RMIP - RMIPCI4
Configuration settings page

RMIP is a compact form-factor IP gateway designed for satellite signal reception and secure distribution over IPTV networks. The system is capable of receiving up to eight DVB-S2 multiplexes and selecting up to 64 services for decryption and secure redistribution across an IPTV distribution infrastructure.

Signal reception is performed by eight DVB-S/S2/S2X multistream satellite demodulators operating on four shared full-band tuners.

The **RMIPCi4** variant extends these capabilities by supporting decryption through up to four Common Interface (CI) modules.

Both RMIP and RMIPCi4 integrate a Digital Rights Management (DRM) solution compliant with the Simulcrypt protocol, enabling interoperability with standard Conditional Access System (CAS) servers, including compatibility with Samsung DRM Lynk One. Services may also be encrypted using the LG Pro:Idiom encryption protocol.

For this purpose, various settings can be configured on the page below, which can be accessed by clicking the module from the module list ❶.

This page is structured into three distinct sections: the tab selection buttons ❷, the controls associated with the active tab ❺, and the services list ❻.

Two key status indicators are permanently displayed on this page:

❸ The total bandwidth of the services currently being streamed by the module(s).

❹ The module temperature, enabling verification that the device is operating within acceptable environmental conditions (e.g., adequate ventilation and airflow).

First, click one of the five tab buttons in ❷ to configure the required parameters:

IP : These controls are intended to define and manage the IP configuration of the module

Inputs : Allows modification of the LNB settings for the four available inputs (polarity, band, DiSEqC configuration, and selection between Legacy LNB mode or dCSS mode).

Demodulators: Allows configuration of up to eight multiplexes from which services are to be received (selected input, frequency, symbol rate, etc.).

CAM: Provides access to the CAM module menu, if a module is used.

Status: Displays a summary of the input status.

Once IP and input parameters have been configured, the services list ❻ can be used to select and configure the services to be streamed.

On this properties page, the user can configure the IP settings ❶, select the streaming protocol ❷, adjust various streaming options ❸, and configure the Digital Rights Management (DRM) parameters ❹.

❶ IP settings
- The MAC address is displayed for informational purposes only and cannot be modified.
- The module may be configured with a static IP address by manually entering the IP address, subnet mask, and default gateway, or it may be set to obtain its network configuration automatically via a DHCP server by enabling the DHCP option

❷ Streaming configuration
- The module supports two streaming **protocols** : UDP and RTP. UDP is recommended for minimal overhead and low-latency transport, whereas RTP should be selected when enhanced synchronization, packet sequencing, and stream identification capabilities are required.
- Adjust the **QoS** (Quality of Service) settings so that media packets are given higher priority within the network infrastructure (switches and routers), helping to maintain stable video quality and prevent artifacts such as freezing, pixelation, or audio dropouts.
- Set Time To Live field (**TTL**) to control how far multicast packets propagate across a network

❸ Streaming options
- Session Announcement Protocol (**SAP**), when enabled, allows receivers to automatically detect and list available multicast services without requiring manual configuration. The module will periodically announce streaming session details, such as multicast address, port, and media description, using the default multicast address 224.2.127.254 on UDP port 9875, as defined in the SAP protocol specification (RFC 2974).
- The **IGMP Auto-Join** option, when enabled, helps ensure that traffic is properly distributed across the network. It also provides an additional safety mechanism in the event of network topology changes or receiver restart, while potentially reducing the criticality of receiver-side group subscription depending on the deployment architecture.
- **IGMP Query** can be enabled on the module (and the query interval defined) when the multicast switches used in the network do not provide this function. When enabled, the module will periodically send IGMP queries to verify that devices subscribed to multicast groups are still active on the network, helping prevent unnecessary multicast traffic from being forwarded to network segments where no active listeners exist.
- As service discovery and program metadata are often handled through alternative mechanisms such as XML-based guides, proprietary EPG protocols, or other metadata delivery methods, the Event Information Table (EIT) is therefore not always useful in IPTV environments. To reduce CPU load and conserve network bandwidth, the **scheduled event EIT tables** transmission can be disabled so that these tables are not forwarded onto the network. This is particularly relevant when DVB signaling compatibility with the Digital Video Broadcasting Project is not required.

❹ Digital Right Management

Digital rights management protection may be mandatory depending on content licensing agreements and operator requirements. To meet this requirement, RMIP modules are able to encrypt streamed content using two encryption methods: Samsung Electronics Lynk and LG Corporation Pro:Idiom encryption.

To configure Digital Rights Management, click the DRM button on the IP page. This will open the corresponding configuration dialog box.

Select the encryption method in ❶ and ensure that the licence is already activated ❷. If the Activate button is not greyed out, a licence must be purchased from Anttron before the selected encryption method can be used.

Note: Separate licences are required for Lynk and Pro:Idiom encryption. The licence for the Lynk solution is not applicable to the Pro:Idiom solution, and vice versa.

If Pro:Idiom is selected in ❶ and the licence has been entered, no further action is required. Click OK to confirm the configuration, and the selected services (see encryption activation in the services list section) will start being encrypted.

If Samsung Electronics Lynk is selected in ❶, the IP address and port of the Lynk CAS server must be entered. Please contact the CAS server administrator to obtain the required connection information.

The RMIP module can operate as a server and provide the required CAS information when no external server is configured. To use the internal server of the RMIP module, set the IP address to **127.0.0.1** and the port to **9999**. This configuration will ensure that the stream is encrypted in accordance with the Lynk protection requirements.
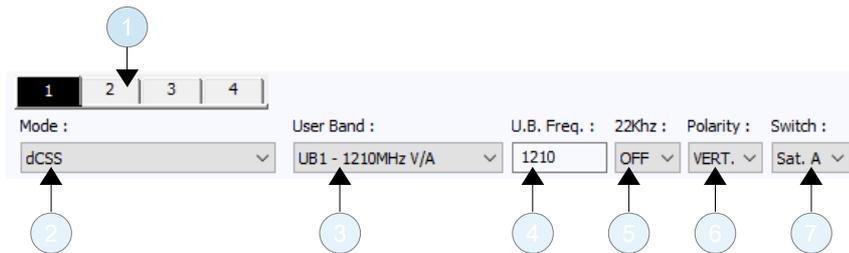
Up to four LNBs may be connected to the module. Each LNB can operate either in Legacy mode or in dCSS/SatCR mode.

Prior to configuring an LNB, select the corresponding input to which it is connected by clicking one of the four input buttons on ❶.

Once the input has been selected, set the operating mode ❷.

a) Legacy mode

In Legacy mode, user band selection and frequency are not available. Only the following parameters must be configured:

❺ The band (Low / High, corresponding respectively to 22 kHz OFF / ON),

❻ The polarity (Vertical / Horizontal),

❼ If the LNB is connected via a DiSEqC switch, the corresponding switch port (A, B, C, or D).

b) dCSS/SatCR mode

Refer to your LNB documentation and select either dCSS mode (EN 50607) or SatCR mode (EN 50494), as appropriate.

N.B. : If SatCR mode is selected and user bands greater than 4 are used, the module will automatically operate in EN 50607 for those user bands.

Once the mode has been selected, first click ❸ and choose one of the 24 user bands. The subsequent settings — user band frequency ❹, 22 kHz ❺, polarity ❻, and switch ❼ — will then apply to the selected user band.

Refer to the LNB documentation to correctly specify the user band frequency. This information will subsequently be used by the module to calculate the frequency offset to be applied.

The selected user band settings will automatically be reflected in the user band selection field ❸, allowing you to verify which user bands have been defined and which settings are applied to each.

If a user band has been selected in error, click ❹ and delete the corresponding frequency.

All associated information in the user band selection field ❸ will be cleared, and the user band will no longer be used.
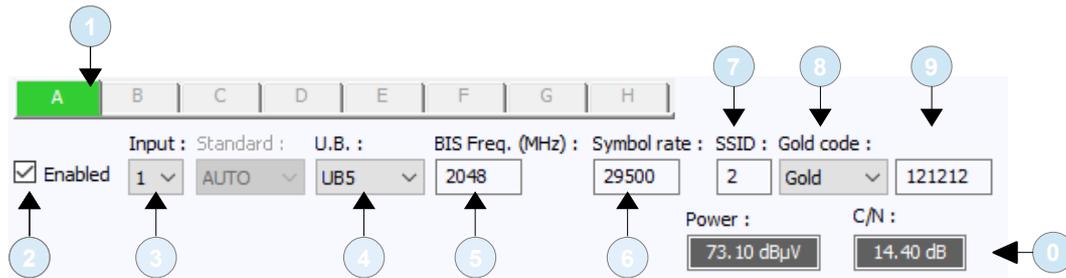
The module can demodulate up to eight multiplexes (A to H), each of which may be received from any of the four inputs.

Each of the eight demodulators can also be used to extract a stream from a multistream DVB-S2 signal.

To configure a demodulator, first select it by clicking ❶, then enable it by clicking ❷. If a demodulator is not used, ensure that it is disabled to minimize power consumption.

Then configure the multiplex by selecting the input from which the signal is received ❸ and, in the case of a dCSS/SatCR LNB, the user band ❹.

Finally, set the BIS frequency ❺ and the symbol rate ❻.

N.B. : If a RF frequency is entered in field ❺ (for example, 12648 MHz) instead of the IF frequency, the module will automatically calculate and display in ❺ the BIS frequency using the standard local oscillator frequencies (9750/10600 MHz).

If the multiplex carries multistreams, set the stream ID in ❼ and the PLS information in ❽ and ❾. If you wish to receive another stream from the same multistream DVB-S2 signal, configure another demodulator in the same manner but using a different SSID.

Once all parameters are configured, the TAB control background color reflects the demodulator status:

● Grey: demodulator not enabled

● Red: demodulator enabled but not locked

● Orange: signal locked but data is unstable or being acquired

● Green: multiplex correctly acquired (the service list is automatically updated based on the multiplex data).

Signal acquisition status information, including power strength and carrier-to-noise ratio, is displayed in ❿.

4) CAM
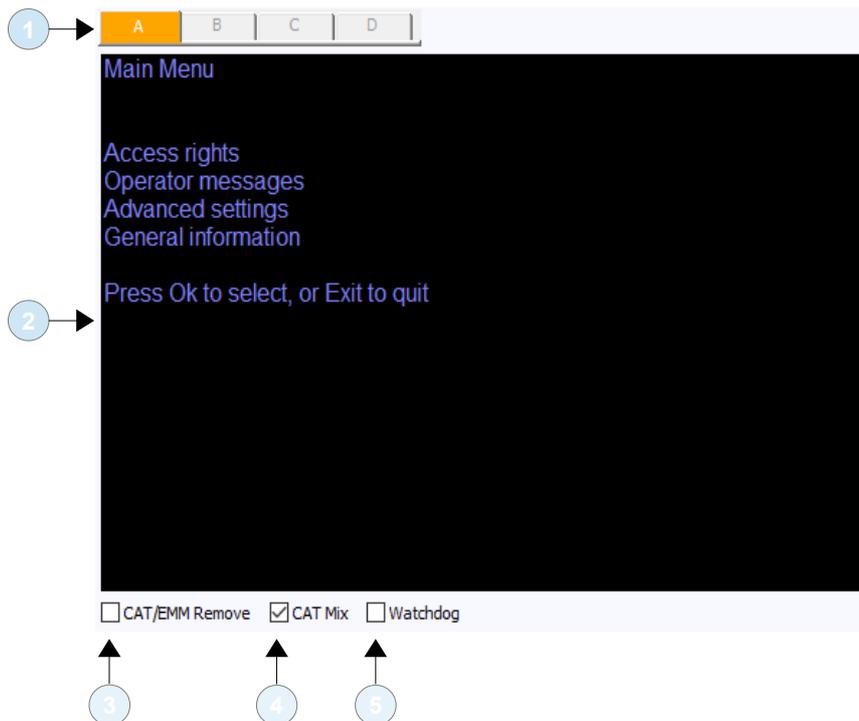
IMPORTANT: Before accessing the CAM menu through this dialog, at least one service must be selected for decryption so that the CAM can be detected. If the background color of the CAM tab ❶ is not orange, the CAM is not accessible. Please refer to the service list section for more information on activating service decryption.

To navigate within the CAM menu ❷, ensure that the correct CAM is selected in ❶, that the CAM is accessible (orange state), and wait for the CAM menu to be displayed in ❷. Once the CAM menu is properly shown, use the keyboard arrow keys to navigate, the **Enter** key to access a sub-menu, and the **Esc** key to exit a sub-menu.

Three additionnal settings are available on this page.

❸ **CAT/EMM Remove** : Because CAT and EMM tables are rarely used in IPTV environment and to conserve network bandwidth, you may choose to completely remove them from the output stream by enabling ❸.

❹ **CAT Mix** : If this option is enabled, a new CAT table, composed of all CAT tables encountered in the multiplexes containing services to be decrypted, will be generated and sent to the CAMs.

When using multiple service providers for decryption, it is generally recommended to enable this option so that the CAM receives all EMMs present across all multiplexes, and not only those present in the first multiplex containing services to be decrypted. However, some CAMs may not properly handle very large CAT tables, so this option should be used with caution.

❺ **Watchdog** : When activated, the module will monitor all decrypted services and, if a service is no longer decrypted, it will reset the CAM and restart the decryption process.

5) Status

The overall input activity status can be found on this screen in ❶

The status is displayed in grey whenever an input is not locked, not enabled, or when an output is not used.

All input levels and carrier-to-noise ratios are displayed so that any abnormal situation or configuration can be easily detected.

A daily reboot can be scheduled using control ❷ by enabling the option and entering the time (UTC) at which the reboot will occur.

Under normal operating conditions, the DVB headend is designed for continuous 24/7 operation and does not require daily rebooting. However, in certain network environments, a scheduled restart may be implemented as a preventive measure to refresh system processes, network sessions, and conditional access communications, thereby maintaining optimal performance and service stability.

Although this function is available, it is not recommended to enable it unless specifically required by the installation environment.

6) Services List

Once at least one demodulator has been correctly configured, the services list is updated with all services found in each demodulator and displayed in the table below.

This table consists of four main columns:

❶ **Service source**: Indicates the demodulator number from which the service is received, followed by its ID.

❷ **Service name and audio/video information**: Displays the service name. This column also indicates whether an audio PID filter is applied and whether the service is a TV or radio service.

❸ **Decryption**: Indicates whether the service is encrypted and, if so, which CAM is used to decrypt it. This column can also be used to specify if a service must be decrypted using BISS or if it contains an encapsulated stream (such as T2-MI or other protocols), and how it should be expanded.

❹ **Output**: Indicates the IP address and port used to stream the service.

This table can be sorted according to any of the four columns. To do so, simply click on the column header. The software will automatically sort the services list according to the selected column, in either ascending or descending order, using the ▲ and ▼ symbols displayed on the left side of the column header.

This feature allows services to be sorted by output, decryption CAM or other available criteria.

Important: *A service that has been previously configured but is currently not present at the inputs (due to signal absence at the input) will be displayed in grey in the list.*

Always verify these absent services and ensure that their absence is only temporary, as the modulator will wait for a few seconds for their return before starting modulation. In rare cases, this may prevent the streamer from starting if it waits indefinitely for a service displayed in grey (for example, a RMIP module may wait for services from a previous DTVHD4 configuration if those services are scheduled for streaming). Therefore, ensure that services displayed in grey are expected and represent a normal condition. If not, remove it from the output.

The service streaming configuration is done in the following way.

<u>a) Selection of the streaming destination</u>

Before selecting the CAM or applying any other configuration, the service must first be assigned to a streaming destination.

To do so, double-click the streaming destination field (indicated by the arrow above) and enter the destination IP address followed by the destination port, separated by a colon.

For example, to stream the service to the multicast IP address 239.192.1.1 on port 5004, enter:

239.192.1.1:5004

Then press the Enter key to confirm.

The IP address can be either unicast or multicast.

In the case of a multicast address, it should be within the range **239.0.0.0** to **239.255.255.255**. This is known as the administratively scoped multicast range, which is intended for use in internal or private networks to avoid conflicts with globally reserved multicast addresses.

It is recommended to avoid using the following ranges:

- 224.0.0.0 – 224.0.0.255, which are reserved for local network control protocols.
- 224.0.1.0 – 238.255.255.255, which correspond to globally scoped multicast addresses and may conflict with public multicast assignments.

In RTP mode, although this convention is not always strictly enforced by all systems, compatibility with the receiving equipment should be considered. It is recommended to use an even port for streaming media packets, while the subsequent odd port (even port + 1) is used for RTCP control and feedback packets.

RMIP modules are capable of handling both multi-service and single-service streams.

To create a multi-service stream, assign the same destination address and port (address:port) to each service you want to group within the stream.

When a service no longer needs to be streamed, double-click the streaming destination field, delete the entire destination address and port, and then press the Enter key.

<u>b) Service encryption</u>
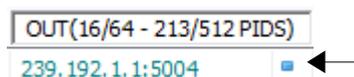
Before being streamed, each service can be encrypted using the selected Digital Rights Management method (refer to the IP section for configuration details).

To enable encryption, double-click the blue square located in front of the streaming destination field. Once selected, the service list will be updated and a closed padlock will be displayed next to the address of the encrypted services.
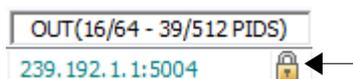

To deactivate encryption, double-click the padlock icon.

Multiple Selection : *The Ctrl key can be used to select or deselect the encryption for multiple services. To do this, first select a service by clicking anywhere on its row. Then, while holding the Ctrl key, click on other services you want to configure. Finally, still holding the Ctrl key, double-click the blue square or padlock symbol of the service to which you want to assign or remove the encryption. The selection or deselection will be applied to all selected services.*

Similarly, the Shift key can be used to select a continuous range of services by clicking on the first service and then double-clicking on the last service of the desired range while holding the Shift key.

c) Audio PID filtering
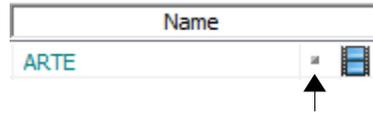
A service may contain multiple audio PIDs for different languages. In some cases, it may be useful to allow only certain languages to be present in the output stream. This can be achieved by double-clicking the field indicated by the arrow (see above) and then selecting up to three allowed languages in the dialog box that appears.
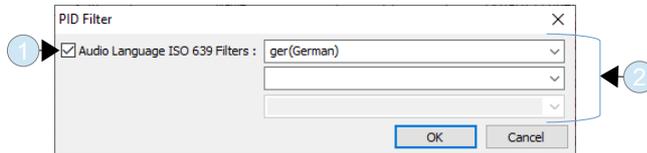
Enable or disable the audio filter by clicking ❶ and add up to three allowed languages in ❷. Once the filter is applied, the module will scan the PMT table in the source stream and check for the presence of audio languages associated with the concerned service. Whenever a PID matching one of the selected languages is found, it will be passed through and the PMT will be updated to include only the allowed audio PIDs.

However, if no audio PID matching the selected languages is found, all audio PIDs will be passed through to avoid producing a service without audio.

The presence of audio-filtered services in the service list is indicated by the funnel symbol in front of concerned services :

d) BISS decryption

BISS scrambled services can be descrambled on RMIP modules without the help of CAMs using biss keys that can be entered using the following method.

In the services list window, double-click the padlock icon in front of the service you wish to descramble. For example, in the screen above, to enter a BISS key for the BBC ONE service, double-click the padlock located in front of BBC ONE (see arrow above).

Note: When the same BISS key is used for multiple services, you can select those services in the list using the multiple selection method described earlier (see the Mutiple Selection in service encryption section)

The following window is displayed, allowing you to enter the required keys :

You can now enter a BISS key (16 characters) in either the even or odd key list by typing it in the corresponding dropdown box or selecting it from the list if the key has already been entered.

If the same key is used for both even and odd streams, please enter the same key in both selection boxes.

If the service is not encapsulated, please ensure that both stream encapsulation method options remain unchecked.

Once the keys have been entered and validated, click the **OK** button.

After a few seconds, the services list will be refreshed and will display the actual service type (video or audio) if the PMT was scrambled. A modified padlock icon ⚿ will also be displayed to indicate that BISS descrambling is active for the selected service.

RMIP modules are capable of de-encapsulating T2-MI streams as well as streams using other encapsulation methods.

Before de-encapsulation, these streams must be identified and configured so that they can be expanded into a new demodulation channel, allowing the user to select the programs contained within them.

Furthermore, if these streams are encrypted using BISS, they can be decrypted prior to de-encapsulation.

Proceed in the same manner as when configuring BISS keys (see previous section) to configure these encapsulated streams. Specify whether the stream is T2-MI or encapsulated within a PID using another method. In the latter case, the system will attempt to synchronize the data by detecting the sync byte within the data PID that composes the stream.
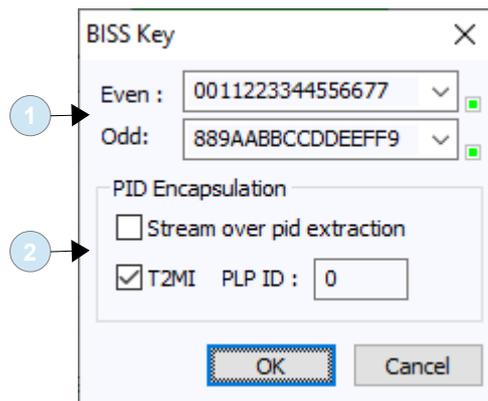
First enter the BISS keys in ❶, if required. Then select the encapsulation method in ❷ and specify the PLP ID (for T2-MI only). Finally, click on OK.

The module will then attempt to extract the stream from the specified service and will automatically create a new input channel in which the extracted stream will be displayed. After a few seconds, the services list will be updated. The output information column for this service will indicate the demodulation channel number to which the stream has been extracted, and the newly extracted services will be displayed under it.

The user can now select the services to be streamed from the extracted stream in the usual manner.

f) CAM activation

Each modulated service may be decrypted using an appropriate CAM prior to streaming.

RMIPCI4 modules are equipped with four CI slots, allowing each module to accommodate up to four CAMs.

A blue square indicates an available slot, while a grey square indicates the absence of a slot. When a service is assigned to a CAM for decryption, the blue square is replaced by a smartcard icon.

Decryption for a service can be enabled by double-clicking one of the four blue squares (depending on the CAM you wish to use), or disabled by double-clicking the smartcard icon.

The multiple selection method described earlier (see the Mutiple Selection in service encryption section) can also be applied when selecting CAMs.

Once a CAM is used for service decryption, it is activated and its menu becomes accessible through the CAM tab controls.