 Current PID Mapping Page

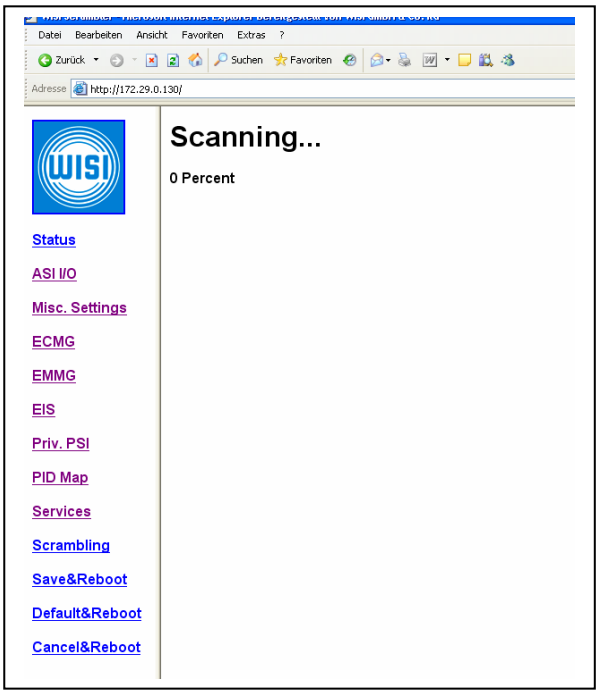
3.16 Service List Page

The Service List page lets you scan the services of the transport stream applied to the ASI Input of the scrambler.

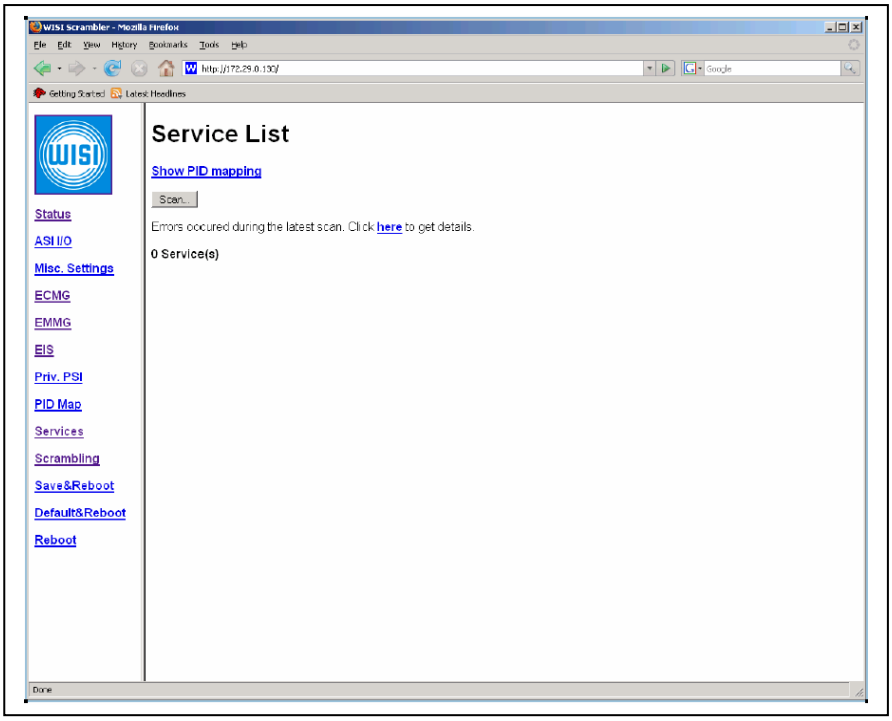
The look of the services page differs, depending on the number of scanned services. If no services are scanned, then the services page notifies you about it like shown below.



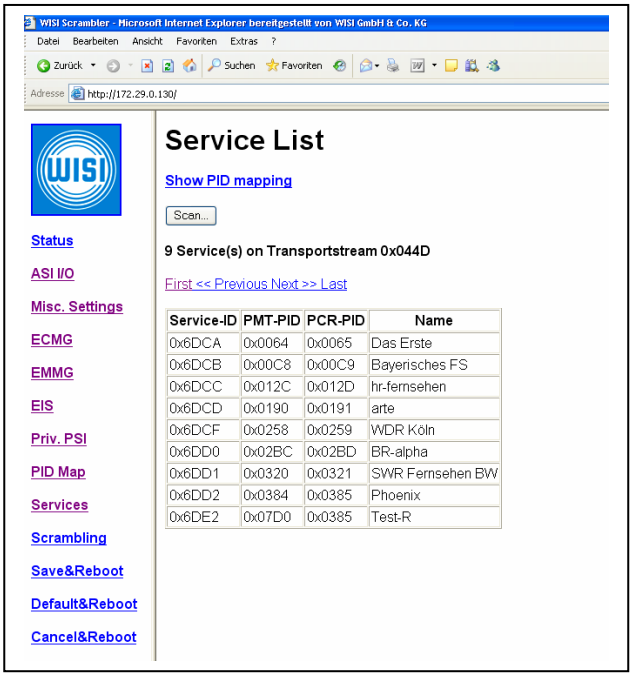
To scan for services, click on the "Scan" button. During scan the page looks like below. If the web browser supports timed updates, the page will be update automatically every 5 seconds and notify you about the scanning progress. If the web browser does not automatically update the page every 5 seconds, you have to manually click on "Services" link in the menu bar once about every 5 seconds to update the scanning progress.



If an error occurs you will get the following information when the scan finishes:



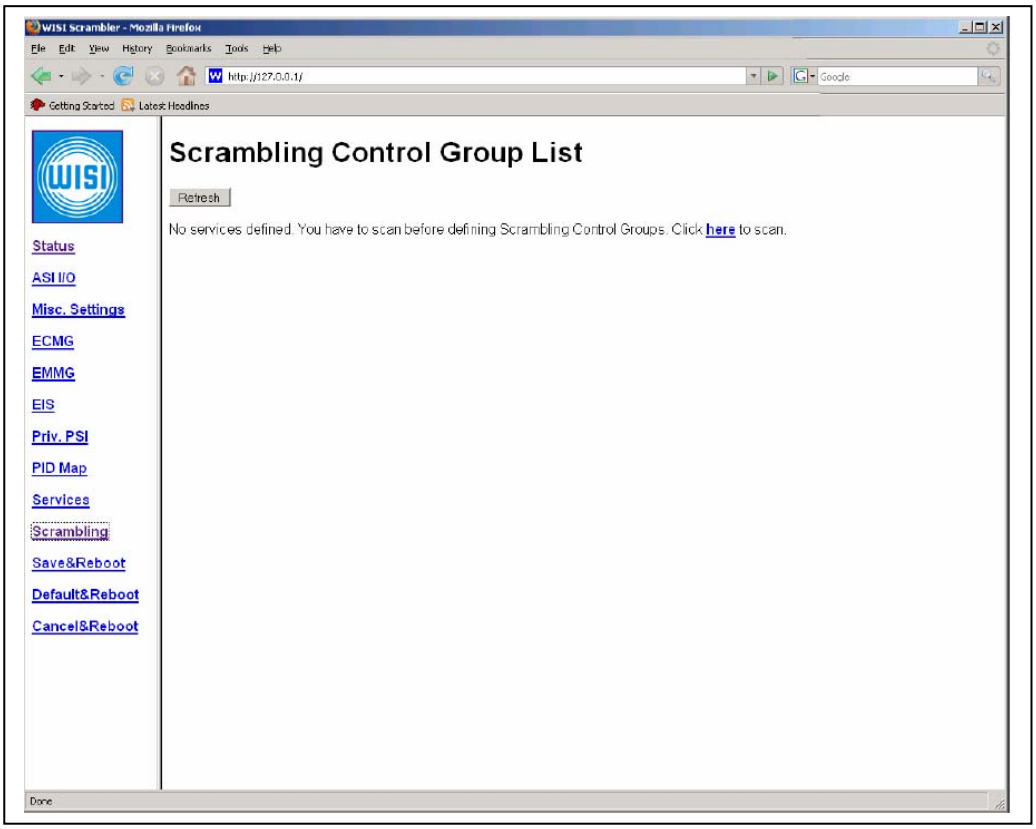
The link "here" will lead you to the "Detailed Event Log" which contains some more detailed information about the reason of the failure.
If everything works well the scrambler will present a list of services like shown in the example below.



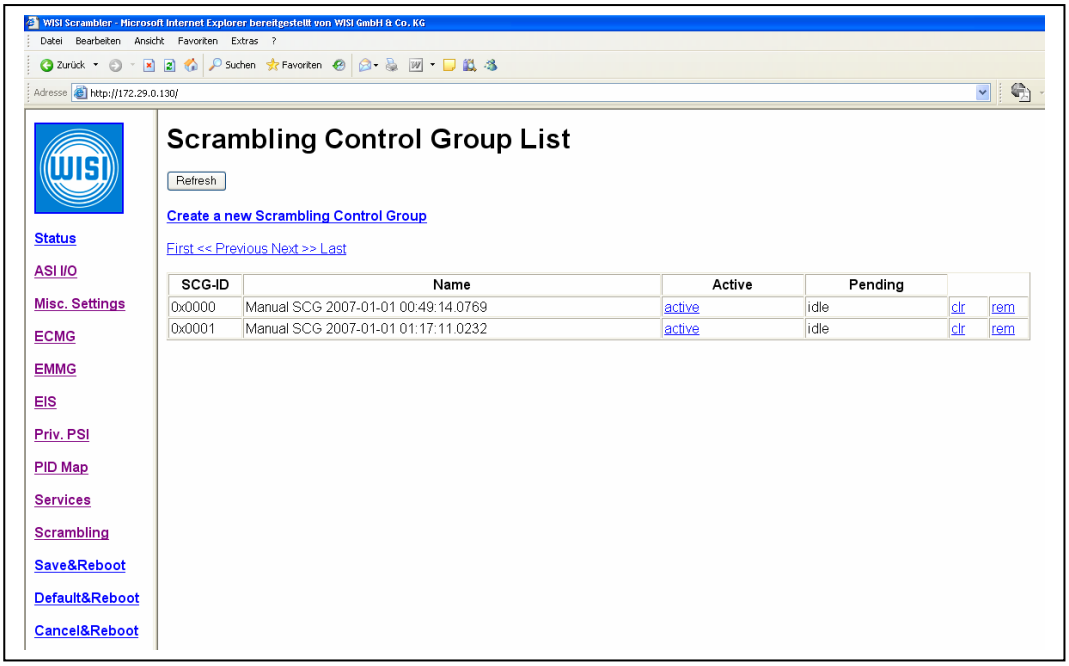
Please note: Scanning is an important process, because in the case of a successful scanning, the scrambler will clear all currently defined Scrambling Control Groups! Also after a successful scanning, the PID mappings become activated.

3.17 Scrambling Control Group List

A Scrambling Control Group (SCG) is a bundle of services to be scrambled at the same time using the same codeword and the same access criteria for specific ECMG.
The look of the scrambling page differs, depending on the number of scanned services. If no services are scanned, then the scrambling page notifies you about it and links to the services page. You may either click on "Services" in the menu bar or on the "here" link to get to the Services page. Its not possible to define Scrambling Control Groups before you successful scanned a transponder.



If there are services scanned, but no Scrambling Control Group is actually defined, clicking on "Scrambling" in the menu bar automatically opens the "Edit new SCG" page (See the appropriate chapter for a detailed description of this page)
If there are Scrambling Control Groups defined, this page lists them. If the list is too long to fit on this page, you may use the "First", "Previous", "Next" and "Last" links to navigate through the list.
Clicking on the "Refresh" button refreshes the contents of this page.



The Scrambling Control Group (SCG) lists consists of 6 columns.

• **SCG-ID**: This is the ID of the Scrambling Control Group. Its an unique number identifying the SCG. You may manually define this value on the "Edit (new) SCG Page". If you don't define the value, the scrambler chooses one automatically.

• **Name**: The name of the SCG. This name is a string of characters and its use is to be a mnemonic for the SCG contents. You select this name in the "Edit (new) SCG Page). For example, if this SCG contains scrambled cartoon programs, you may call it "Cartoon Package". If you don't define a name, the scrambler chooses one automatically.

• **Active**: The "Active" column contains the codeword "idle" or "active" or a date/time like "2007-01-01 15:00:00". "Idle" indicates, that the SCG is not active = does not actually scramble any content. "Active" or the date/time indicates, that the SCG is currently active = does scramble content. The date/time in addition to "active" indicates the activation time, when the scrambling started. You may click on the "active" codeword (or the date/time) to open the "Edit (new) SCG page". This lets you verify the services currently being scrambled by this SCG (and also the other scrambling parameters, for example access criteria).

• **Pending**: The "Pending" column contains the codeword "idle" or "active" or a date/time. If "idle" there is no change in the SCG pending. If "active", the scrambling of the SCG will change as soon as possible (depending on the workload of the scrambler) the "active" will be replaced by idle soon. If there is a date/time, the SCG change will occur at the given time. You may click on the "active" codeword (or the date/time) to open the "Edit (new) SCG page". This lets you verify the services currently being scrambled by this SCG (and also the other scrambling parameters like access criteria). Every new or edited SCG appears as pending for some seconds, even if it has no activation time.

• **Clr**: This is an abbreviation for "clear". If you click on this link, the scrambler will schedule a deprovision of all services scrambled by this SCG. This means, that all services will as soon as possible become free-to-air (clear / not scrambled). This scheduled clear will replace any currently pending operation.

• **Rem**: This is an abbreviation for "remove". If you click on this link, the scrambler will remove the content of the "Pending" column. Its useful for removing any pending operation (possibly scheduled for a given date/time), without changing the status of scrambling.

The scrambler does not distinguish between Scrambling Control Groups defined by the EIS or SCG´s defined manually by the web browser interface. Although both kinds of Scrambling Control Groups are handled the same way, the name of SCG´s provisioned by the EIS begins with "EIS", while SCG´s defined manually begin with "Manual" if the scrambler automatically chooses a name.
To create a new Scrambling Control Group, click on the link "Create new scrambling control group", this will open the "Edit (new) SCG" Page. See below.

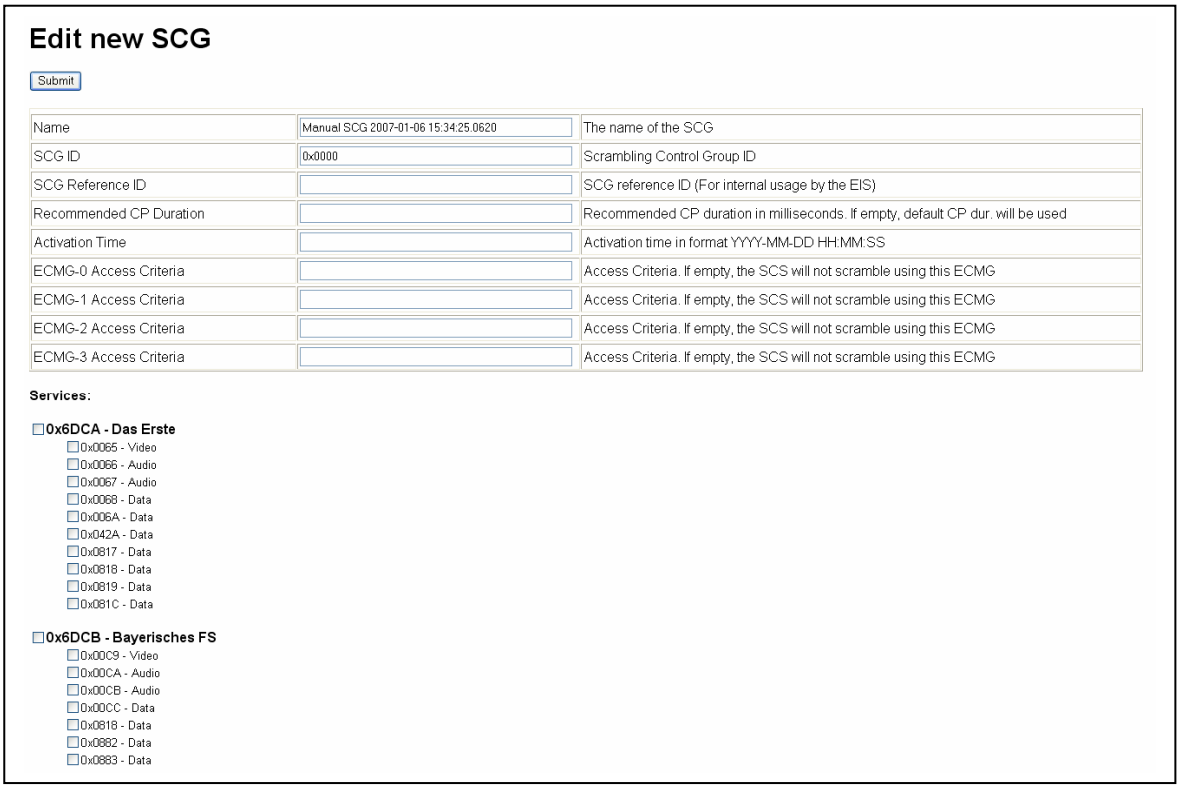
3.18 Edit (new) SCG Page

The scrambler shows the following page, if you

• Click on "Create new scrambling control group" on the "Scrambling Control Group List" page.

• If you click on "Scrambling" in the menu bar and there scanned services but currently no Scrambling Control Groups defined.

The page consist of two parts. The upper part containing scrambling parameters to be applied by the scrambler. The bottom part contains a list of services.



The parameters in the upper part are:

• **Name**: This is a string of characters. It is just used as a mnemonic to identify the Scrambling Control Group for the administrator.

• **SCG ID**: This word variable used as a handle of the Scrambling Control Group. This parameter is of importance if you use the EIS interface. The EIS uses this value as an unique identifier. If you don't use the EIS interface (define SCG´s manually) then you don't need to change the value (automatically choosen by the SCG)

• **SCG Reference ID**: This double word value is used by the EIS only. Its presented for administrative purposes when you are using an EIS to define Scrambling Control Groups.

• **Recommended CP Duration**: This value is the length of the crypto period in milliseconds. If you leave this field empty, the scrambler will use the default crypto period duration (see Misc. Settings). The minimum crypto period duration of the scrambler is 8000ms. The scrambler will round smaller durations up to 8000ms.

• **Activation Time**: This value defines the time when the scrambler will activate the Scrambling Control Group. The activation time has the format "YYYY-MM-DD HH:MM:SS". Until this time, the SCG will be marked as "pending" in the Scrambling Control Group List. If you leave this field empty, no activation time will be defined and the Scrambling Control Group will be activated as soon as possible. Please note:

Even without an activation time defined, the SCG will be marked pending for some seconds, until the scrambler is able to process the request.

• **ECMG-0 Access Criteria**: This field contains a hexadecimal string, defining the access criteria of the Scrambling Control Group of the first ECMG. The exact content to be included here depends on the CAS.

• **ECMG-1 Access Criteria**: Same as "ECMG-0 Access Criteria", but for the second ECMG.

• **ECMG-2 Access Criteria**: Same as "ECMG-0 Access Criteria", but for the third ECMG.

• **ECMG-3 Access Criteria**: Same as "ECMG-0 Access Criteria", but for the fourth ECMG.

The bottom part of the page lists services and the components of each service (like video elementary stream, multiple audio elementary streams).

The content of the list depends on the currently scanned services and other currently defined Scrambling Control Groups. The content of the list also differs, if you are editing and existing Scrambling Control Group, or if you are defining a new one.

Each service can be part of one Scrambling Control Group only. Service means, that at least one component of the service is part of one Scrambling Control Group. For example: It is not

possible to have the video component of a service in an SCG with ID "0x0001" while the audio components of the same service are part of an SCG with ID "0x0002" (another SCG). If you define a new Scrambling Control Group, the list contains all services, which are currently not part of other defined Scrambling Control Groups. So the list contains the services, that you are free to scramble.

If you edit an existing Scrambling Control Group, the list contains all services, that are currently part of the Scrambling Control Group.

3.19 Provision a new Scrambling Control Group

The following description shows the minimum steps necessary to scramble one or more service.

• Click on "Create a new Scrambling Control Group" on the "Scrambling Control Group List" page. This will automatically choose a name and an appropriate SCG ID.

• Enter the access criteria hexadecimal strings for each CAS to be used. At least one filed of the 4 access criteria fields needs to be filled, to scramble. If you leave a CAS entry empty, the service(s) will remain free-to-air for users of this CAS.

• Then check the service or component (or multiple services/components) in the bottom part of the page. If there are many services available you might need to scroll the page down in the browser. If you check the box to the left of the service name, all components of the service will be scrambled. This is the same effect as if you would check all component check boxes of the service. If you want to scramble single components only, uncheck the box left to the service name and check the appropriate boxes to the left of the component.

• Click on Submit. The scrambler will present the "Scrambling Control Group List" page, where you will find the new SCG (identified by name and ID).
Please note: If you include multiple services in one Scrambling Control Group, all services will be scrambled using the same codeword and will be using the same access criteria. If you want each service to be scrambled with a different codeword (although possibly using the same access criteria), you have to define a separate SCG for every service.

3.20 Modifying an existing Scrambling Control Group

In the "Scrambling Control Group List" page click on the "active" or date link in the list of the appropriate Scrambling Control Group. The scrambler will show the "Edit SCG" page. The bottom part will include a list of services, consisting of services, that are currently being scrambled (having check marks on at least one component) and services that are currently free-to-air, but could be scrambled in the future. The latter services having no check marks. For example: If you want a currently scrambled component to be free-to-air in the future, uncheck the appropriate component and then click on "Submit" button.

For example: If you want a currently free-to-air service / component to become scrambled in the future, check the appropriate component and click on the "Submit" button.
For example: If you want the access criteria to change, modify the appropriate hexadecimal access criteria string and click on the "Submit" button.

Of course, you may also mix an access criteria and scrambling state change.

3.21 Deprovision of an existing Scrambling Control Group

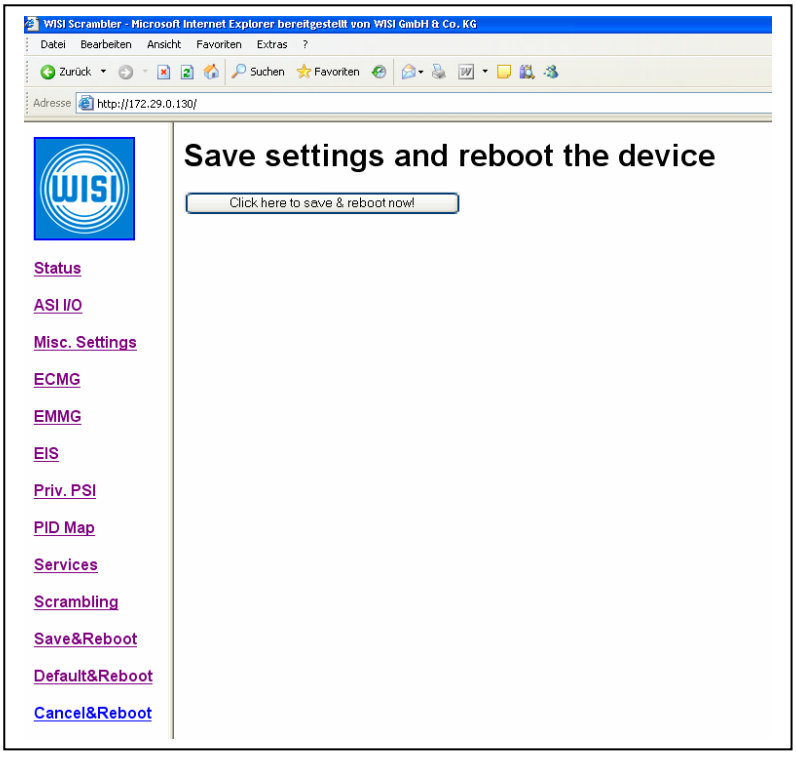
Deprovision means, that all services of a Scrambling Control Group will become free-to-air services. There are several ways to deprovision an existing Scrambling Control Group. One way is to click the appropriate "clr" link in the SCG list of the "Scrambling Control Group List" page.

Another way is to edit the Scrambling Control Group as described under "Modifying an existing Scrambling Control Group". To deprovision the SCG, you just have to clear all contents of all access criteria input fields and then click on the "Submit" button. You may enter an activation time, to schedule the deprovisioning in the future.

After processing the deprovision, the scrambler will remove the Scrambling Control Group from the list.

3.22 Save&Reboot

If you click on "Save&Reboot" in the menu bar on the left hand side, the scrambler returns the following page:



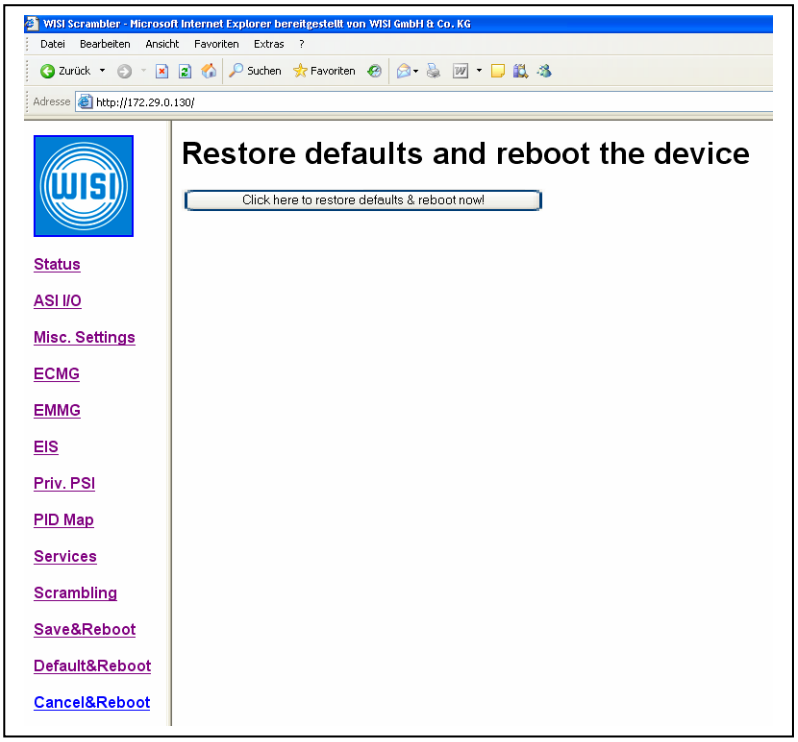
To save the current settings into the flash and reboot the scrambler, click on the button named "Click here to save & reboot". There will be no reply. the scrambler will start the shutdown as soon as possible. During the shutdown the settings will be saved into the flash. This may take about 90 seconds. During this time, the scrambler lights all front panel LEDs red (power yellow).

Note: Do not turn off power, while the LED´s indicate RED. If you turn off power during the flash process,your current settings will be lost and the scrambler will use default settings after the reboot.

The scrambler will save all currently active and the pending Scrambling Control Groups. It will also store the clock and adjusts it by an approximate boot process duration after the reboot. However, if you are using the "Activation time" feature of the scrambler, you have to manually adjust the current date/time after a reboot in the "Misc. Settings", to setup the exact date/time.

3.23 Default&Reboot

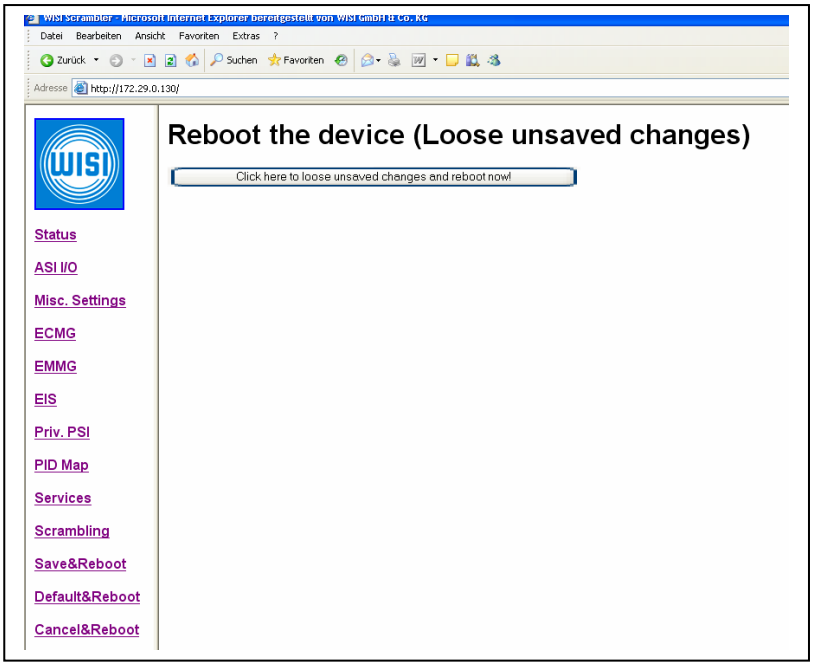
If you click on "Default&Reboot" in the menu bar on the left hand side, the scrambler returns the following page:



Click on the button to clear the contents of the settings in the flash memory and reboot the device. This option clears **all** settings including IP address settings.

3.24 Cancel&Reboot

If you click on "Cancel&Reboot" in the menu bar on the left hand side, the scrambler returns the following page:



Click on the button, to destroy all temporary unsaved changes and reboot the scrambler using the settings currently stored in the flash memory. All changes made since the last reboot will be lost.

4. Specifications

ASI – receiver (input)

ASI – receiver (input)

Data format	DVB A010 ASI-C, EN50083-0
Packet framing	188 / 204 byte per packet
Bitrate	270 Mbps
ASI mode	Burst or Continous
Signal level	200 mV (p-p)
Max. signal level	800 mV (p-p)
Output impedance	75 Ω
Input return loss	> 17 dB (5-270 MHz)

ASI – transmitter (output)

Data format	DVB A010 ASI-C, EN50083-0
Packet framing	188 / 204 byte per packet
Bitrate	270 Mbps
ASI mode	Burst
Signal level	800 mV (p-p)
Output impedance	75 Ω
Output return loss	> 17 dB (5-270 MHz)
Deterministic Jitter	10 %
Random Jitter	8 %

Control

Interface	100Base-T Ethernet
Userinterface 1	Web-based
Userinterface 2	Command Line
Monitoring and Alarm	SNMPv2c

Applicable standards

ETSI TR 102 035 Implementation Guidelines of the DVB Simulcrypt Standard
ETSI TS 101 197 DVB Simulcrypt: Head-end architecture and synchnisation
ETSI TS 103 197 Headend implementation of DVB Simulcrypt

3. General data

Housing	19 “ 1HE
Size	440 x 440 x 40 mm
Scrambler	PCB 150 x 350 mm

Signaling

1 x power led green
2 x operating led green
2 x alarm led red

Connectors

ASI-input	BNC-connector
ASI-throughput	BNC-connector
ASI-output	1 BNC-connector
ASI-output	2 BNC-connector
Control	Ethernet

Power supply

	100 - 240 VAC
	3,3 V (± 2%) 5000 mA DC max.
	5,0 V (+ 4/- 2%) 5000 mA DC max.
	200 mA DC min.

	12,0 V (± 8%) 500 mA DC max.
Power consumption …	W
Operating temperatur range	5°C to 45°C
Nominal temperatur range	15°C to 35°C

WISI Communications GmbH & Co. KG
Empfangs- und Verteiltechnik
P.O. BOX 1220, 75219 Niefern-Oeschelbronn, Germany
Phone +49 7233 66 280. Fax - 66 350. http://www.wisi.de

... a link to the future