KENWOOD

Application Note

KAIROS DMR System

IP Gateway KPG-1013GW Version 1.11

Last Updated: Oct. 14. 2020
Language: English
Document No.: AN-19-0013

JVCKENWOOD

Revision History

Version	Date of issue	Note
1.00	August-8 2019	First edition
1.10	December-9 2019	2nd edition
1.11	October-14-2020	Corrected the number of connectable systems in the Tier II KAIROS system. Updated the additional values of “Maximum Jitter Buffer Size” and changed default value.

Document Copyrights

Disclaimer

This document is intended to provide basic and general information about the specifications of the products listed above and the system configuration. The intended purpose of all technical descriptions herein shall be, to improve your understanding of the product specifications and system configuration. The descriptions provided in this document are carefully examined and are believed to be entirely reliable. JVCKENWOOD Corporation shall be entirely free from any responsibility and liability for inapplicability, damage or loss arising from inaccuracies in this document and reserves the right to change the product specifications herein in order to improve readability, function or product design. Applicability of the descriptions in this document may vary depending upon the product specifications and configurations of relevant equipment.
Furthermore, you are neither licensed nor entitled to use and/or divert any descriptions in this document to your application.
Contact JVCKENWOOD Corporation for further details.

Table of Contents

1. Release Information

IP Gateway designed based on DMR AIS (Application Interface Specification) works with Radio Activity KAIROS System is released. IP Gateway is interface of KAIROS system to connect a console, a Voice Logger and an OTAP manager. In addition, IP Gateway stores various logs for maintenance.

1.1. Version Information

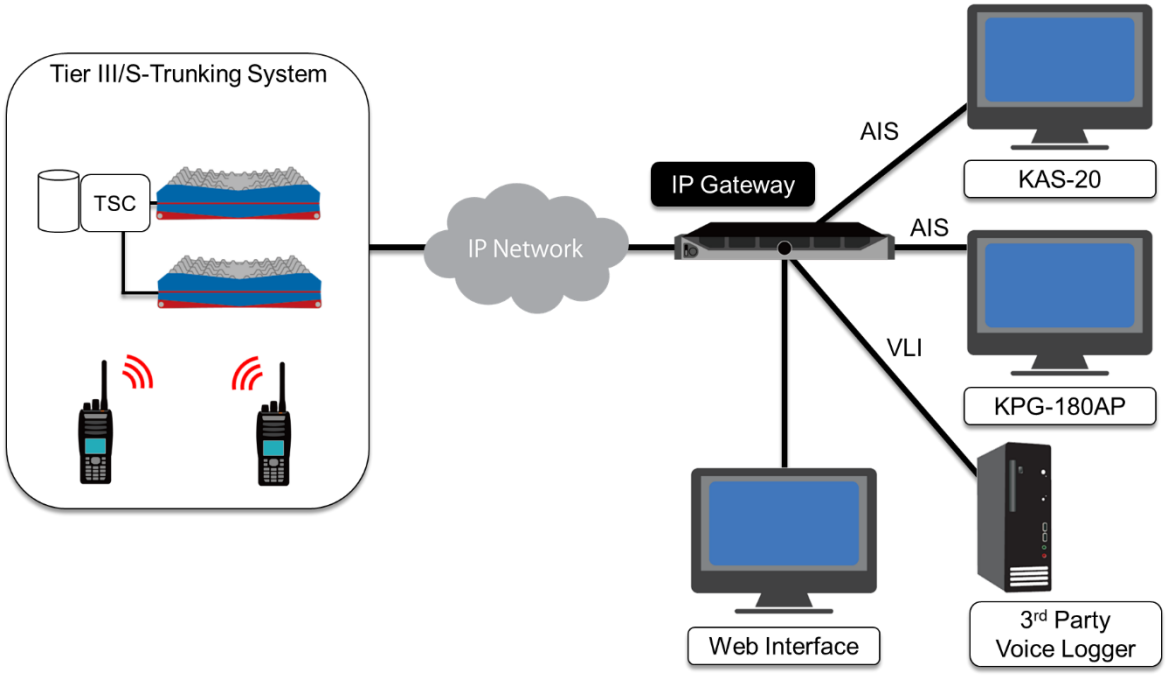
This document describes IP Gateway, Console and OTAP Manager that KAIROS system supports. Version information is as follows.

Product	Supported Version in Release
IP Gateway	KPG-1013GW Version 1.10
Console	KAS-20S/KAS-20C Version 3.00
OTAP MANAGER	KPG-180AP Version 3.00
KAIROS System	Operating System: Linux 2.4.31 Version 01, Build 07 KAIROS Main Firmware Version 1.6.B.1_stable KAIROS DSP Firmware Version 4.5C KAIROS PLD Firmware Version 4.13 Tier III Controller Version 1.0.5.0 KAIROS Manager Version 1.7.9

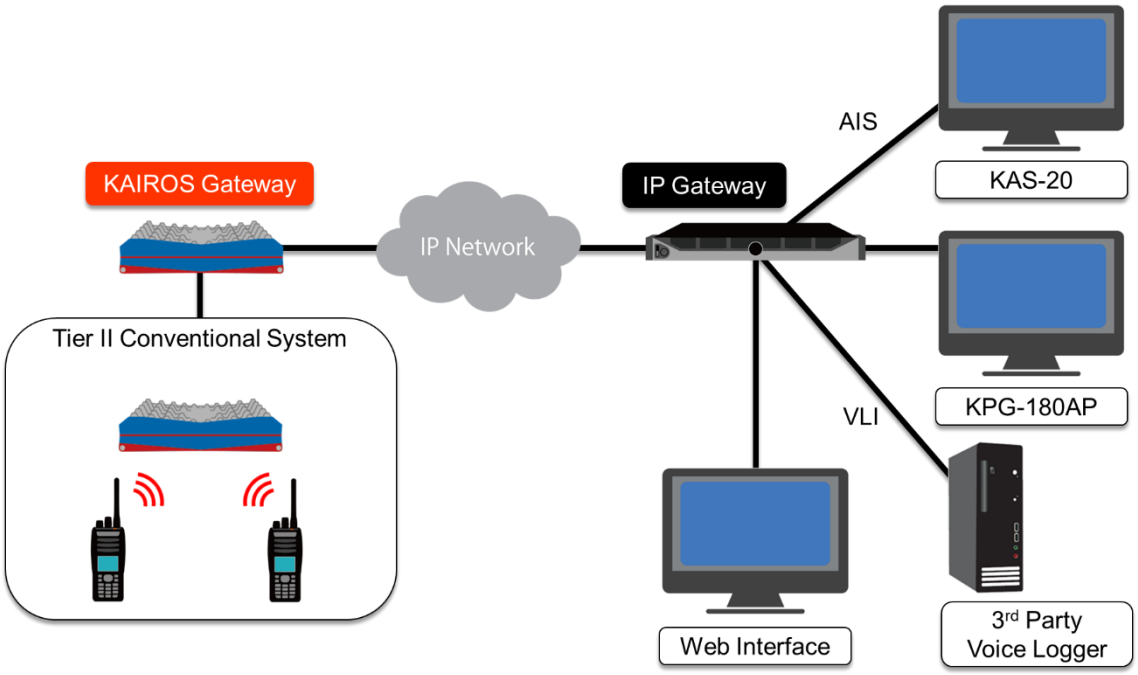
1.2. System Diagram

KAIROS DMR Tier III Trunking system connects consoles and voice loggers via IP network. It can connect to 3rd party products which designed based on AIS as well. It recommends that the system is installed in private network. As a reference, system diagram is as follows:

Tier III Trunking/S-Trunking



Tier II Conventional



2. IP Gateway (KPG-1013GW)

IP Gateway (KPG-1013GW) supports to connect between KAIROS system and consoles/3rd party voice loggers/OTAP Manager. It works Tier III Trunking, S-Trunking and Tier II Conventional system with this software version.

2.1. Model Information

IP Gateway model name is **"KPG-1013GW"**.
To enable PC Server as an IP Gateway is required a software license activation. The software license has three system types. Licenses are able to switch on the web interface if multiple licenses are activated on the PC Server.

[Software License]

System Type	License
Tier III Trunking	KWD-1013T3
S-Trunking	KWD-1013ST
Tier II Conventional	KWD-1013T2

2.2. Features

IP Gateway is operated on a PC Server and must be activated to work with Tier III Trunking, S-Trunking and Tier II Conventional System. IP Gateway service specifications are different with each system. Comparison is as follows:

Item	S-Trunking	Tier III	Tier II
Unit ID Range	1 to 16776415		
Group ID Range	1 to 16776415		
Number of connectable system*1	1		
Number of configurable repeaters*2	5000		N/A
Maximum Number of connectable Voice Loggers	10		
Maximum Number of connectable Consoles	100		
Maximum Number of registrable Group IDs per one console*3	100		
Maximum number of sessions*4	1000		
Maximum Number of configurable Console IDs*5	100		
Maximum Number of configurable Group IDs*6	10000		
Number of storable communication logs*7	Depend on HDD capacity		N/A
Number of storable system logs	200000		

*1: One IP Gateway can support one system only.
*2: The number of repeaters that can be listed by web interface.
*3: 100 Group IDs can be performed group registration per one console.
*4: IP Gateway can process 1000 sessions simultaneously.
*5: The number of consoles that can be listed by web interface.
*6: The number of Group IDs that can be listed by web interface. The Group IDs are calculated by 100 console IDs and 100 registrable Group IDs.
*7: 600GB HDD about 429GB (About 10 years / 480,000 calls per day)
1TB HDD about 800GB (About 19 years / 480,000 calls per day)
It takes about 12 minutes to download the communication log for one month.

2.3. PC Server Information

PC Server for IP Gateway is selected from two venders. The venders are Dell and Supermicro. The server requirement specification for IP gateway is as follows:

Dell Server Requirement Specification

PC Server Hardware	Dell PowerEdge R340 Rack Mount Server
Operating System (OS)	Cent OS 7.6
CPU	Intel Xeon E-21xx (3.0GHz) or more
Memory	4GB or more
HDD	500GB or more
Optical Drive	DVD-ROM

Supermicro Server Requirement Specification

PC Server Hardware	Supermicro SuperServer 5019S-MR
Operating System (OS)	Cent OS 7.6
CPU	Intel Xeon E3-1225 v5 (3.3GHz) or more
Memory	4GB or more
HDD	500GB or more
Optical Drive	DVD-ROM

3. Basic Configurations

This section describes about basic configuration of IP Gateway.

3.1. Preparation in advance

This preparation is to build a system on a repeater or a PC server.

3.1.1. KAIROS Repeater setting

It prepares KAIROS repeater configured as Tier III Trunking, S-Trunking and Tier II Conventional. How to set each system describes the following documents.

[Document]

System Type	Document
Tier III Trunking	AN-19-0001_DMR_Tier3_KAIROS_Trunking
S-Trunking	AN-19-0005_KAIROS_S-Trunking
Tier II Conventional	AN-19-0002 KAIROS Function Manual

3.1.2. IP Gateway setting

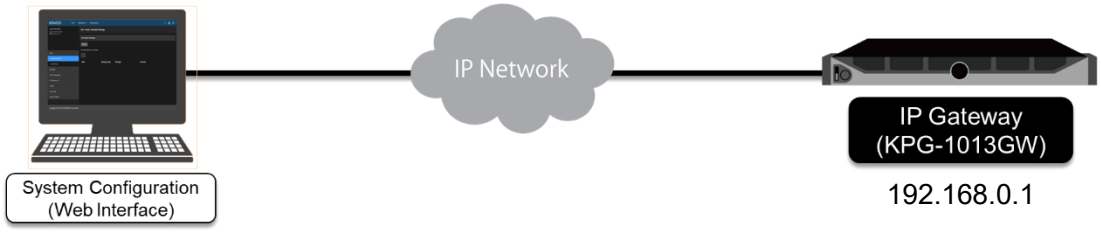
It prepares a PC server for IP Gateway. The PC server specification refers “2.3 PC Server Information”. Firstly, it’s required to be operated a PC server as IP Gateway.

How to set PC server describes
“TM-19-0001_KPG-1013GW_Initial_Setting_Guide_EN.pdf”.

After PC server setting completes, it must be activated the license for IP Gateway on web interface.

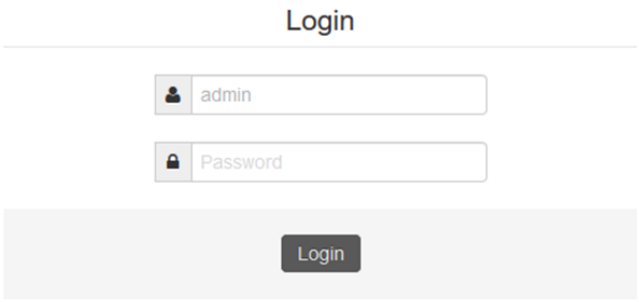
3.1.2.1. Login

IP Gateway configuration is done by web interface. IP Gateway can be accessed by starting a web browser and entering the IP address of the server as a URL. Default IP Address is “192.168.0.1”.



Login displays on web browser. For initial state, User Name is “admin” as an Administrator User. Password is no configuration. The password must be changed. Do not set the password that easy to be guessed by others.

User Name	admin
Password	(blank)



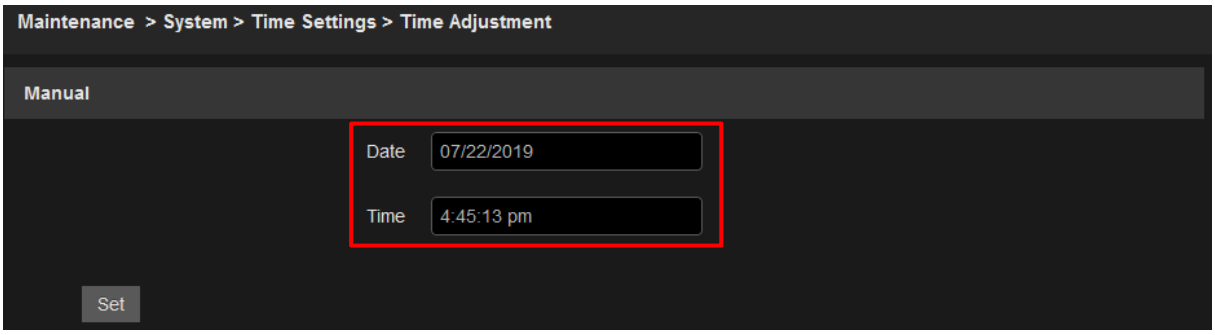
Note:

- Recommend browser is Firefox.
- It should not be forgot password for Administrator user. If the password is forgot, the IP Gateway must be initiated Factory Reset by serial interface. PC server setting and database become an initial state by Factory Reset. It’s required to set PC server again. The activated license never deleted by Factory Reset.

3.1.2.2. Time Adjustment

It must be configured Date and Time. The time settings are very important for trouble shooting when system log, communication log and Diagnostic data are stored.

Maintenance > System > Time Settings > Time Adjustment

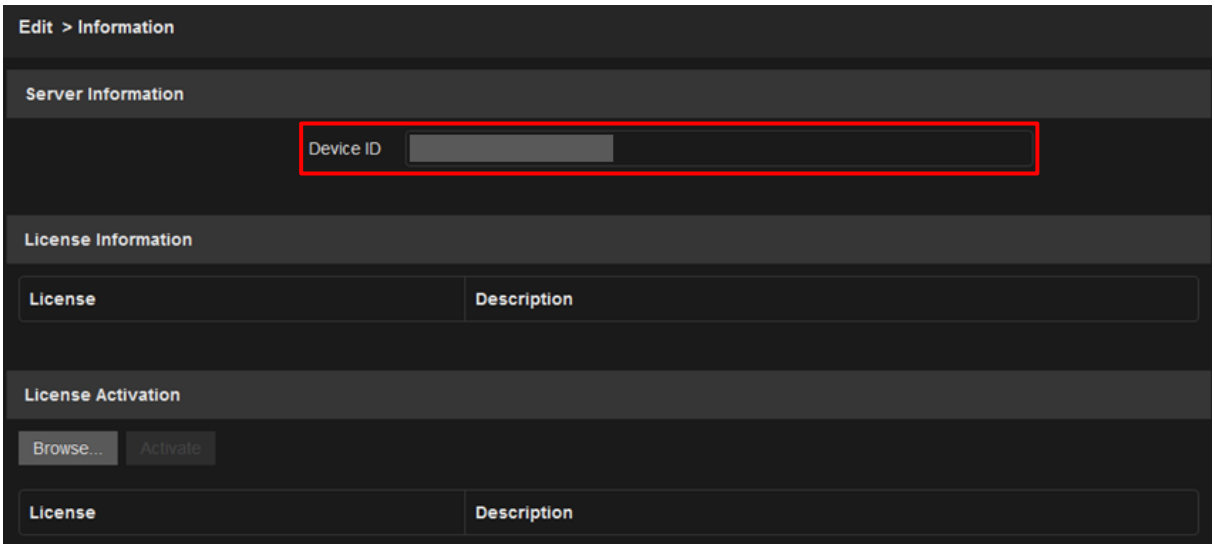


3.1.2.3. License Activation

Software license upgrades is activated while offline by KPT-300LMC. The authentication files (.jklfs) are created based on a device ID of IP Gateway. It needs to get the device ID of PC server. In this section, it describes Tier III activation as a reference.

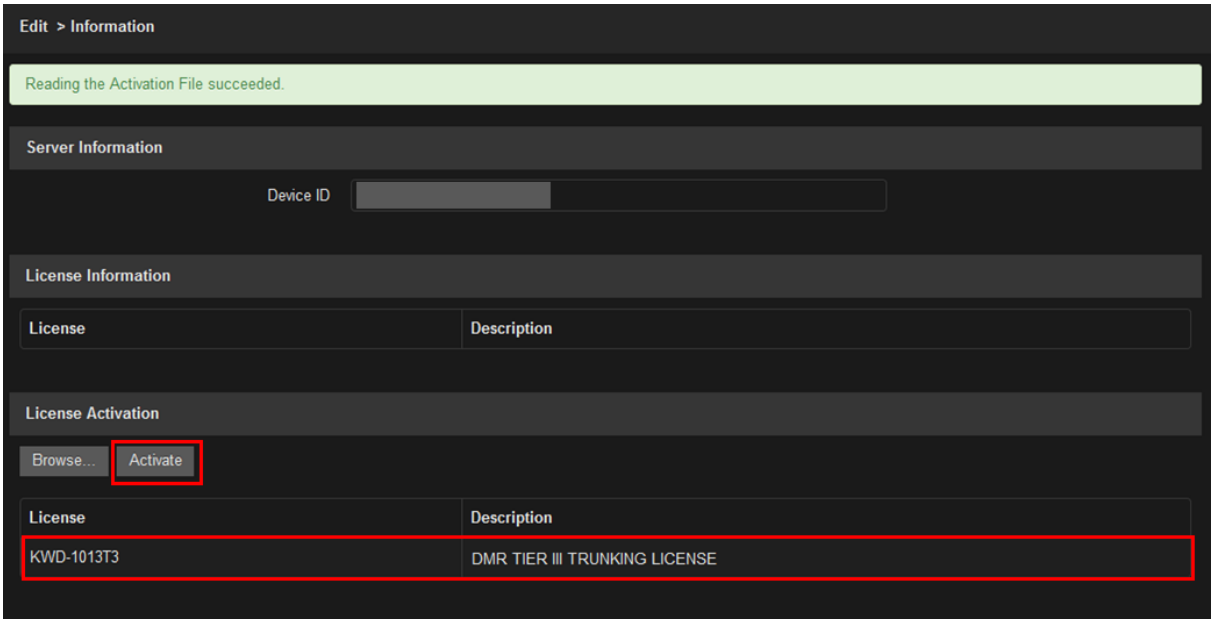
How to create the authentication file refers to "KPT-300LMC Basic Operations". (Basic Operations is saved on installed PC with KPT-300LMC.

Edit > Information

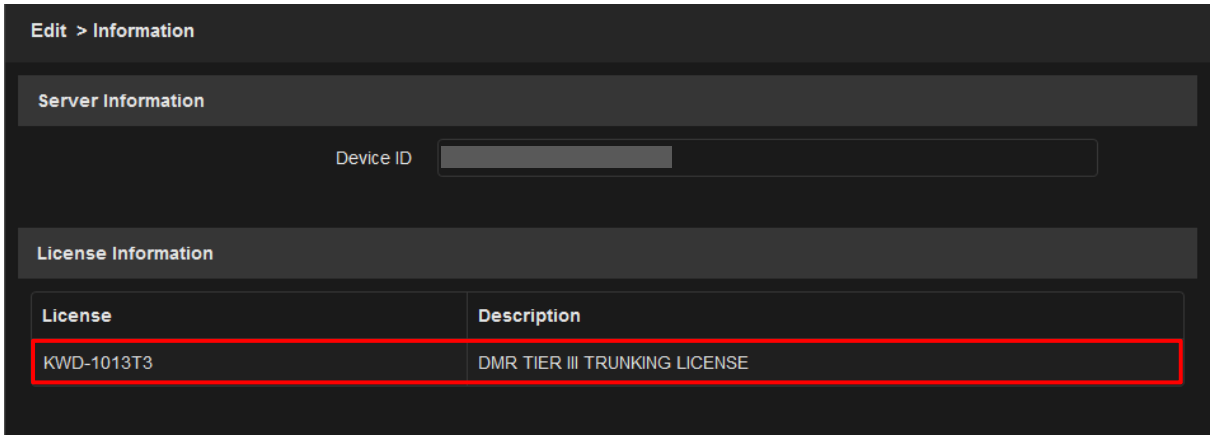


The authentication file is installed on web browser. Selects the proper authentication file.

If the authentication file is read correctly, “KWD-1013T3” is displayed. Click the “Activate”.

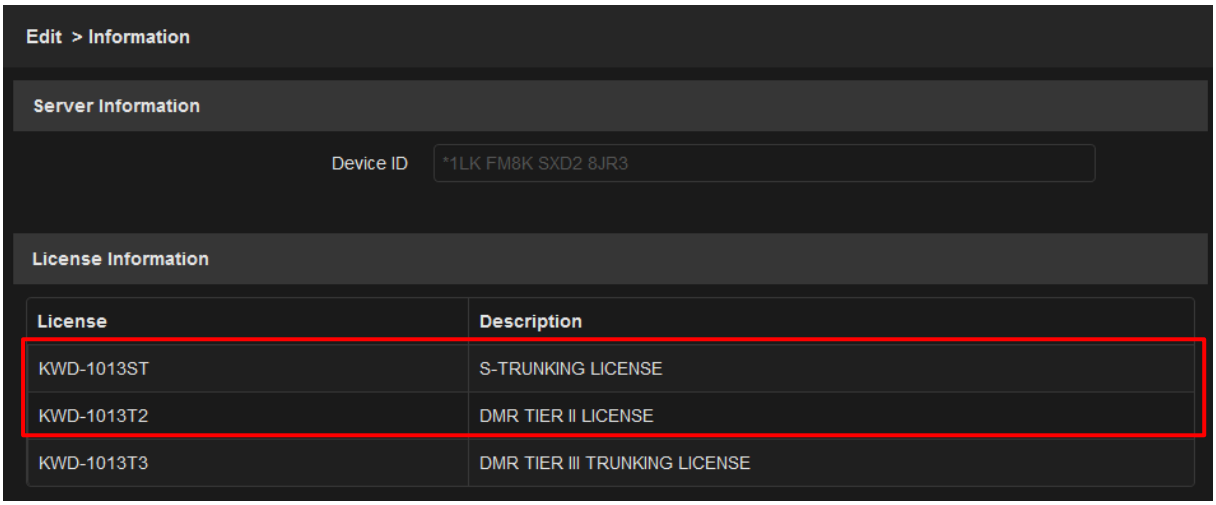


The license activation for IP Gateway is done on this menu. If the license “KWD-1013T3” is displayed correctly, the license is available as IP Gateway.



The others system displays below.

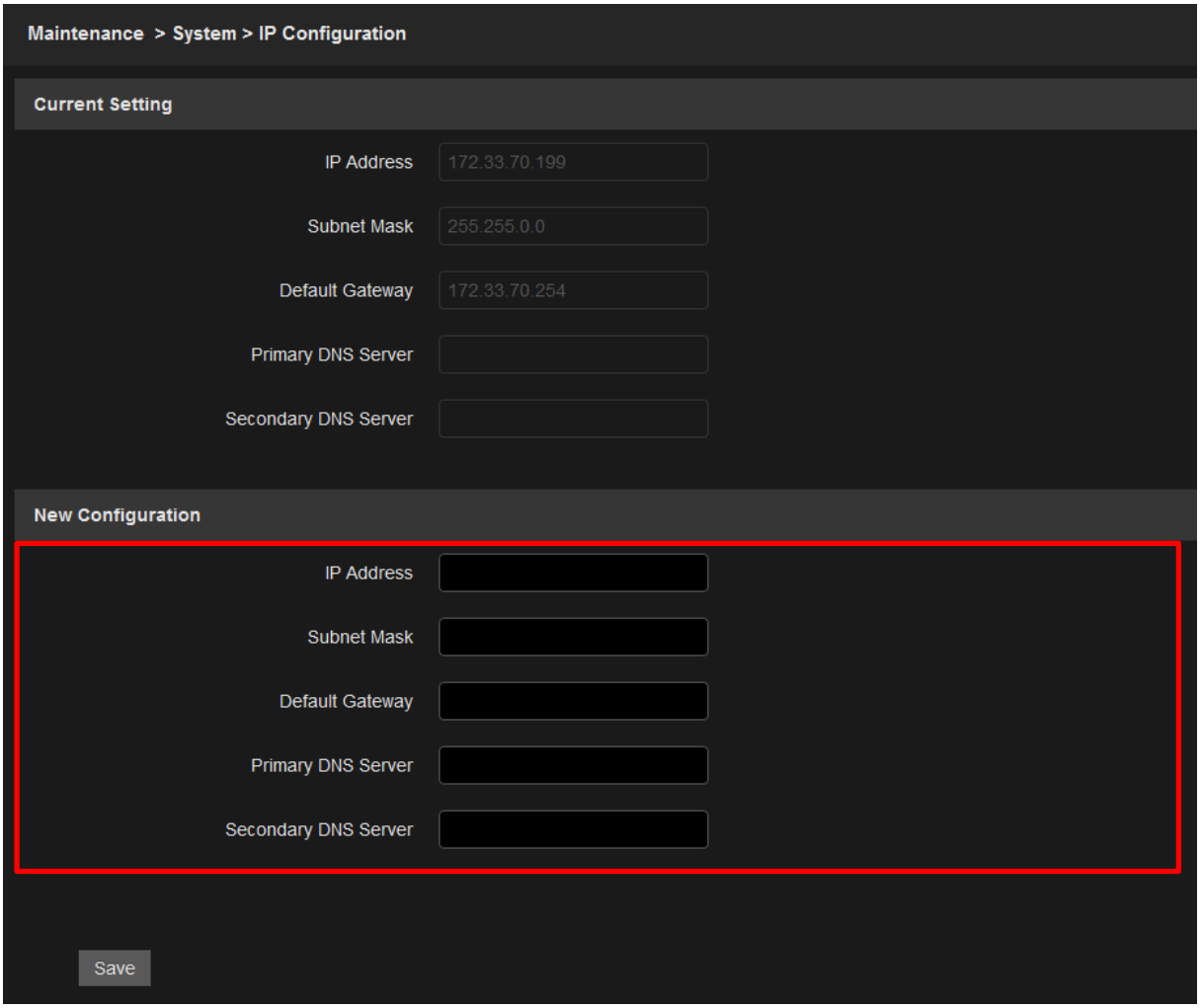
S-Trunking
Tier II Conventional



3.1.2.4. IP Configuration

IP Configuration is the function to confirm/change IP Address of an IP Gateway. After changing IP Address, IP gateway restarts. The current IP Address is displayed in Current Setting menu. The new IP Address is configured in New Configuration menu.

Maintenance > System > IP Configuration



3.2. IP Gateway setting

This section describes IP gateway setting to connect KAIROS System, Console, Voice Logger and OTAP Manager.

3.2.1. Server Configurations

Server Configurations menu has General and Network.

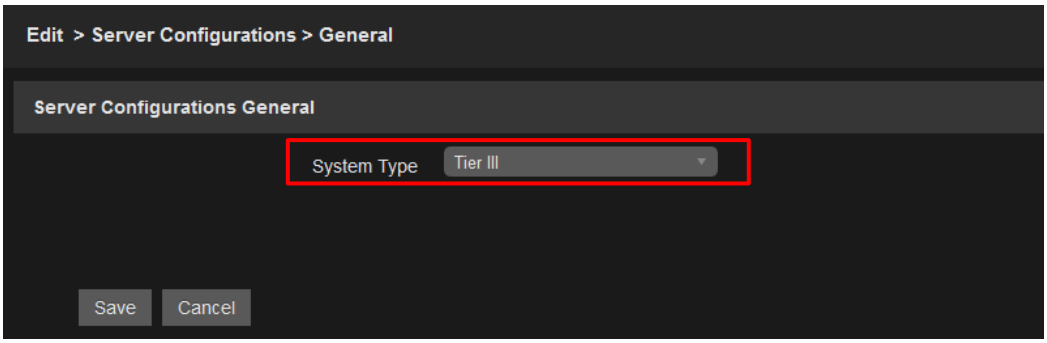
3.2.1.1. General

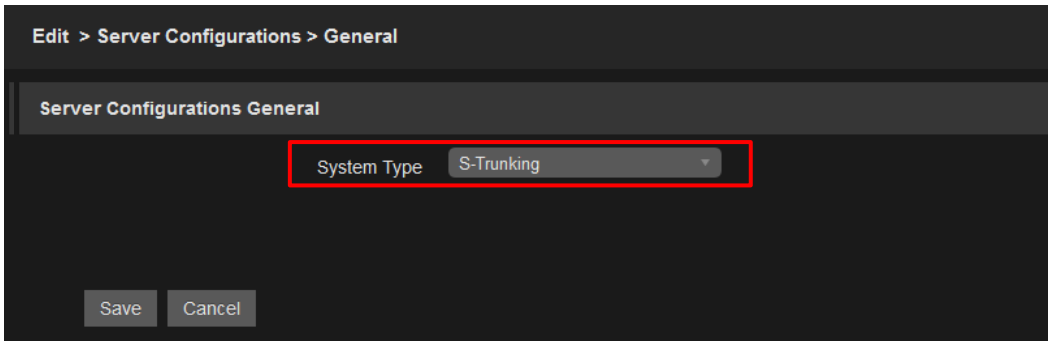
This configuration is for selecting System Type that IP Gateway is connected. The available System Type depends on the license activation status.

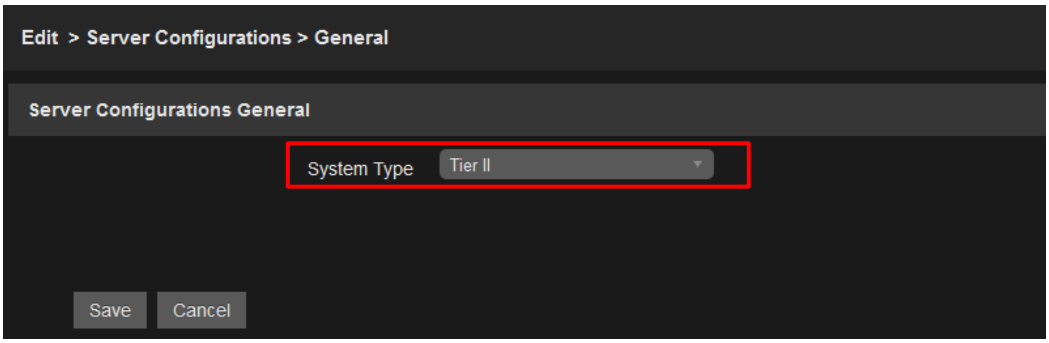
[System Type]

License	System Type
KWD-1013T3	Tier III
KWD-1013ST	S-Trunking
KWD-1013T2	Tier II

Edit > Server Configurations > General







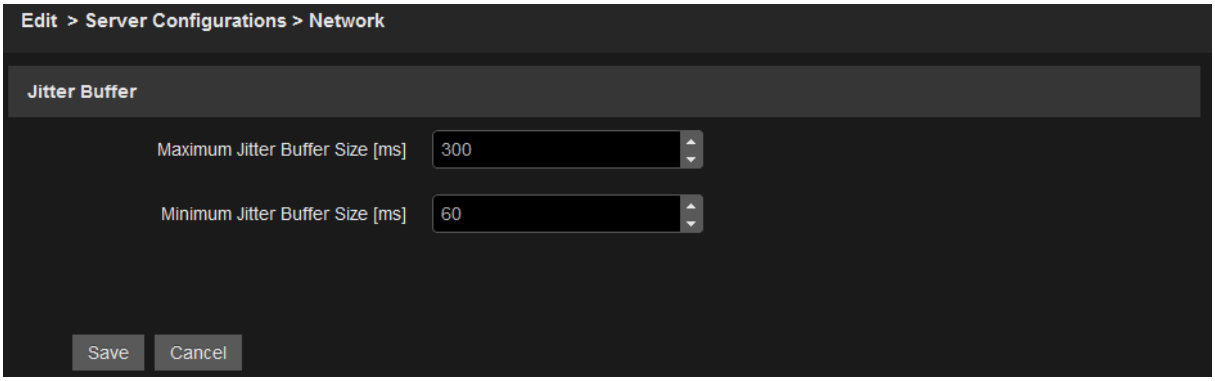
3.2.1.2. Network

Jitter Buffer is a buffer memory to absorb the timing dispersion of the packet data that IP gateway received from KAIROS System/Console on network. To use this setting is useful to reduce audio dropout. In case of bigger buffer size, a voice delay becomes bigger and audio dropout becomes lower. In case of smaller buffer size, a voice delay becomes smaller and audio dropout becomes higher.
Maximum / Minimum Jitter Buffer Size becomes effective for voice call only.

Maximum Jitter Buffer Size [ms]: Off, 60, 120, 180, 240, 300, 360, 420, 480, 540, 600, 660,720 (default), 780, 840, 900, 960, 1020, 1080
Minimum Jitter Buffer Size [ms]: Off, 60 (default), 120, 180, 240

Maximum Jitter Buffer Size “Off” and “60” can be set when Minimum Jitter Buffer Size is “Off”.

Edit > Server Configurations > Network



3.2.2. TSC/Gateway List

In TSC/Gateway List, it is registered TSC/Gateway connected with IP Gateway.

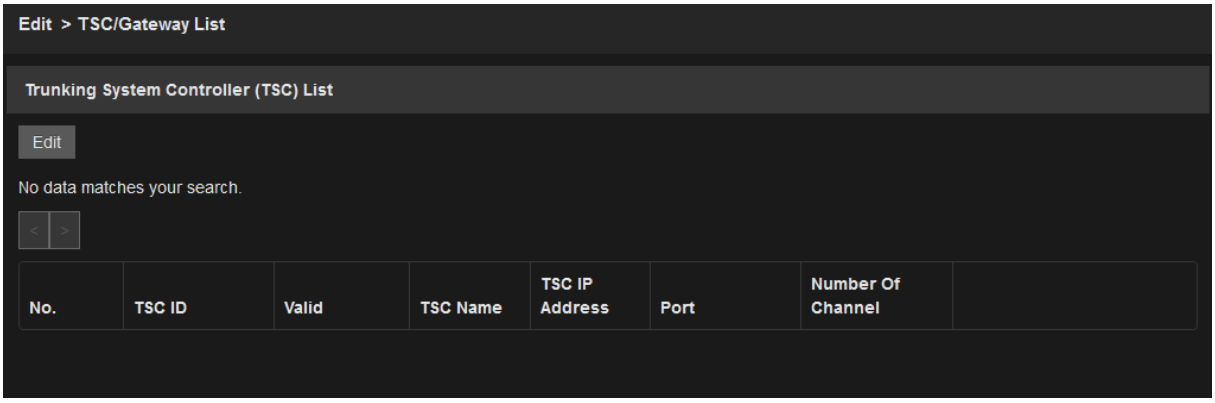
3.2.2.1. TSC/Gateway List

TSC/Gateway List is the list to register TSC/Gateway connected with IP Gateway. The maximum number of registration TSC/Gateway depends on System Type.

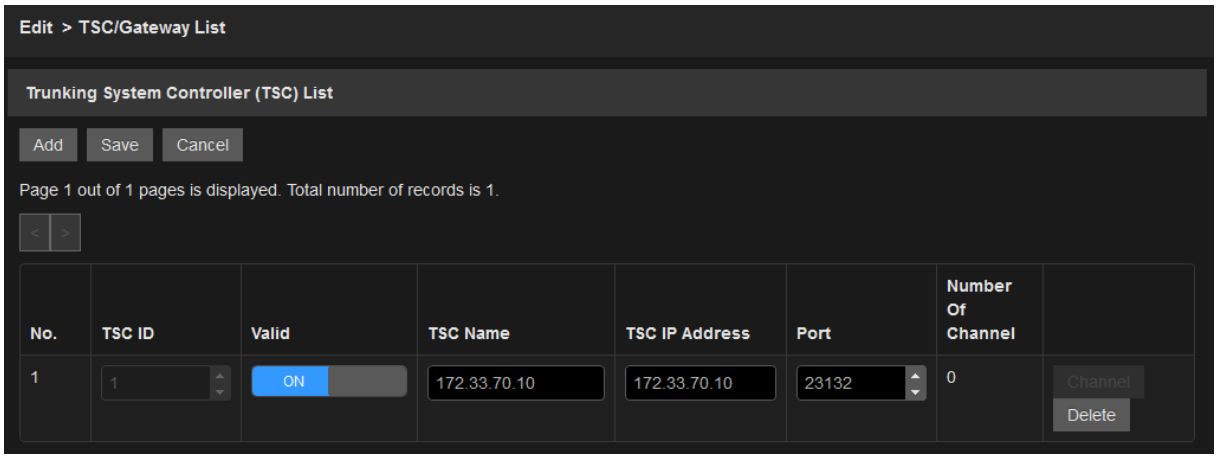
System Type: Tier III/S-Trunking

IP Gateway can connect one DMR Tier III system. One TSC is needed per one system. Actually, one TSC is registered on this list.

Edit > TSC/Gateway List



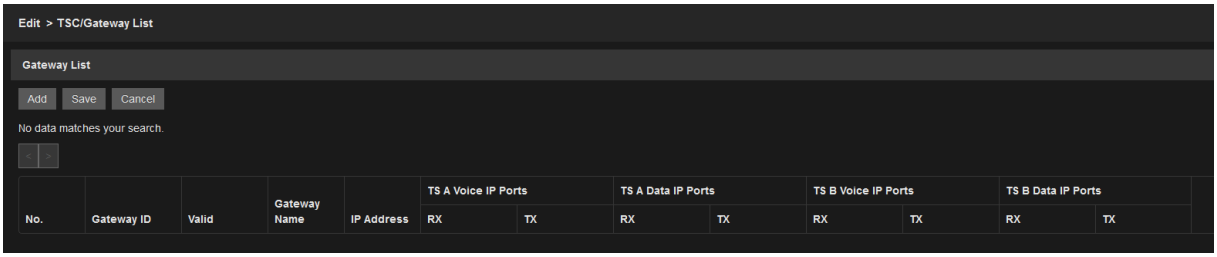
TSC ID: Unique number to manage TSC. The ID is used on Console List.
Valid: Enabling/Disabling to connect the TSC.
TSC Name: Any name to identify TSC.
TSC IP Address: Set the IP Address of the TSC.
Port: Set the receive port of TSC. IP Gateway sends a packet to TSC using the port. The default port number 23132 is fixed by KAIROS repeater.
“Use default port 23123, because normally it does not need to modify the port number.”
Number of Channel: The number of repeaters in the system.



System Type: Tier II

IP Gateway can connect up to seven KAIROS Gateway.

Edit > TSC/Gateway List

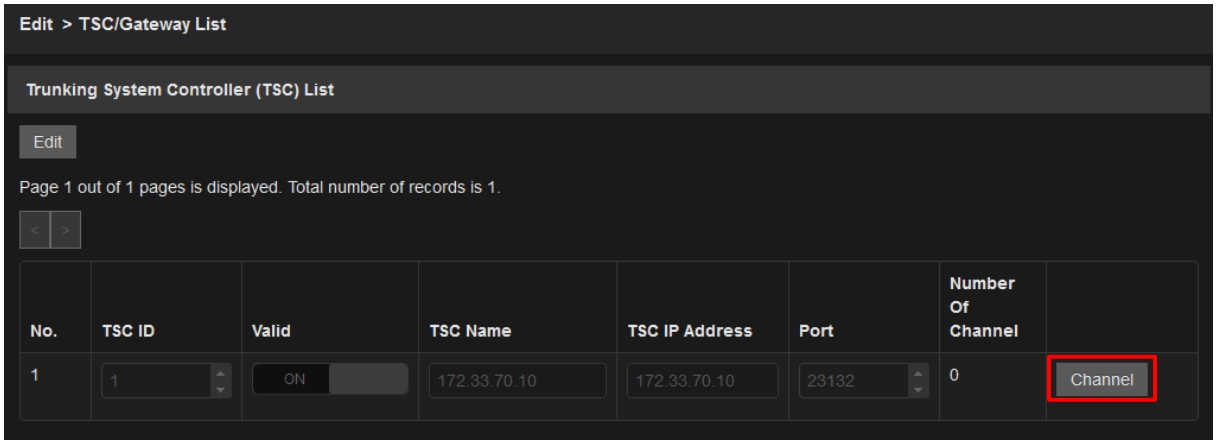


Gateway ID: Unique number to manage Gateway. The ID is used on Repeater List.
Valid: Enabling/Disabling to connect the Gateway.
Gateway Name: Any name to identify Gateway.
IP Address: Set the IP Address of the Gateway.
TS A/B Voice IP Ports RX: Set receive port for voice communication using slot1/slot2.
TS A/B Voice IP Ports TX: Set transmitting port for voice communication using slot1/slot2.
TS A/B Data IP Ports RX: Set receive port for data communication using slot1/slot2. The data ports are common with TS A/B Voice IP Ports RX setting.
TS A/B Data IP Ports TX: Set transmitting port for data communication using slot1/slot2.

3.2.2.2. Channel List

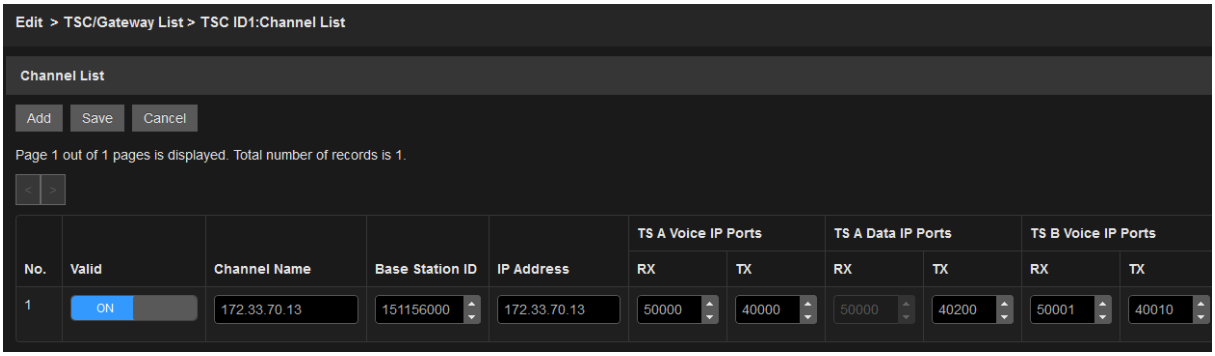
Register all repeaters connected with the DMR Tier III system. This configuration is to assign RTP port for voice/data communication used in each repeater. The maximum number of repeaters that a TSC can connect is 5000. Therefore, it can be registered from 1 to 201 in Channel List.

Edit > TSC/Gateway List



Valid: Enabling/Disabling to connect the repeater in the system.
Channel Name: Any name to identify each repeater.
Base Station ID: Set the Base Station ID of the repeater.
IP Address: Set the IP Address of the repeater.
TS A/B Voice IP Ports RX: Set receive port for voice communication using slot1/slot2.
TS A/B Voice IP Ports TX: Set transmitting port for voice communication using slot1/slot2.
TS A/B Data IP Ports RX: Set receive port for data communication using slot1/slot2. The data ports are common with TS A/B Voice IP Ports RX setting.
TS A/B Data IP Ports TX: Set transmitting port for data communication using slot1/slot2.

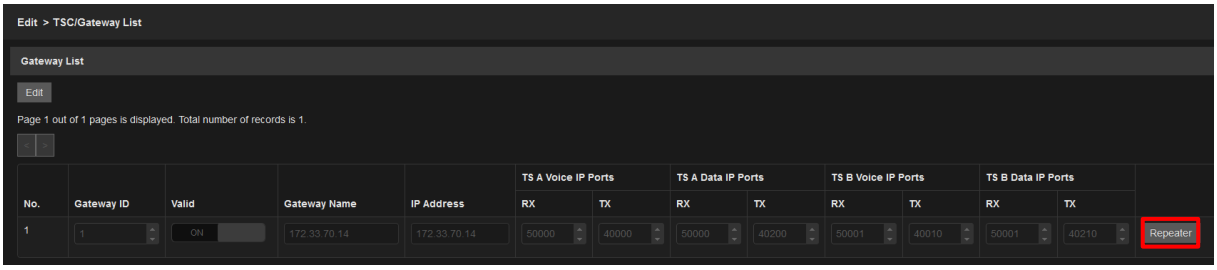
Edit > TSC/Gateway List > TSC ID1:Channel List



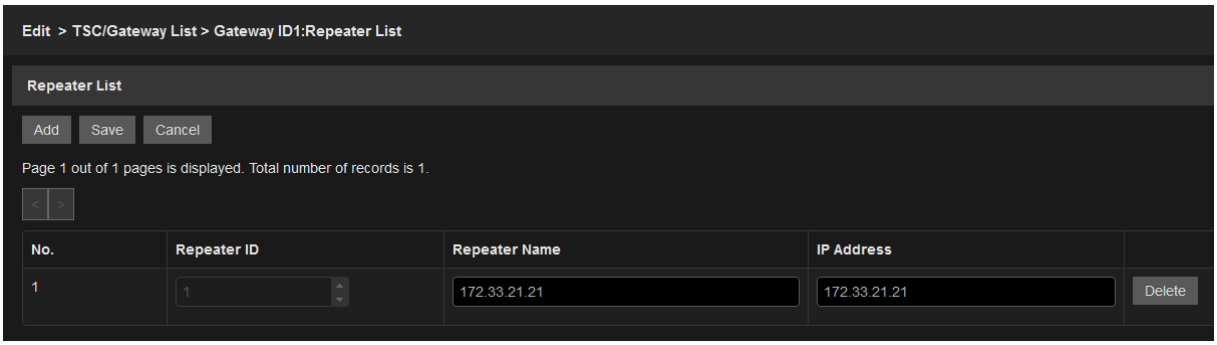
3.2.2.3. Repeater List

Register all repeaters connected with the DMR Tier II system. This configuration is used for monitoring Busy Status of each repeaters by IP Gateway. (Busy Monitoring function)

Edit > TSC/Gateway List



Edit > TSC/Gateway List > Gateway ID1:Repeater List



Repeater ID: Unique number to manage Repeater.
Repeater Name: Any Name to identify each repeater.
IP Address: Set the IP Address of the repeater.

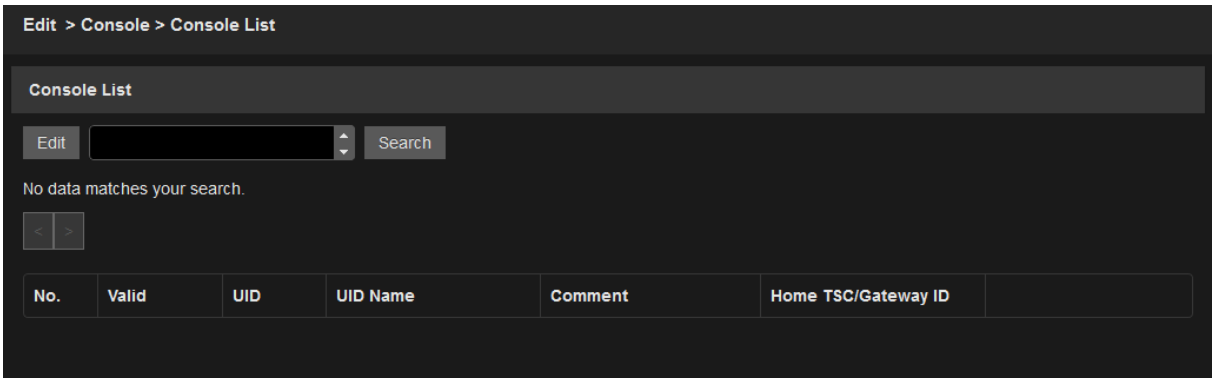
3.2.3. Console

In Console menu, it is registered console connected with IP Gateway.

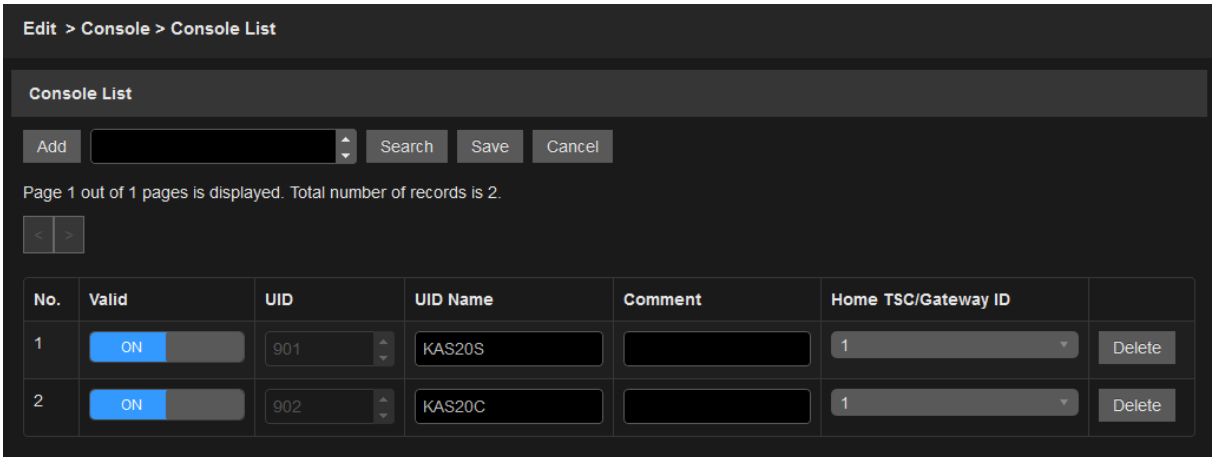
3.2.3.1. Console List

Register a console connected with the DMR system. This configuration is for console to do registration to IP Gateway. The maximum number of consoles that an IP Gateway can connect is 100. Therefore, it can be registered the range from 1 to 100 in Console List.

Edit > Console List



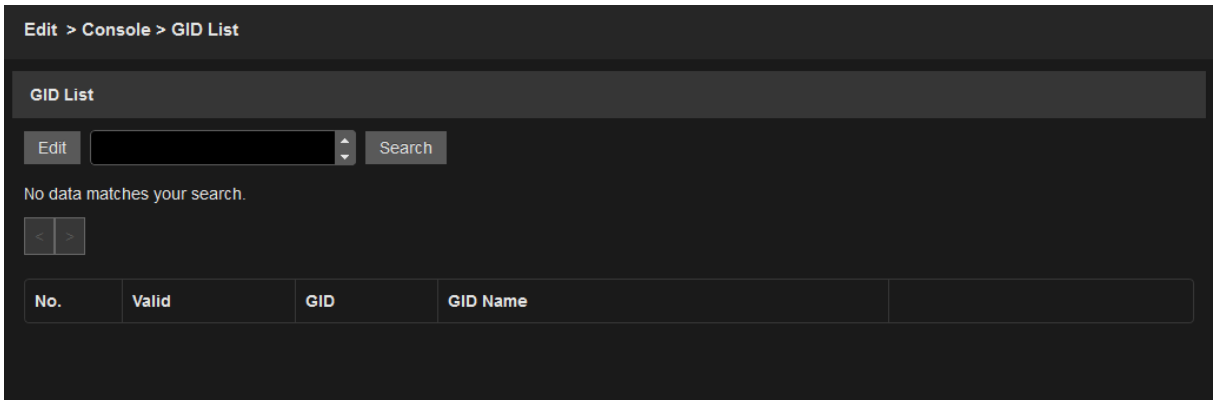
Valid: Enabling/Disabling to connect the console in the system.
UID: Set console ID. It must be matched console ID assigned for the console.
UID Name: Any name to identify each console.
Comment: Any comment for each console.
Home TSC/Gateway ID: Select TSC ID from TSC/Gateway List. The console makes a call request to the TSC.



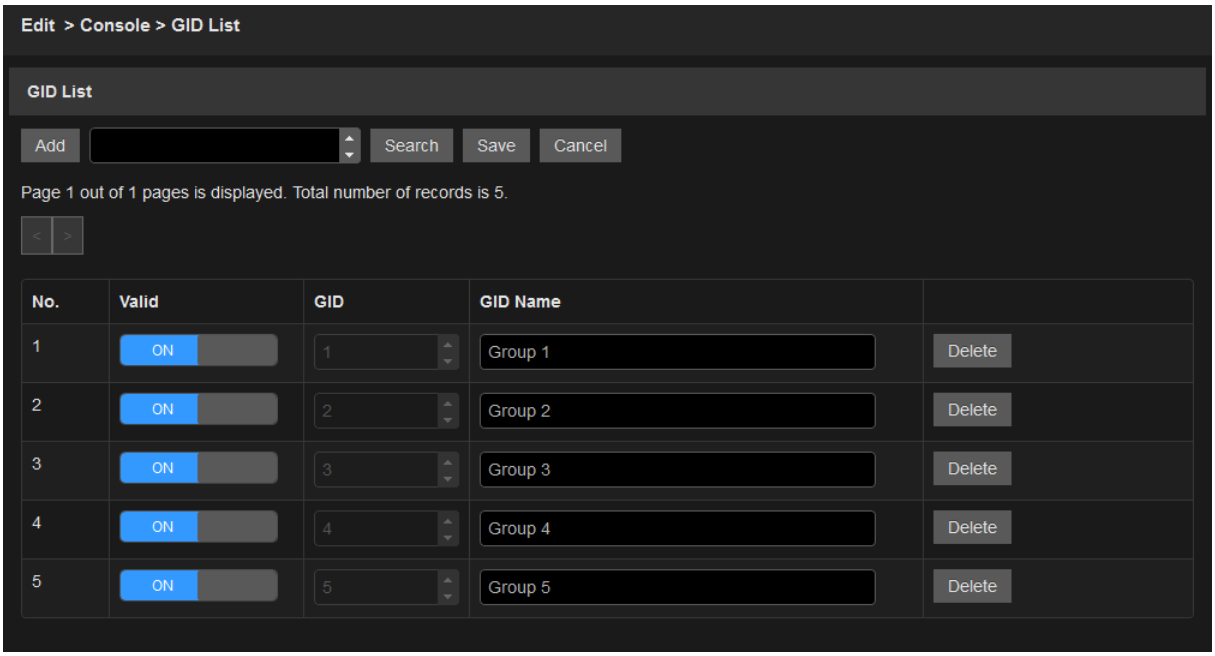
3.2.3.2. GID List

Register GIDs used on a console. This configuration is for console to do group registration to IP Gateway. The maximum number of GIDs that a console can use is 10000. Therefore, it can be registered the range from 1 to 10000 in GID List.

Edit > GID List



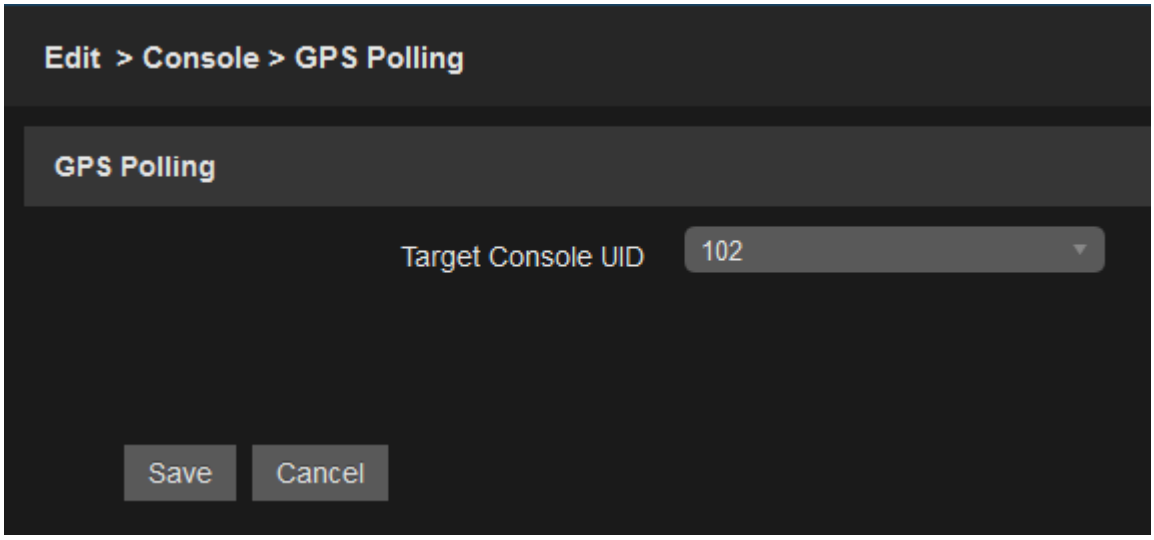
Valid: Enabling/Disabling to use GID in the system.
GID: Set GID. It must be matched GID configured for the console.
GID Name: Any name to identify each GID.



3.2.3.3. GPS Polling

IP Gateway may receive location information that does not have specific Console UID as Destination ID. IP Gateway sends the location information to Target Console UID when receiving unaddressed location information. This function is used for USBD Polling Service.

Edit > Console > GPS Polling



Target Console UID: Select UID from Console List.

Note:

- It is recommended to set KAS-20S UID for Target Cnsole UID.

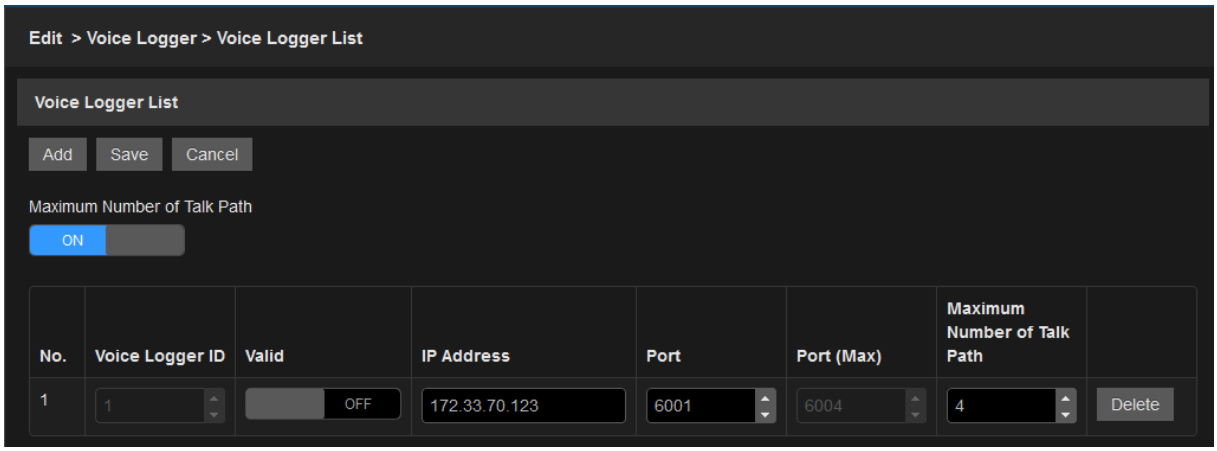
3.2.4. Voice Logger

In Voice Logger menu, it is registered voice logger connected with IP Gateway.

3.2.4.1. Voice Logger List

Register IP Address and Port of connected Voice Logger. This configuration is for target of RTP packet is sent. The maximum number of voice loggers that an IP Gateway can connect is 10. Therefore, it can be registered the range from 1 to 10 in Voice Logger List.

Edit > Voice Logger > Voice Logger List

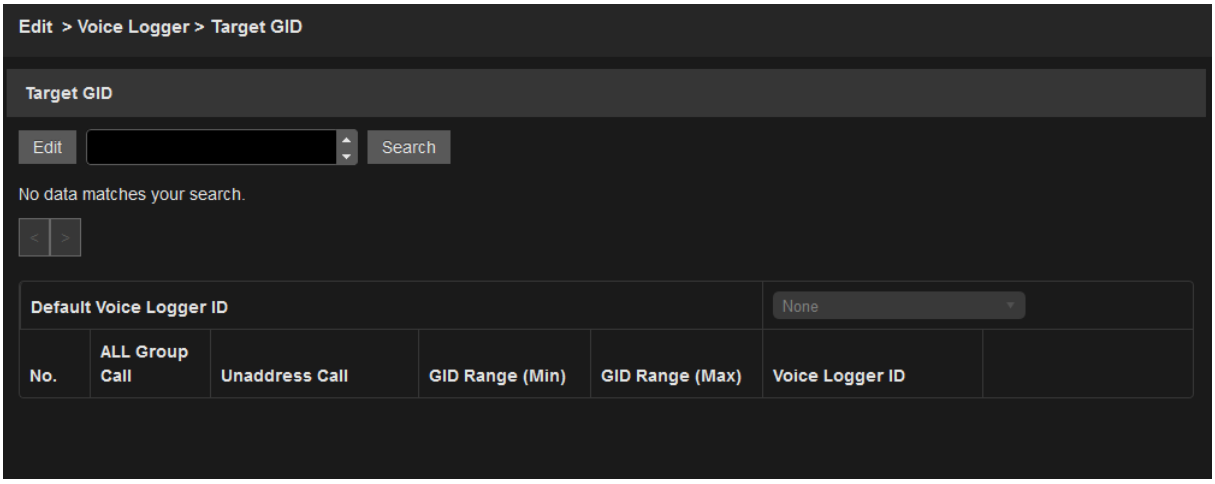


Voice Logger ID: Unique number to manage Voice Logger. The ID is used on Target GID/UID.
Valid: Enabling/Disabling to connect the Voice Logger in the system.
IP Address: Set the IP Address of the Voice Logger. (Tier II only)
Port: Set the receive port of Voice Logger. IP Gateway sends a packet to Voice Logger using the port.
Maximum Number of Talk Path: Set the receive port range. If “Maximum Number of Talk Path” above the list is enabled, this configuration is active.

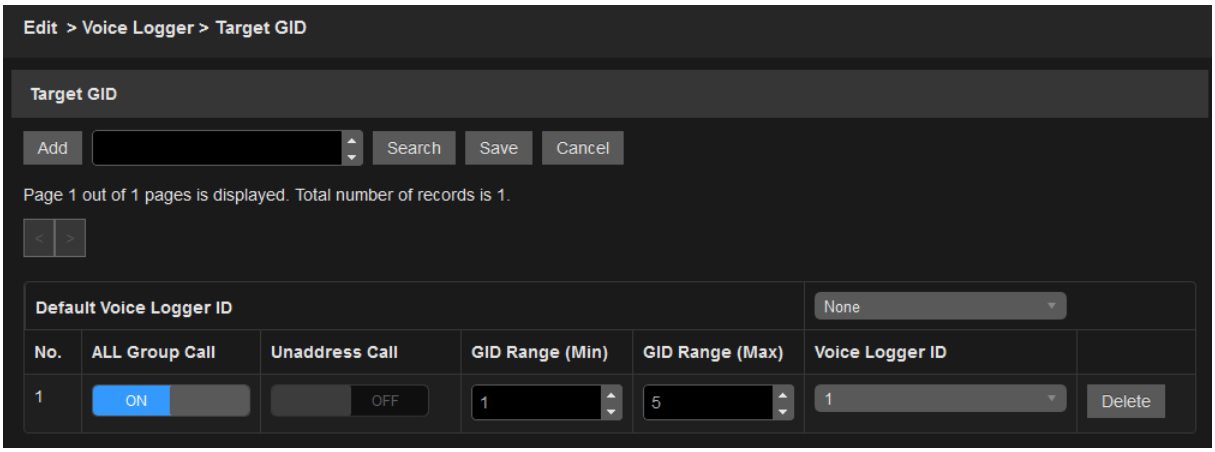
3.2.4.2. Target GID

The target GID of recording is configured by range.

Edit > Voice Logger > Target GID



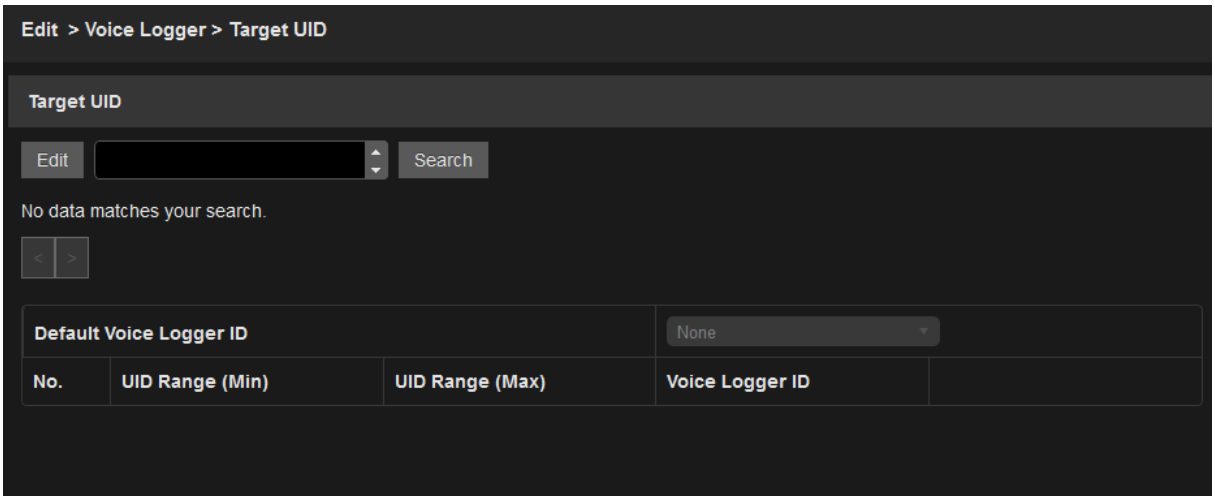
Default Voice Logger ID: Select Voice Logger ID from Voice Logger List. Default Voice Logger ID is for recording Group Calls other than Target GID configuration.
ALL Group Call: Enable for recording All Group Call.
Unaddress Call: Enable for recording Unaddress Call.
GID Range (Min/Max): Set GID Range for recording. Set same GID in GID Range (MIN) / GID Range (MAX) for recording only one GID.
Voice Logger ID: Select Voice Logger ID from Voice Logger List. All Group call / Unaddress call / Group calls of GID Range are recorded to the Voice Logger ID.



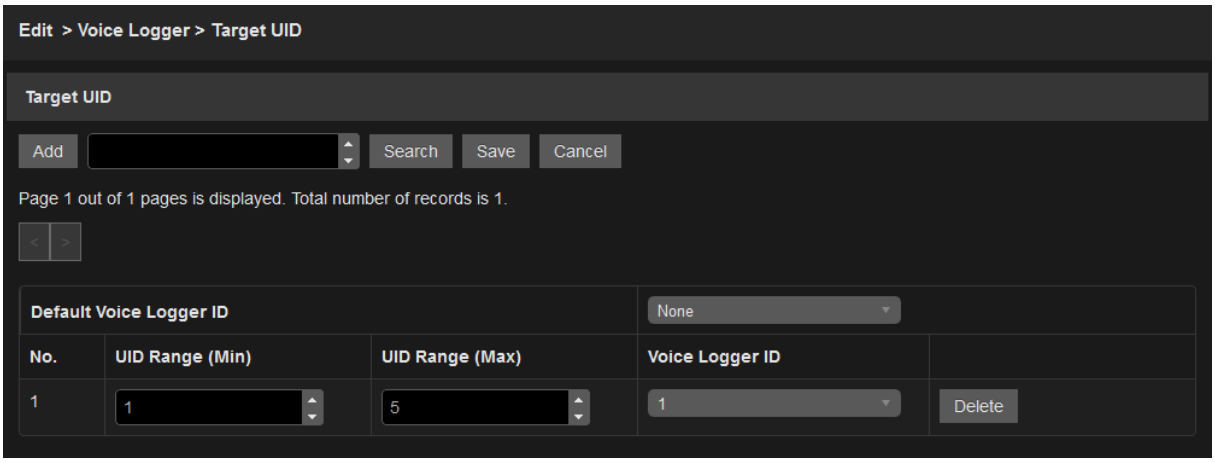
3.2.4.3. Target UID

The target UID of recording is configured by range.

Edit > Voice Logger > Target UID



Default Voice Logger ID: Select Voice Logger ID from Voice Logger List. Default Voice Logger ID is for recording Individual Calls other than Target UID configuration.
UID Range (Min/Max): Set UID Range for recording. Set same UID in UID Range (MIN) / UID Range (MAX) for recording only one UID.
Voice Logger ID: Select Voice Logger ID from Voice Logger List. Individual calls of UID Range are recorded to the Voice Logger ID.



3.2.5. Advanced Settings (Admin User Only)

In Advanced Settings, it is configured various settings about IP Gateway communication protocol. The recommendation is default settings. The settings are available to modify the port number and timer dependent on network condition. Only admin user can edit the Advanced Settings using web interface. If other than admin user logins, Advanced Settings menu does not display.

3.2.5.1. Parameters 1

Parameter 1 is used between IP Gateway and Console. The following items are default values according to DMR AIS.

Port

Receive Port from Console: Default is “5060”. If the port number is modified, it must be matched with transmitting port of console.

AIS Configuration Timers

Registration Default Expires [s]: Time for IP console registration to expire. Default is “3600”.
Registration Minimum Expires [s]: Minimum time of expires that IP Gateway can allow for console registration. Default is “1800”.
Registration Maximum Expires [s]: Maximum time of expires that IP Gateway can allow for console registration. Default is “43200”.
Keep Alive Time [s]: Time to expire session between IP console and IP Gateway. Default is “60”.

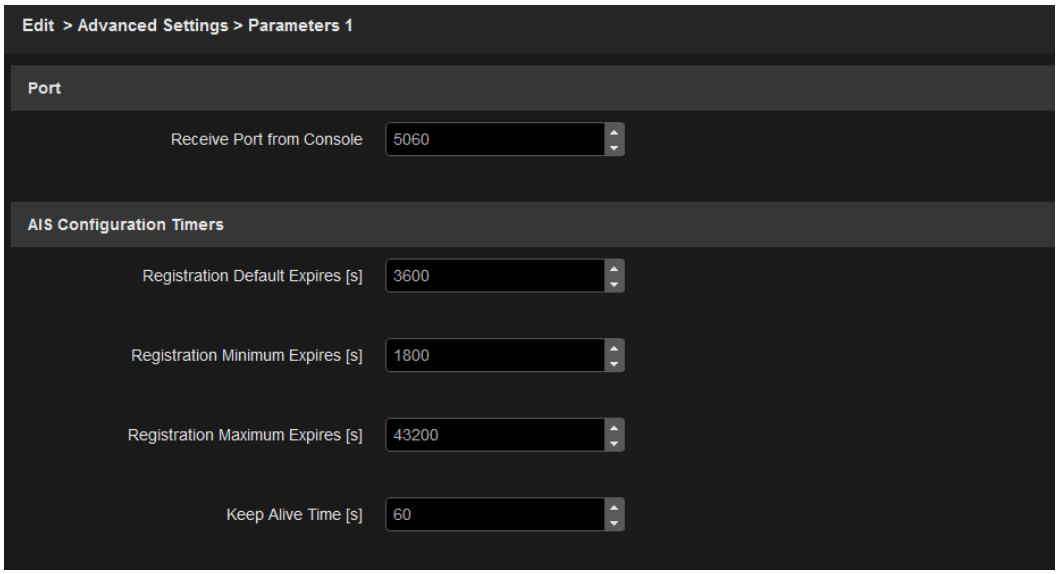
SIP Timers

T1 [ms]: Each Timer for AIS SIP are calculated based on T1. Default is “5000”.

RTP Timers

T_heartbeat [s]: IP Gateway sends AIS RTP Heartbeat packet at T_heartbeat intervals. Default is “10”.
T_end [ms]: IP Gateway sends AIS RTP PTT End packet at T_end intervals. Default is “20”.
T_numend: It’s the number of AIS RTP PTT End packet sends. Default is “3”.

Edit > Advanced Settings > Parameters 1



3.2.5.2. Parameters 2

Parameter 2 is used between IP Gateway and KAIROS repeater.

Port

Receive Port from Repeater: Default is “60000”. If the port number is modified, it must be matched with transmitting port of repeater.

Repeater Session Timers

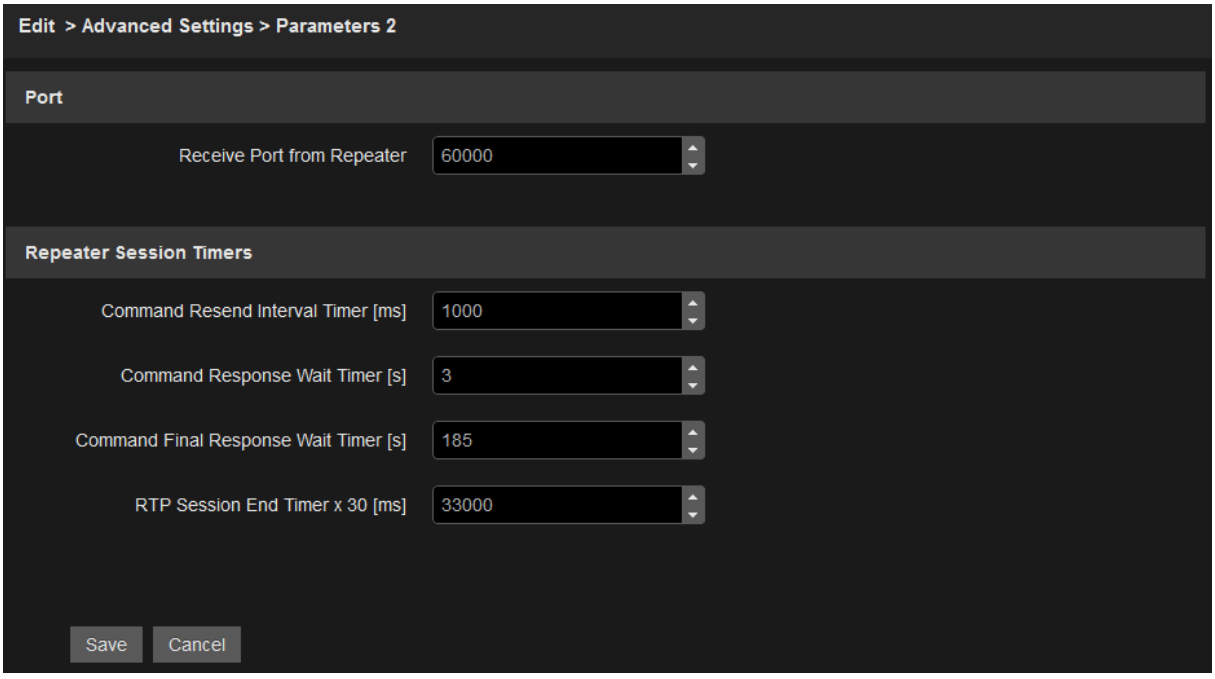
Command Resend Interval Timer [ms]: JSON message from IP Gateway to repeater is sent at the interval timer. Default is “1000”.

Command Response Wait Timer [s]: Wait timer to respond from repeater. When IP gateway sends JSON message to the repeater, the wait timer starts to count. Default is “3”.

Command Final Response Wait Timer [s]: Final wait timer to respond from repeater. When IP gateway receives response message from the repeater, the timer starts to count. The default is “185”.

RTP Session End Timer x 30 [ms]: RTP Session time to expire. When RTP Session is established between IP gateway and the repeater, the timer starts to count. After IP Gateway stops receiving RTP packets and the timer expires, RTP Session terminates. Default is “33000”.

Edit > Advanced Settings > Parameters 2



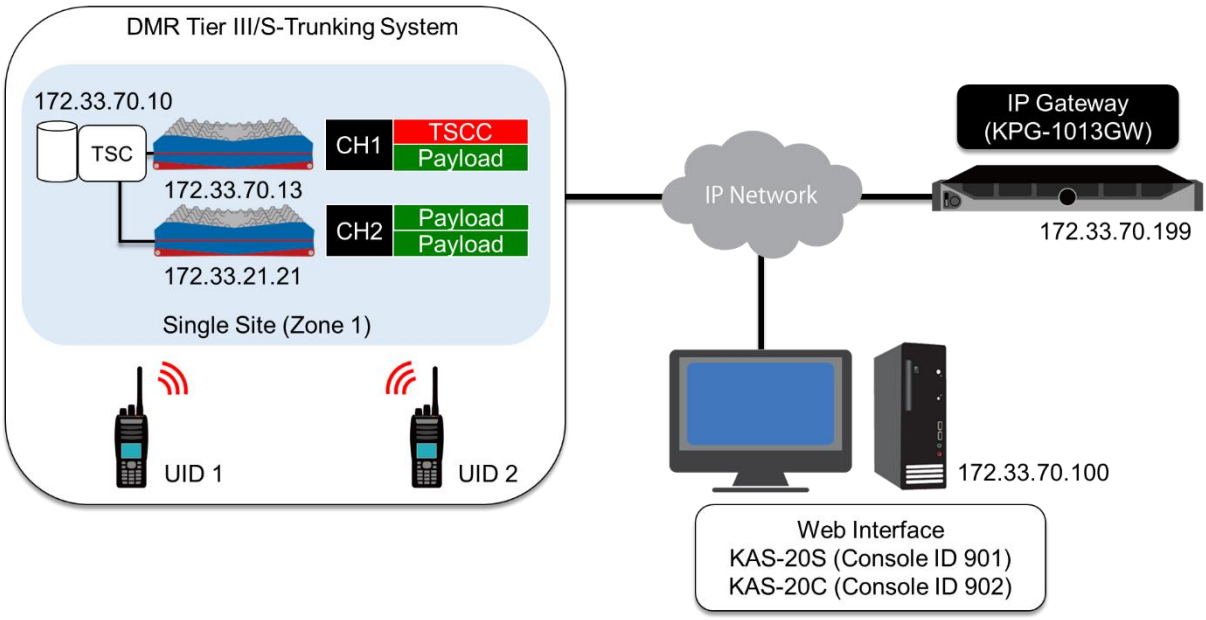
3.3. Basic Configurations w/ Tier III/S-Trunking and KAS-20

This section describes how to set system configuration with IP Gateway, DMR Tier III/S-Trunking System and one KAS-20 Dispatch Console. KAS-20 is used Version 2.00.
The following flow is for building the model case. Please refer “AN-19-0001_DMR_Tier3_KAIROS_Trunking.pdf” how to configure DMR Tier III Trunking System.

Target

Make a call between radio and console.

Model Case



Configuration Flow

How to configure IP Gateway and KAIROS repeater

Step1 Server Configurations w/ IP Gateway

▼

Step2 TSC/Gateway List w/ IP Gateway

▼

Step3 Channel List w/ IP Gateway

▼

Step4 External Servers w/ KA NMS

How to configure IP Gateway and KAS-20

Step5 Console configuration w/ KAS-20S/KAS-20C

▼

Step6 Console List w/ IP Gateway

▼

Step7 GID List w/ IP Gateway

▼

Step8 Gateways w/ KA NMS

▼

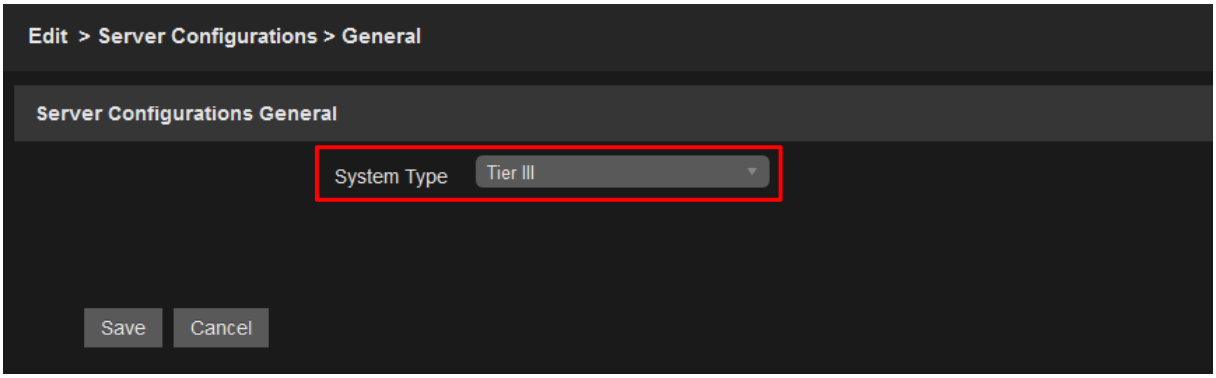
Step9 Individual ID List w/ KA NMS and KAS-20C

3.3.1. Step1: Server Configurations w/ IP Gateway

"Tier III" and "S-Trunking" are selectable for System Type if Tier III license "KWD-1013T3" and S-Trunking license "KWD-1013ST" are activated for IP Gateway.

System Type: Tier III, S-Trunking

Edit > Server Configurations > General

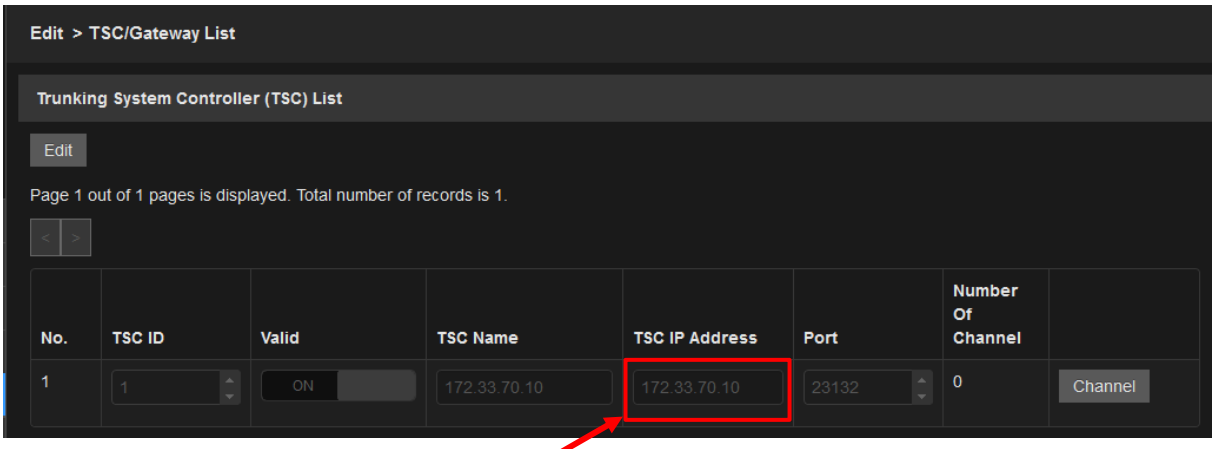


3.3.2. Step2: TSC/Gateway List w/ IP Gateway

Add TSC IP Address and Port information on TSC/Gateway List. It can be confirmed IP address of TSC by KA NMS. KAIROS repeater's port is fixed. The port cannot be changed by user flexibly.

Assign correct IP address of TSC.
Port: 23132 (Default)

Edit > TSC/Gateway List



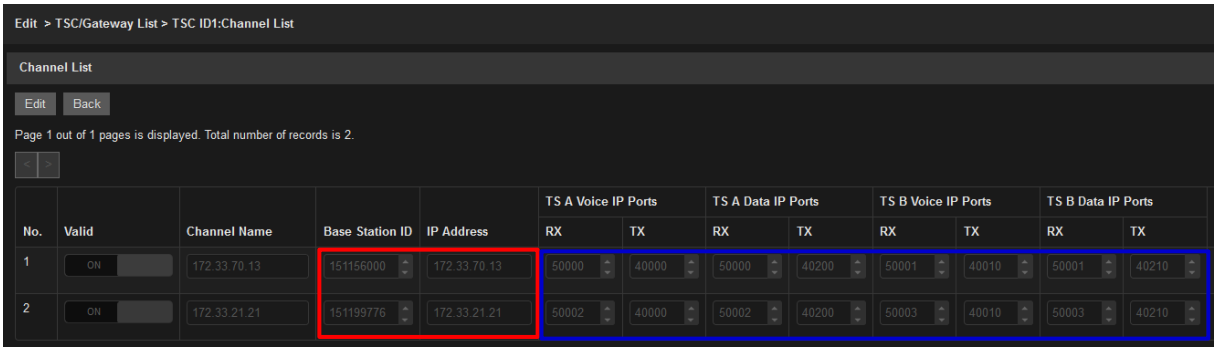
KA NMS

3.3.3. Step3: Channel List w/ IP Gateway

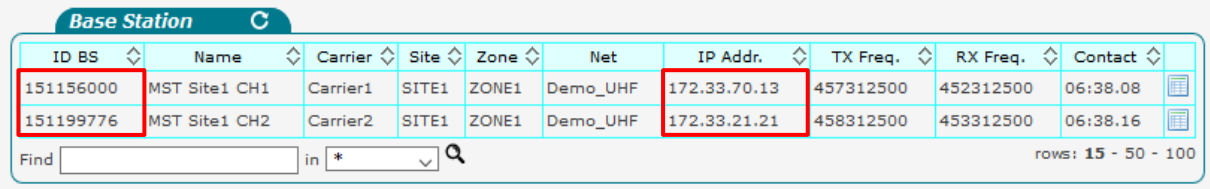
Add Base Station ID, IP Address, Voice/Data Port of all channels used in the system on Channel List. It must be confirmed IP address and Base Station ID of repeaters by KA NMS. Moreover, voice/data port is confirmed by KAIROS Manager

Assign correct IP address and RTP ports of repeaters connect with system.
Voice and Data Rx Ports are common.
The Tx/Rx port of each repeater are matched using KAIROS Manager.

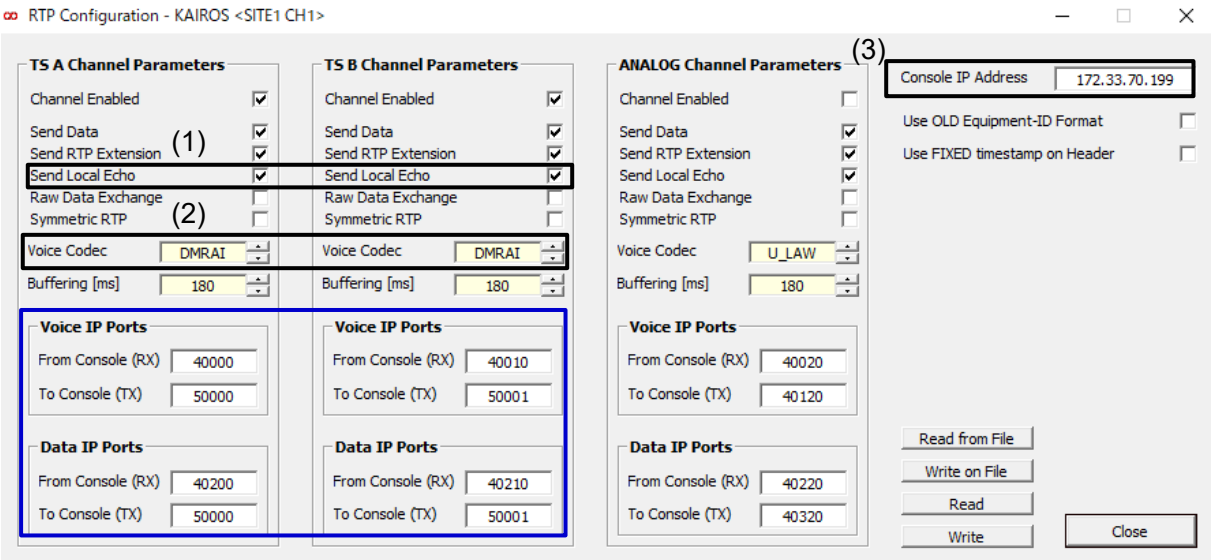
Edit > TSC/Gateway List > TSC ID1:Channel List



KA NMS > Status > Base Station

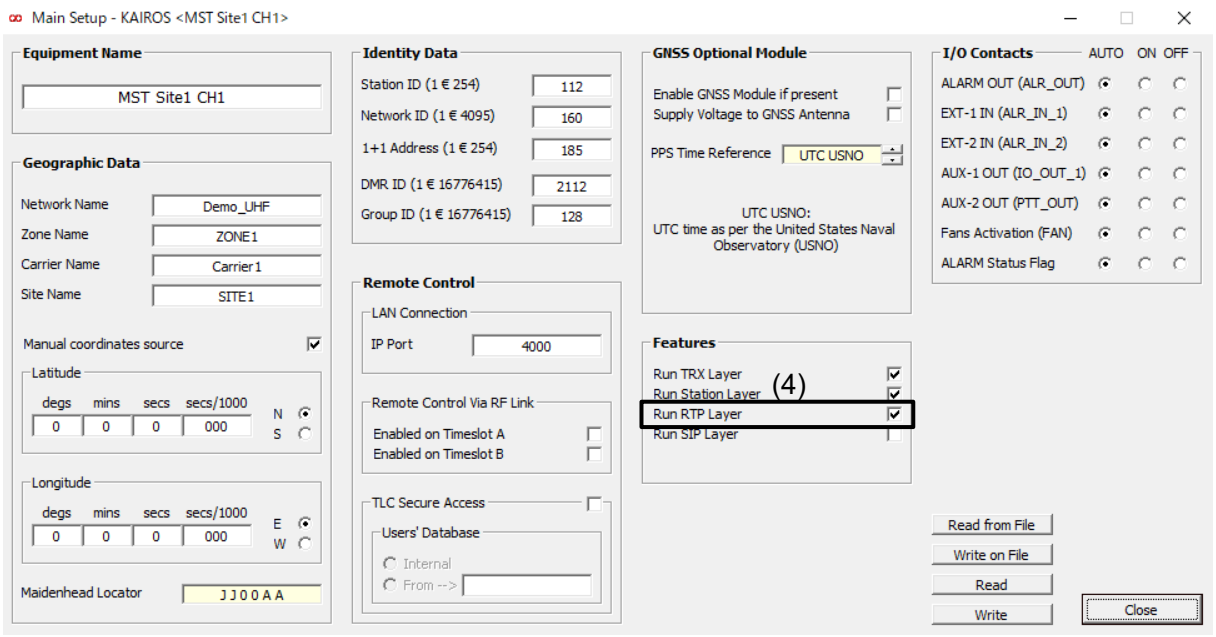


KAIROS Manager > KAIROS Menu > Configuration > RTP Configuration



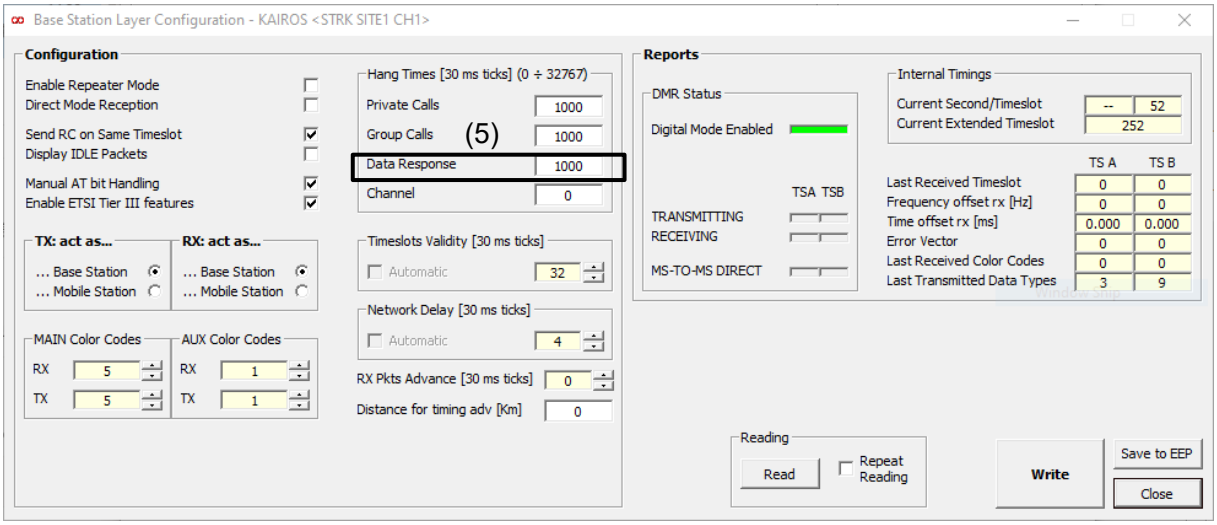
(1) Enable “Send Local Echo”.
(2) Voice Codec sets to “DMRAI”.
(3) Console IP Address is set the IP Address for IP Gateway. It’s “172.33.70.199”.

KAIROS Manager > KAIROS Menu > Configuration > Main Setup



(4) Enable “Run RTP Layer”. RTP layer should be activated only if RTP interface is used.

KAIROS Manager > KAIROS Menu > Configuration > Base Station Layer Configuration

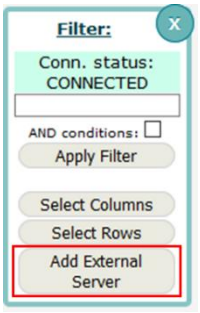


(5) Set “Data Response” to 1000.

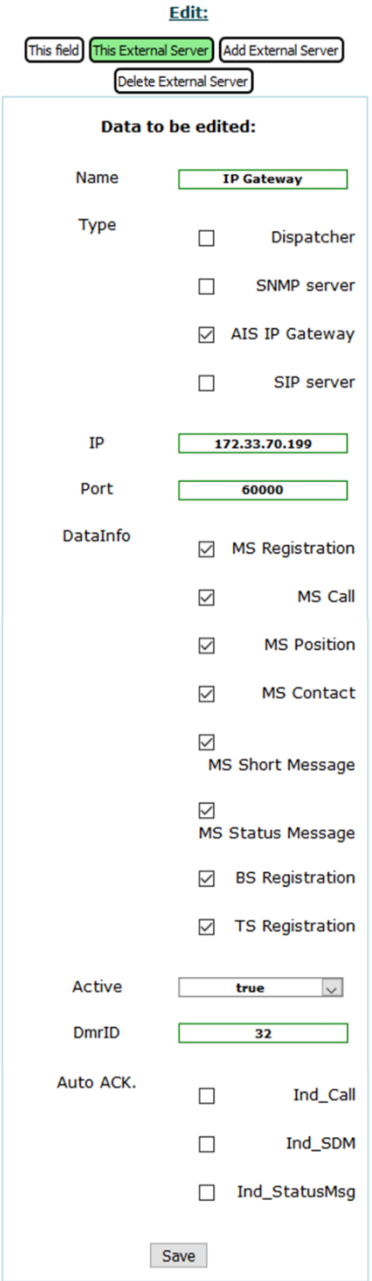
3.3.4. Step4: External Servers w/ KA NMS

KA NMS has the menu “External Servers”. The external server information is added to connect with TSC on this menu. Add the external server for IP Gateway.

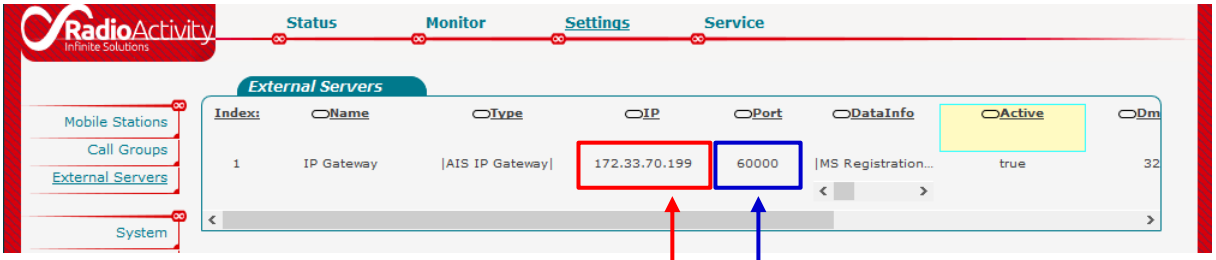
KA NMS > Settings > External Servers



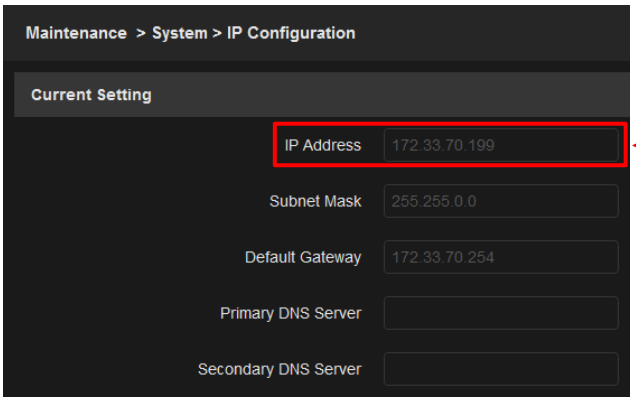
Configure the each parameters below.



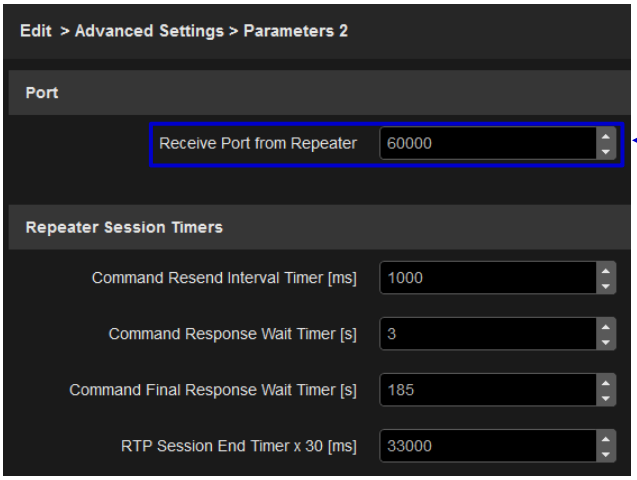
Name: Any name to identify external server.
(Exp. IP Gateway)
Type: Enable “AIS IP Gateway”.
IP: Set IP Address of IP Gateway.
Port: Match to “receive port from repeater” of IP Gateway.
Use default port number.
DataInfo: Enable “MS Registration”.
Enable “MS Cal”.
Enable “MS Position”.
Enable “MS Contact”.
Enable “MS Short Message”.
Enable “MS Status Message”.
Enable “BS Registration”.
Enable “TS Registration”.
Active: Select “true”.
DmrID: Any DMR ID.
Auto ACK.: Disable “Ind_Call”.
Disable “Ind_SDM”.
Disable “Ind_StatusMsg”.



Maintenance > System > IP Configuration



Edit > Advanced Settings > Parameters 2



[Admin user only]

Use default value “60000”.

If External server setting is changed by KA NMS, Port number must be matched.

Communication Test

Make a Group call Radio to Radio.

If configuration is correct, calling logs are stored on communication log.

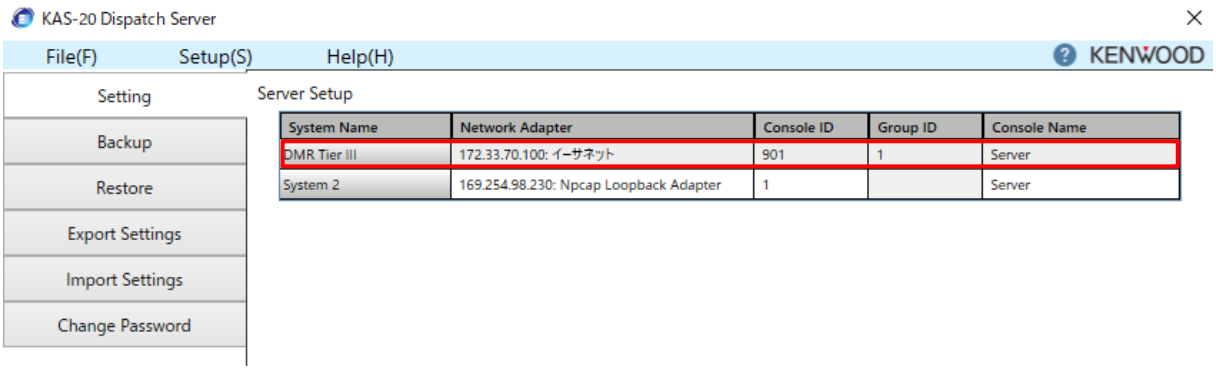
Downloaded communication log file is “IPGW_communication_log_xxxx-xx-xx.csv”.

calling_id	called_id	telephone_number	called_id_type	call_relay	base_station_id	controller_name	timeslot
1	1	unused	G	I	151156000	172.33.70.10	B
3	2	unused	G	I	151199776	172.33.70.10	A
1	3	unused	G	I	151199776	172.33.70.10	B

3.3.5. Step5: Console configuration w/ KAS-20S/KAS-20C

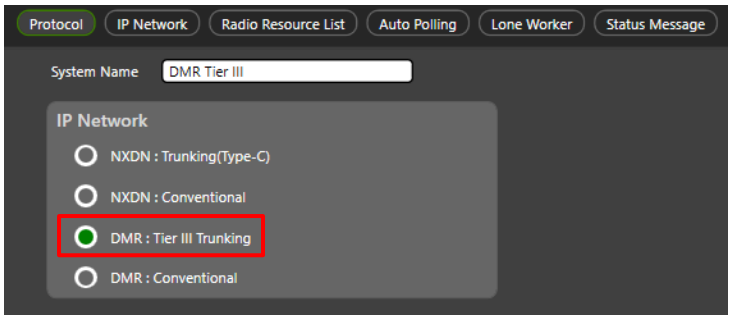
There is a part of configuration for Tier III. For KAS-20S, select Network Adapter and assign Console ID and Group ID. System Name and Fleet Dialing Plan for console ID/Group ID are configured by KAS-20C setting menu. Refer to Basic Operations for KAS-20.
Console ID: 901

KAS-20S

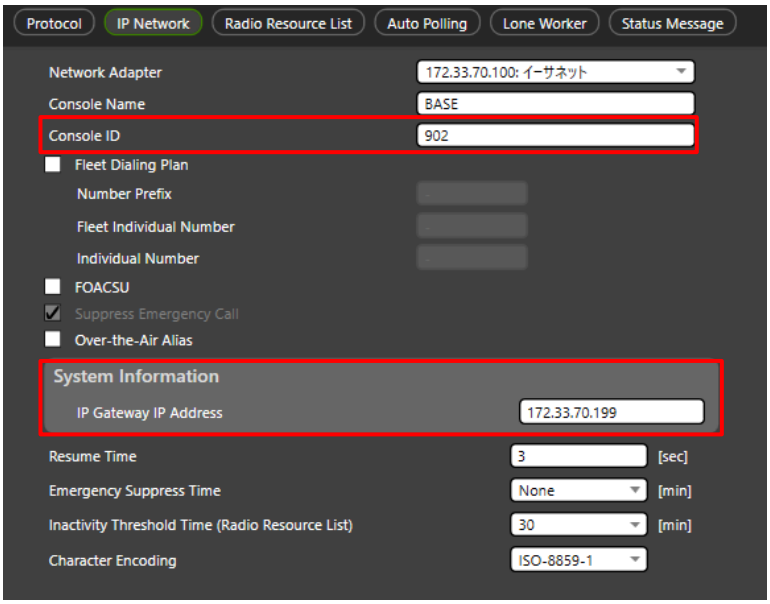


Add system for DMR Tier III Trunking on setting menu of KAS-20C.

KAS-20C



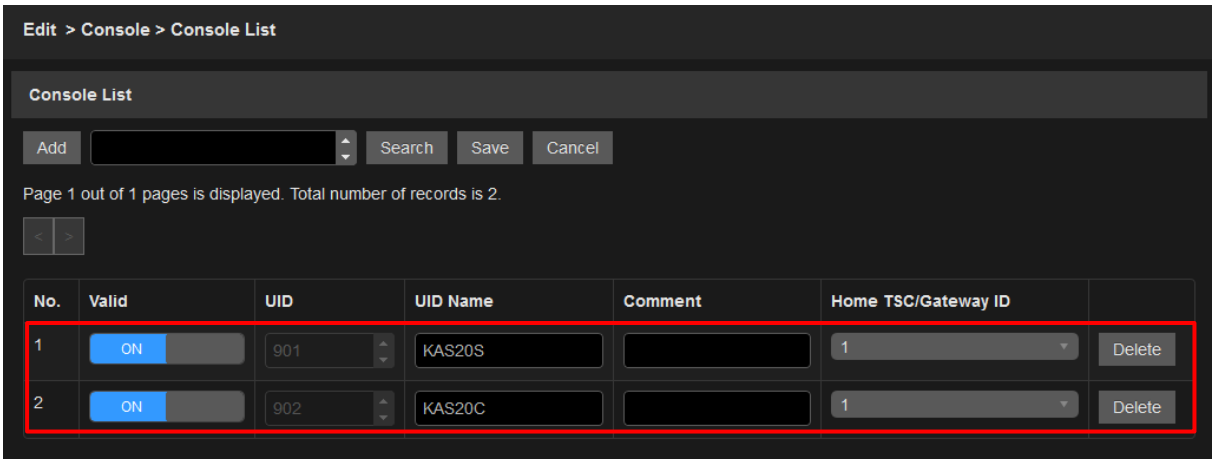
Assign Console ID and IP Gateway IP Address.
Console ID: 902, IP Gateway IP Address: 172.33.70.199



3.3.6. Step6: Console List w/ IP Gateway

Add Console ID connected to the system on Console List. In case of KAS-20, there are two console IDs for KAS-20S and KAS-20C. It must be confirmed the console ID by KAS-20S/C. Moreover, TSC ID connected with IP Gateway is selected from TSC/Gateway List.

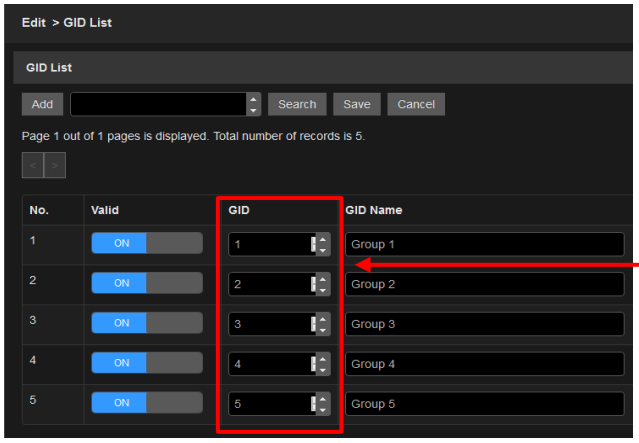
Edit > Console List



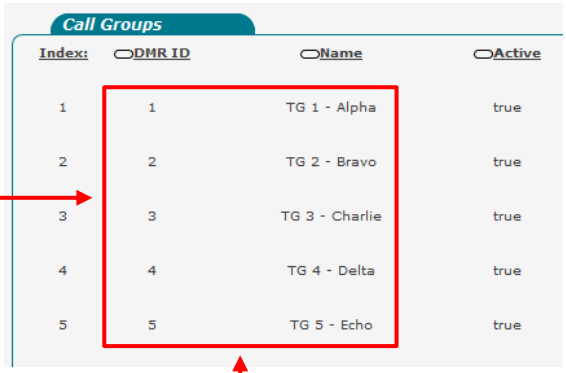
3.3.7. Step7: GID List w/ IP Gateway

Add five GIDs on GID List.
Moreover, same GIDs must be assign to KA NMS and KAS-20C.

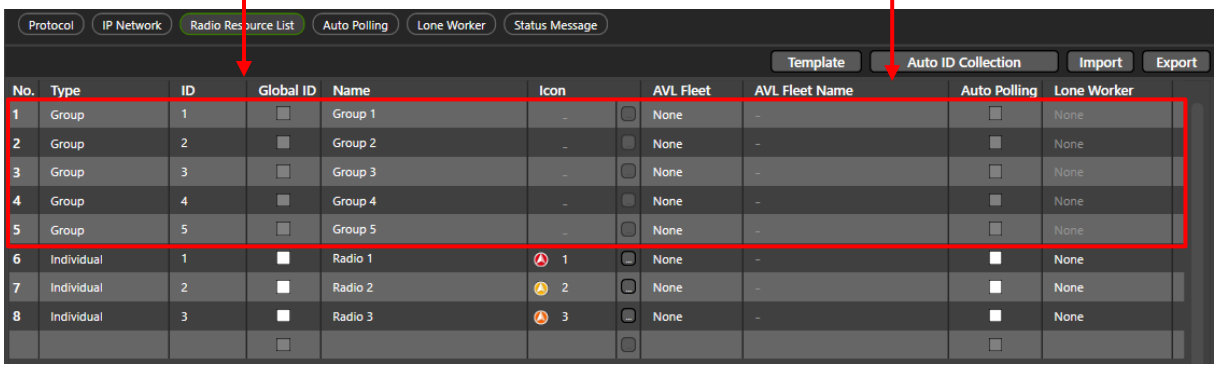
Edit > GID List



KA NMS > Settings > Call Groups



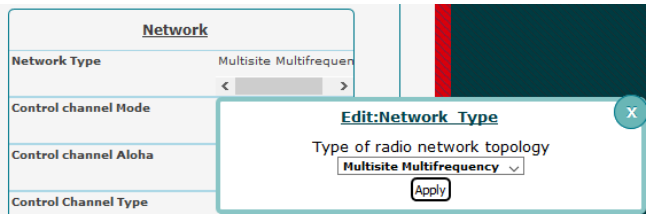
KAS-20C



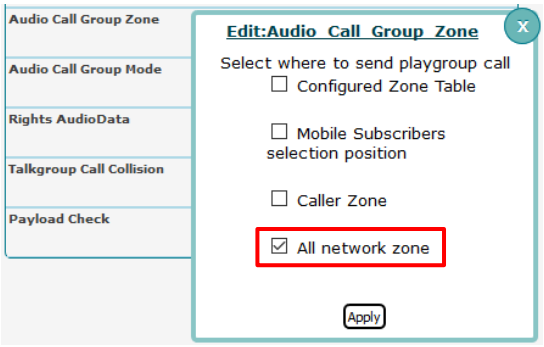
Note:

- This model case is single site. Network Type must be selected “Simulcast/single site”. If the site configuration is multi-site, Audio Call Group Zone must be enabled “All network zone”. Without these settings, Group call does not operate between radio and console correctly.

KA NMS > Settings > System > Network

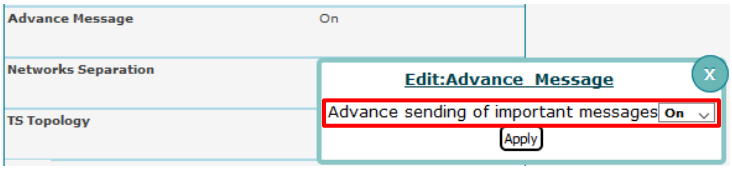


System > Audio/Data Call



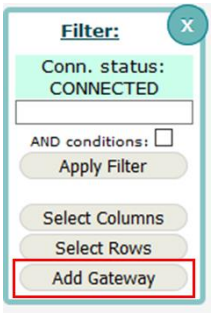
➢ By enabling “Advance Message”, a repeater sends the message for call initiation to console in advance. The setting must be configured for SDM and Voice call.

KA NMS > Settings > System > T3 System

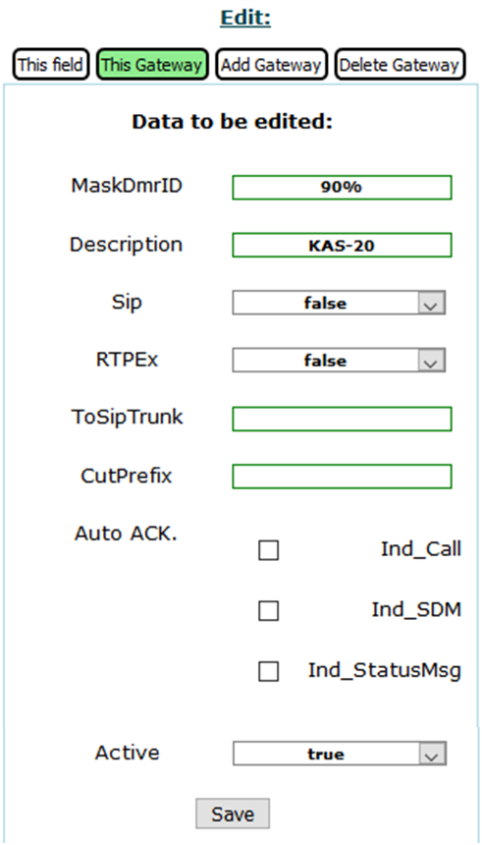


3.3.8. Step8: Gateways w/ KA NMS

KA NMS has the menu “Gateways”. The console information is added to register to KAIROS system on this menu. Add the gateway for console.



Configure the each parameters below.

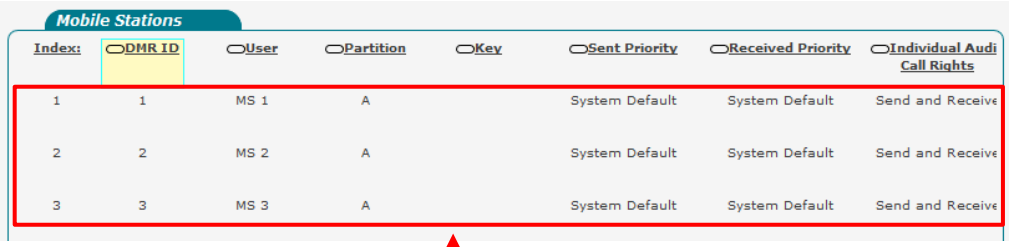


MaskDmrID: Assign console ID. % means wild card. (Exp. Assign 90% if KAS-20 console ID is used from 900 to 909.)
Description: Any name to identify Gateways. (Exp. KAS-20)
Sip: Select “false”.
RTPEx: Select “false”.
ToSipTrunk: No need.
CutPrefix: No need.
Auto ACK.: Disable “Ind_Call”.
Disable “Ind_SDM”.
Disable “Ind_StatusMsg”.
Active: Select “true”.

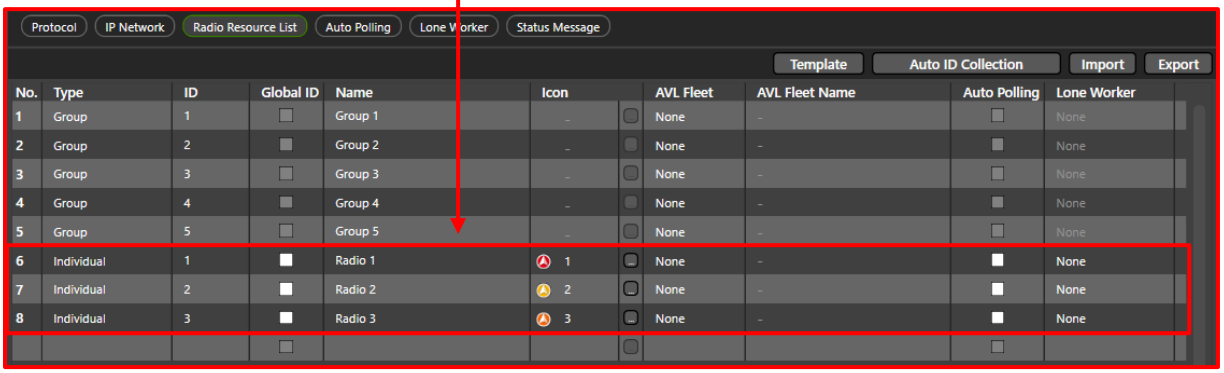
3.3.9. Step9: Individual ID Configuration w/ KA NMS and KAS-20C

Add Individual IDs on KAS-20C.
Moreover, same Individual IDs must be assigned to KAS-20C.

KA NMS > Settings > Mobile Stations

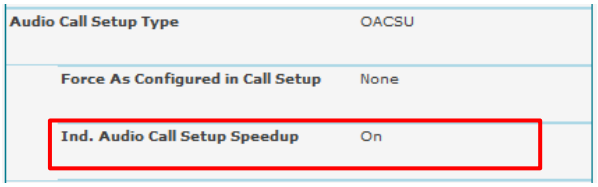


KAS-20C



- Enable “Ind. Audio Call Setup Speedup”. Without this setting, Individual call does not work well between radio to console.

KA NMS > Settings > System > Audio/Data Call



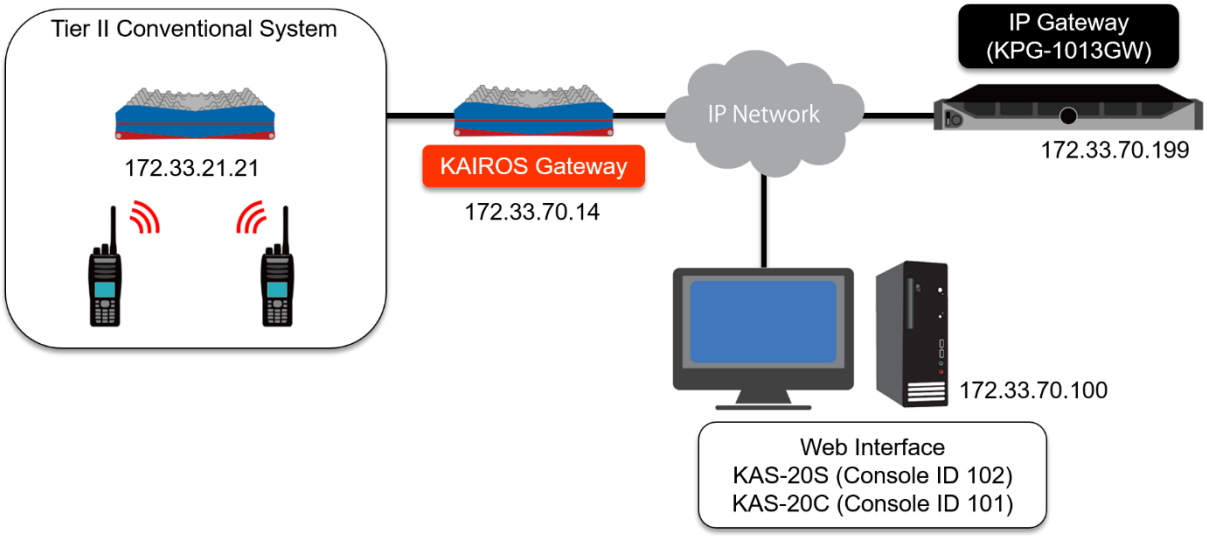
3.4. Basic Configurations w/ Tier II and KAS-20

This section describes how to set system configuration with IP Gateway, DMR Tier II Conventional System and one KAS-20 Dispatch Console. KAS-20 is used Version 3.00.
The following flow is for building the model case. Please refer “AN-19-0002 KAIROS Function Manual_rev110” how to configure DMR Tier II Conventional System.

Target

Make a call between radio and console.

Model Case



Configuration Flow

How to configure IP Gateway and KAIROS repeater

Step1 Server Configurations w/ IP Gateway

▼

Step2 TSC/Gateway List w/ IP Gateway

▼

Step3 Repeater List w/ IP Gateway

How to configure IP Gateway and KAS-20

Step4 Console configuration w/ KAS-20S/KAS-20C

▼

Step5 Console List w/ IP Gateway

▼

Step6 GID List w/ IP Gateway

▼

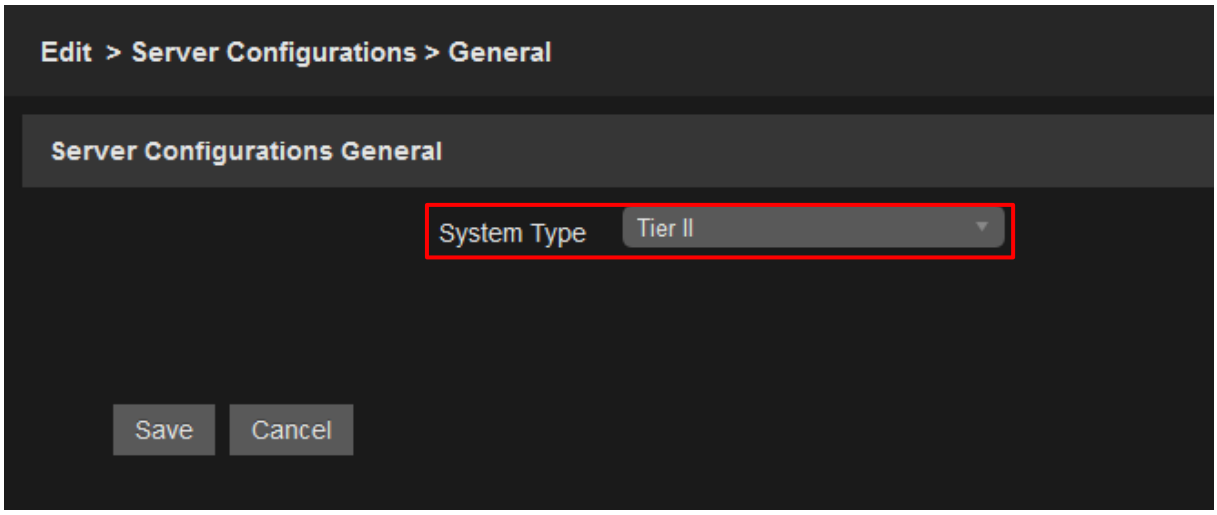
Step7 Individual ID List w/ KAS-20C

3.4.1. Step1: Server Configurations w/ IP Gateway

It can be selected “Tier II” on System Type if the Tier II license “KWD-1013T2” is activated with IP Gateway.

System Type: Tier II

Edit > Server Configurations > General

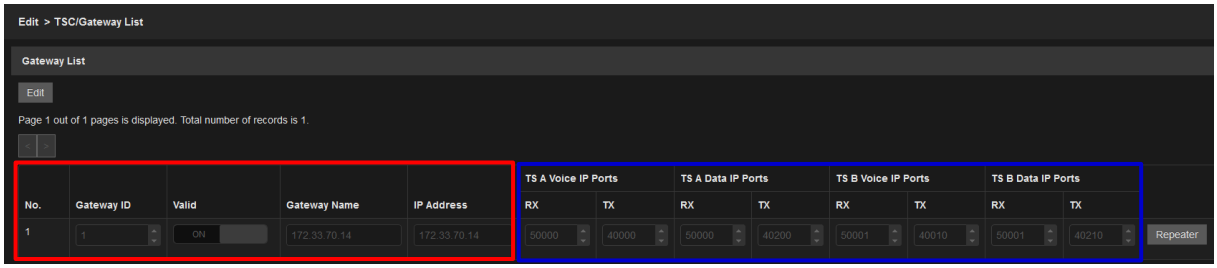


3.4.2. Step2: TSC/Gateway List w/ IP Gateway

Assign Gateway IP Address and Voice/Data Ports information on TSC/Gateway List. These must be matched with KAIROS Gateway configuration. Gateway ID is just identifier for managing Gateway List by IP Gateway. There is no Gateway ID setting on KAIROS Manager.

The Tx/Rx port of KAIROS Gateway are programmed by KAIROS Manager.

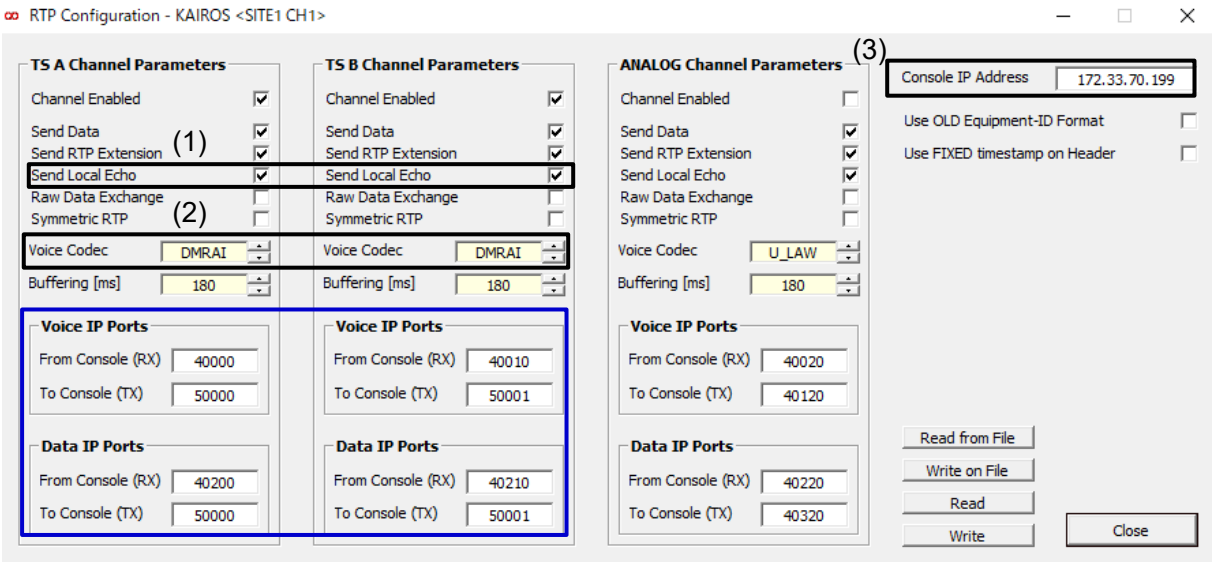
Edit > TSC/Gateway List



Gateway ID : Any ID
Valid : ON
Gateway Name : Any Name
IP Address : KAIROS IP Address

KAIROS Manager > KAIROS Menu > Configuration > RTP Configuration

This setting is for a KAIROS connected to IP Gateway. (172.33.70.14)



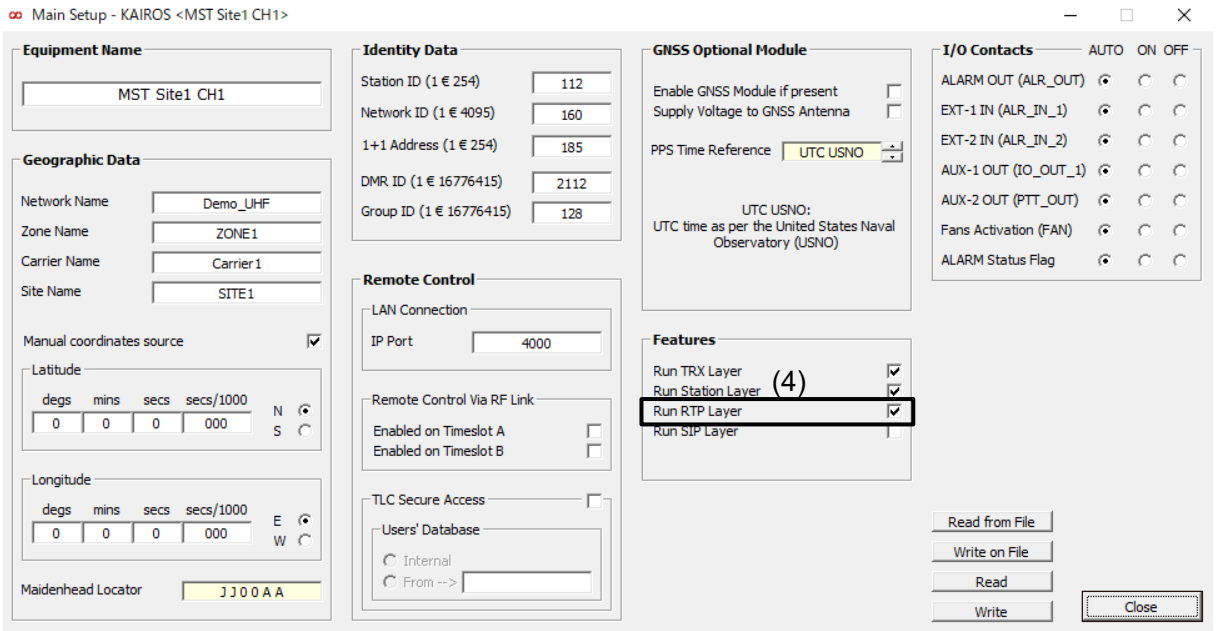
(1) Enable “Send Local Echo”.

(2) Voice Codec sets to “DMRAI”.

(3) Console IP Address is set the IP Address for IP Gateway. It’s “172.33.70.199”.

KAIROS Manager > KAIROS Menu > Configuration > Main Setup

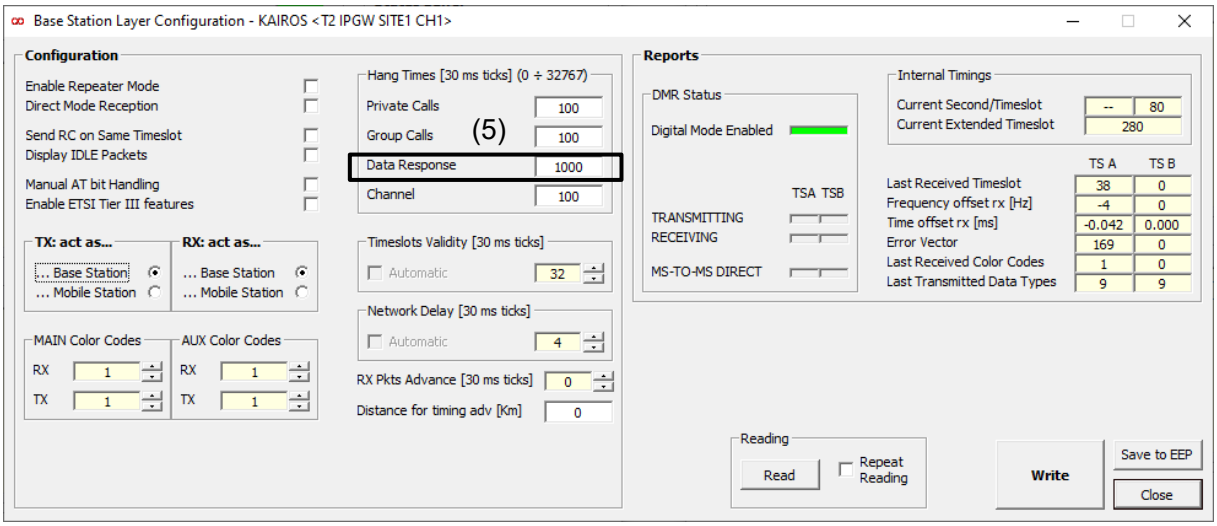
This setting is for a KAIROS connected to IP Gateway. (172.33.70.14)



(4) Enable “Run RTP Layer”. RTP layer should be activated only if RTP interface is used.

KAIROS Manager > KAIROS Menu > Configuration > Base Station Layer Configuration

This setting is not for KAIROS Gateway. KAIROS Repeater needs to set “Data Response” if it has possibility to send long data message.



(5) Set “Data Response” to 1000.

3.4.3. Step3: Repeater List w/ IP Gateway

Assign KAIROS Repeater IP Address on Repeater List. All KAIROS Repeaters in the system need to be added on Repeater List if using “Busy Monitoring” function. IP Gateway uses Repeater List information for monitoring Busy Status of each repeaters. Repeater ID is just identifier for managing Repeater List by IP Gateway. There is no Repeater ID setting on KAIROS Manager.

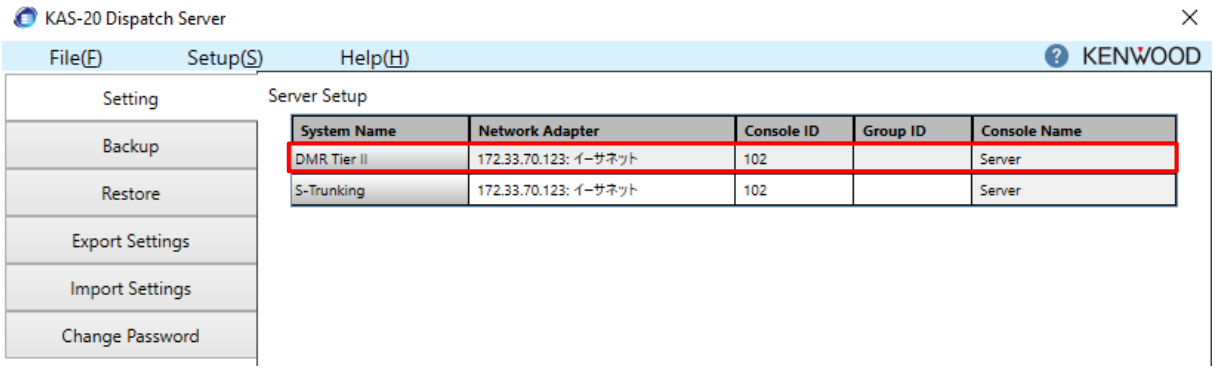
Edit > TSC/Gateway List

Repeater ID : Any ID
Repeater Name : Any Name
IP Address : Repeater IP Address

3.4.4. Step4: Console configuration w/ KAS-20S/KAS-20C

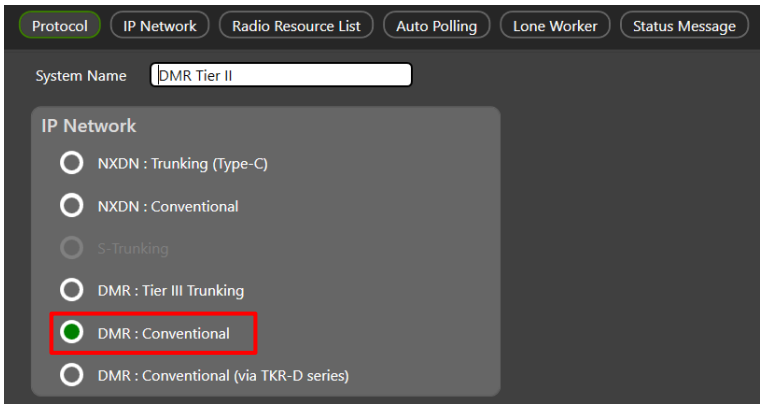
There is a part of configuration for Tier II. For KAS-20S, select Network Adapter and assign Console ID and Group ID. System Name and Fleet Dialing Plan for console ID/Group ID are configured by KAS-20C setting menu. Refer to Basic Operations for KAS-20.
Console ID: 102

KAS-20S

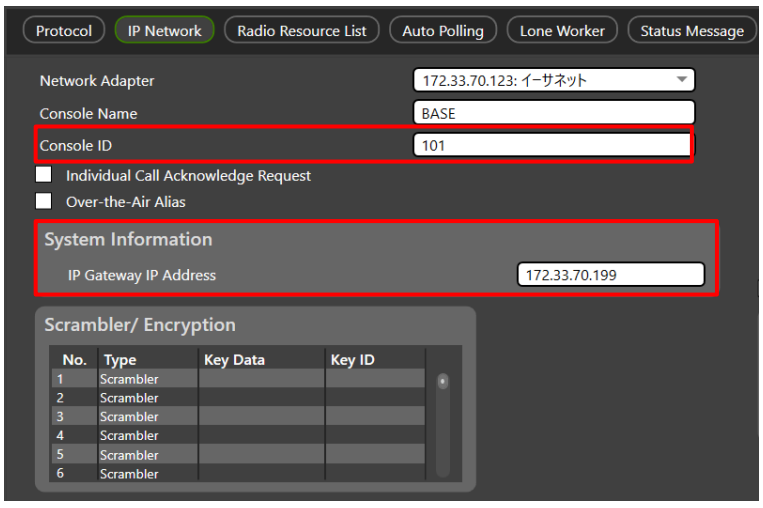


Add system for DMR Tier II Trunking on setting menu of KAS-20C.

KAS-20C



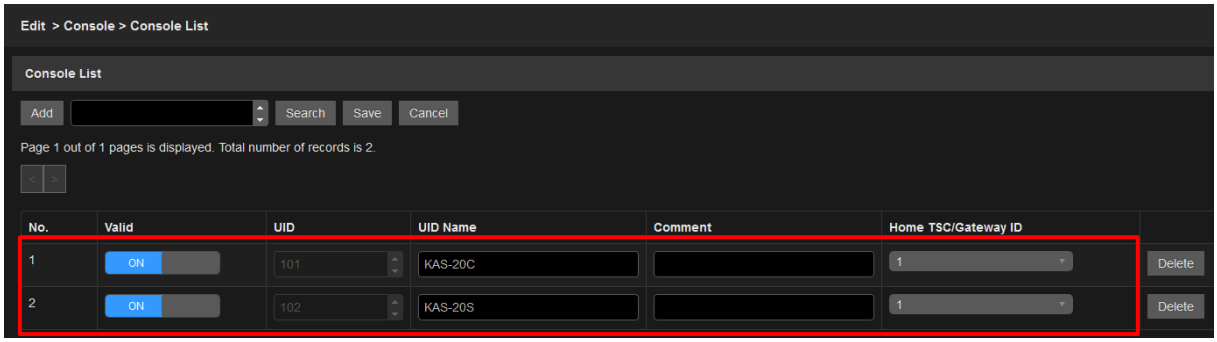
Assign Console ID and IP Gateway IP Address.
Console ID: 101, IP Gateway IP Address: 172.33.70.199



3.4.5. Step5: Console List w/ IP Gateway

Add Console ID connected to the system on Console List. In case of KAS-20, there are two console IDs for KAS-20S and KAS-20C. It must be confirmed the console ID by KAS-20S/C. Moreover, Gateway ID connected with IP Gateway is selected from TSC/Gateway List.

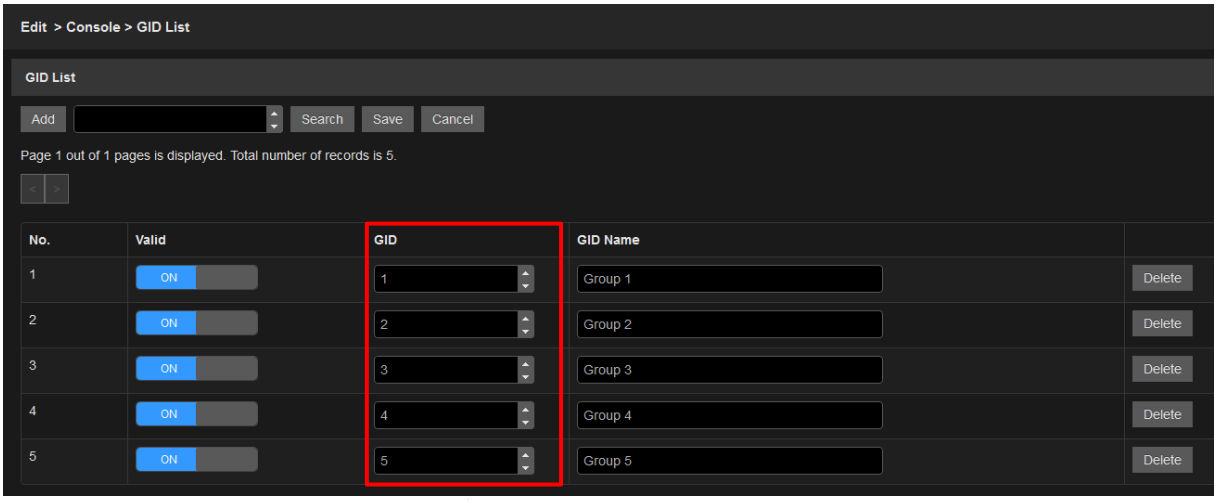
Edit > Console List



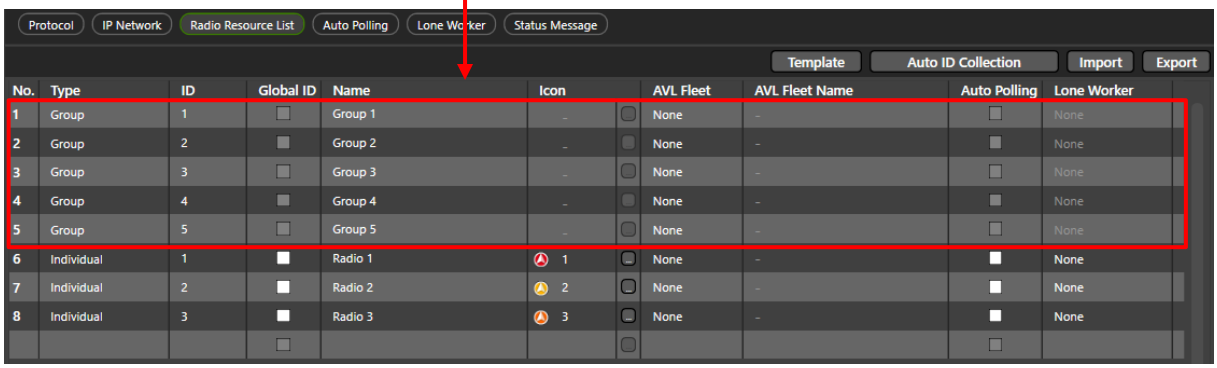
3.4.6. Step6: GID List w/ IP Gateway

Add five GIDs on GID List.
Moreover, same GIDs must be assign to KAS-20C.

Edit > Console > GID List



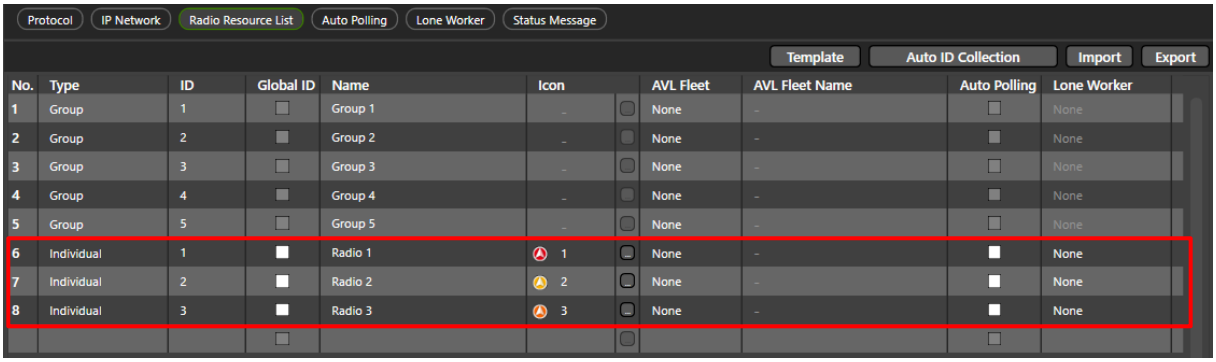
KAS-20C



3.4.7. Step7: Individual ID Configuration w/ KAS-20C

Add Individual IDs on KAS-20C.

KAS-20C



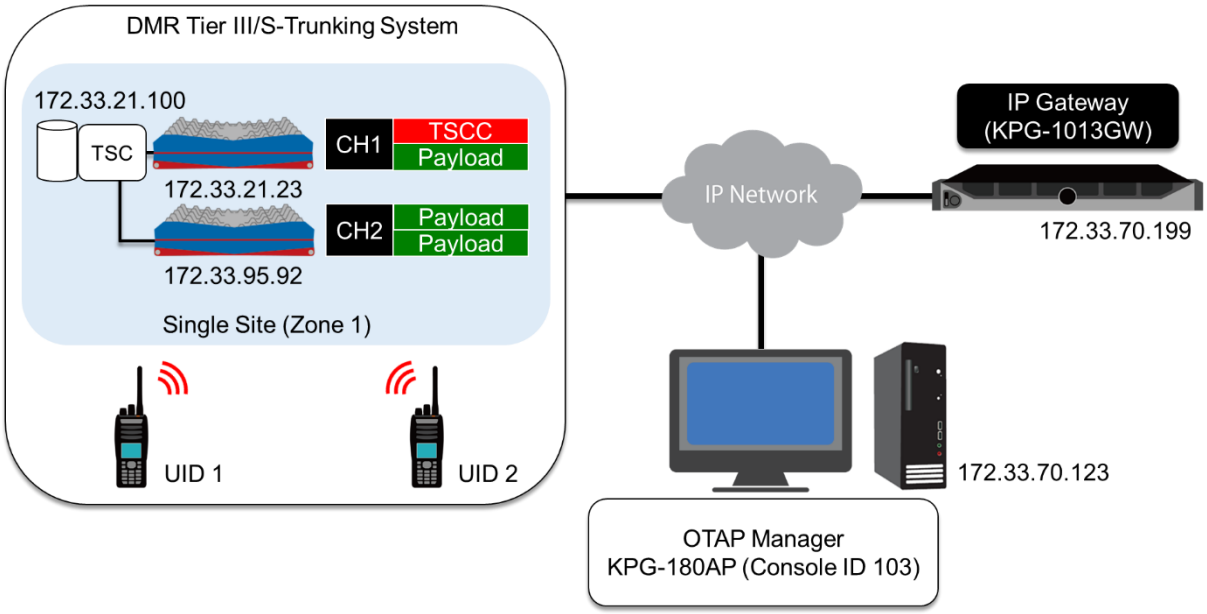
3.5. Basic Configurations w/ Tier III/S-Trunking and KPG-180AP

This section describes how to set system configuration with IP Gateway, DMR Tier III/S-Trunking System and one KPG-180AP OTAP Manager. KPG-180AP is used Version 3.00.
The following flow is for building the model case. Please refer “AN-19-0001_DMR_Tier3_KAIROS_Trunking.pdf” how to configure DMR Tier III Trunking System.

Target

Write a configuration file from OTAP Manager to radio.

Model Case



Configuration Flow

How to configure IP Gateway and KAIROS repeater

Step1	Server Configurations w/ IP Gateway
▼	
Step2	TSC/Gateway List w/ IP Gateway
▼	
Step3	Channel List w/ IP Gateway
▼	
Step4	External Servers w/ KA NMS

How to configure IP Gateway and KPG-180AP

Step5	Console List w/ IP Gateway
▼	
Step6	Communication Profile w/ KPG-180AP

3.5.1. Step1: Server Configurations w/ IP Gateway

See 3.3.1.

3.5.2. Step2: TSC/Gateway List w/ IP Gateway

See 3.3.2.

3.5.3. Step3: Channel List w/ IP Gateway

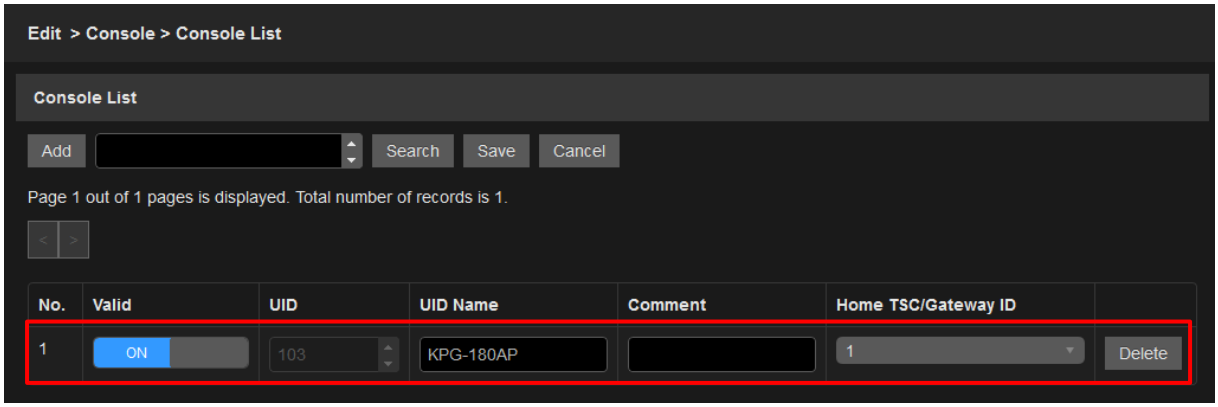
See 3.3.3.

3.5.4. Step4: External Servers w/ KA NMS

See 3.3.4.

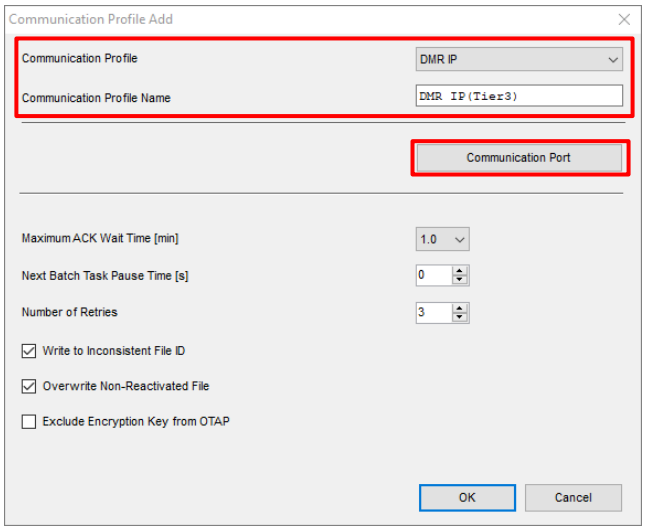
3.5.5. Step5: Console List w/ IP Gateway

Add KPG-180AP Console ID on Console List. Select TSC connected with IP Gateway.

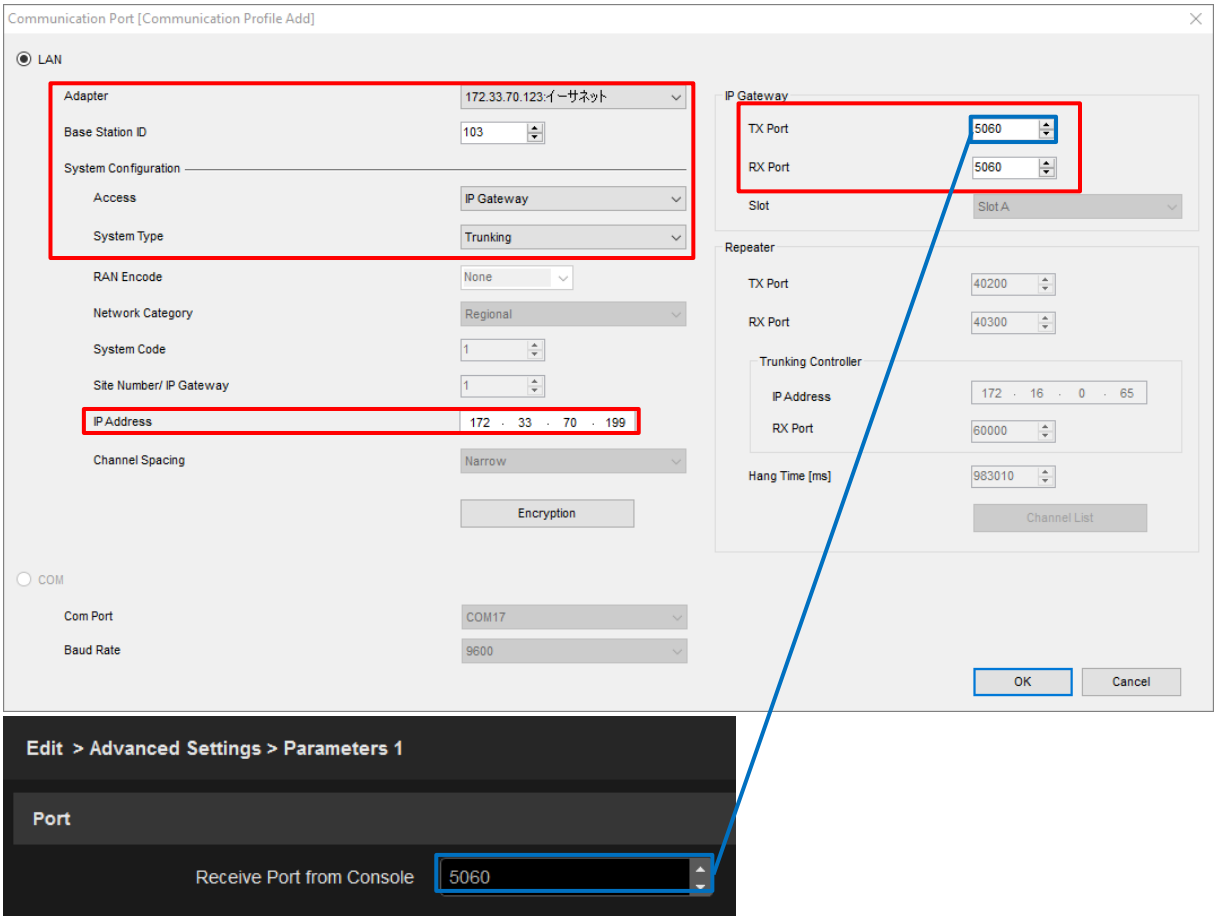


3.5.6. Step6: Communication Profile w/ KPG-180AP

Make Communication Profile to connect KPG-180AP to IP Gateway. Select DMR IP and set Communication Profile Name. Then, click on Communication Port.

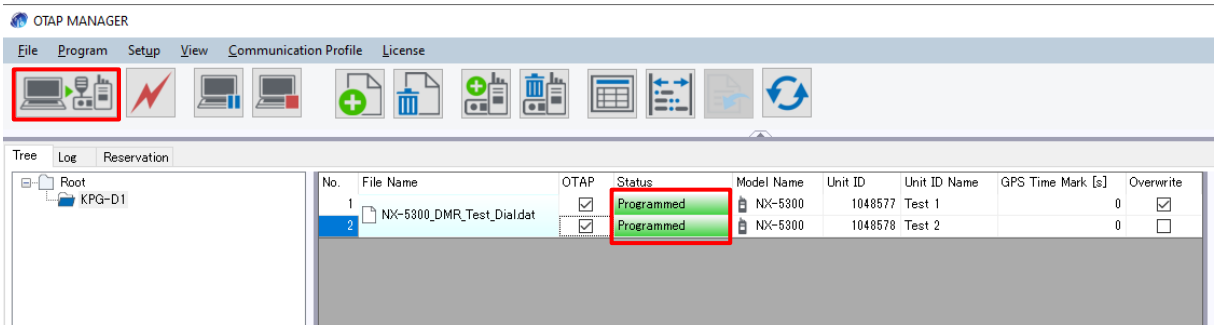


Select Network Adapter and set Base Station ID. The Base Station ID must be registered on the IP Gateway Console List.
Select IP Gateway and select Trunking for System Configuration.
Set IP Gateway IP Address.
Set TX Port and RX Port to communicate with IP Gateway. TX Port must be same as IP Gateway Receive Port from Console. When starting to communicate, KPG-180AP indicate own RX Port to IP Gateway, so IP Gateway does not need to program Transmit Port to Console.



Communication Test

Register Radio configuration file to KPG-180AP, then Execute OTAP.
If OTAP is succeeded, Status is changed to Programmed.



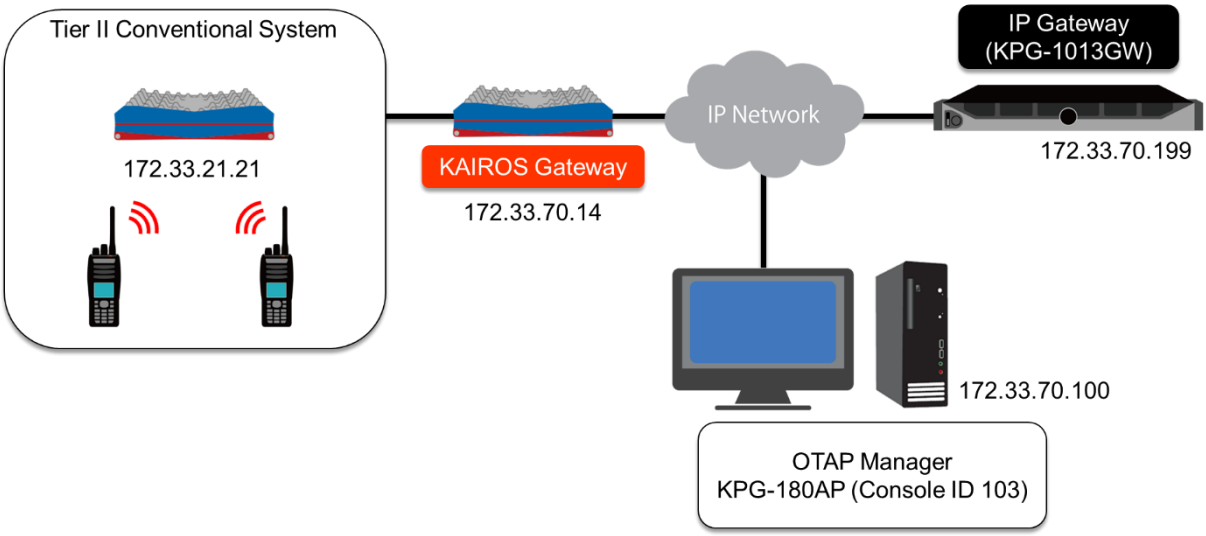
3.6. Basic Configurations w/ Tier II and KPG-180AP

This section describes how to set system configuration with IP Gateway, DMR Tier II Conventional System and KPG-180AP OTAP Manager. KPG-180AP is used Version 3.00. The following flow is for building the model case. Please refer “AN-19-0002 KAIROS Function Manual_rev110” how to configure DMR Tier II Conventional System.

Target

Write a configuration file from OTAP Manager to radio.

Model Case



Configuration Flow

How to configure IP Gateway and KAIROS repeater

Step1	Server Configurations w/ IP Gateway
▼	
Step2	TSC/Gateway List w/ IP Gateway
▼	
Step3	Repeater List w/ IP Gateway

How to configure IP Gateway and KPG-180AP

Step4	Console List w/ IP Gateway
▼	
Step5	Communication Profile w/ KPG-180AP

3.6.1. Step1: Server Configurations w/ IP Gateway

See 3.4.1.

3.6.2. Step2: TSC/Gateway List w/ IP Gateway

See 3.4.2.

3.6.3. Step3: Repeater List w/ IP Gateway

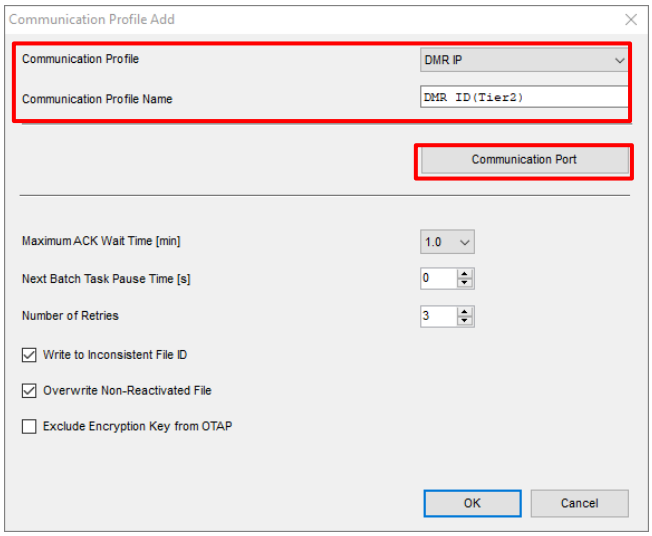
See 3.4.3.

3.6.4. Step4: Console List w/ IP Gateway

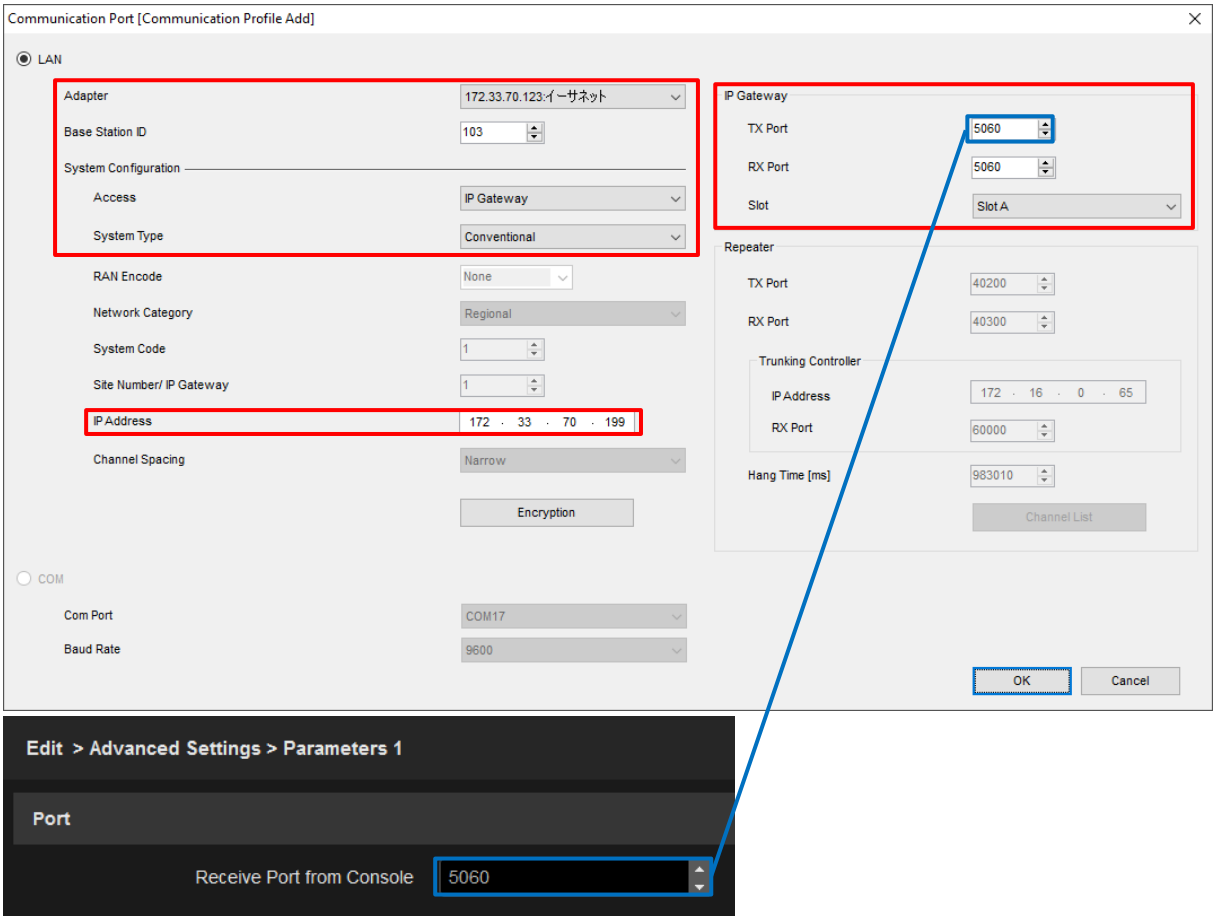
See 3.4.5.

3.6.5. Step5: Communication Profile w/ KPG-180AP

Make Communication Profile to connect KPG-180AP to IP Gateway. Select DMR IP and set Communication Profile Name. Then, click on Communication Port.

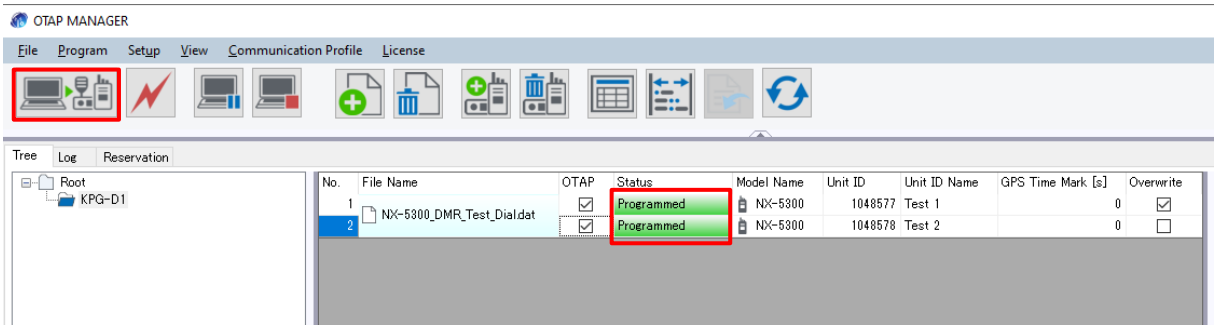


Select Network Adapter and set Base Station ID. The Base Station ID must be registered on the IP Gateway Console List.
Select IP Gateway and select Conventional for System Configuration.
Set IP Gateway IP Address.
Set TX Port and RX Port to communicate with IP Gateway. TX Port must be same as IP Gateway Receive Port from Console. When starting to communicate, KPG-180AP indicate own RX Port to IP Gateway, so IP Gateway does not need to program Transmit Port to Console.



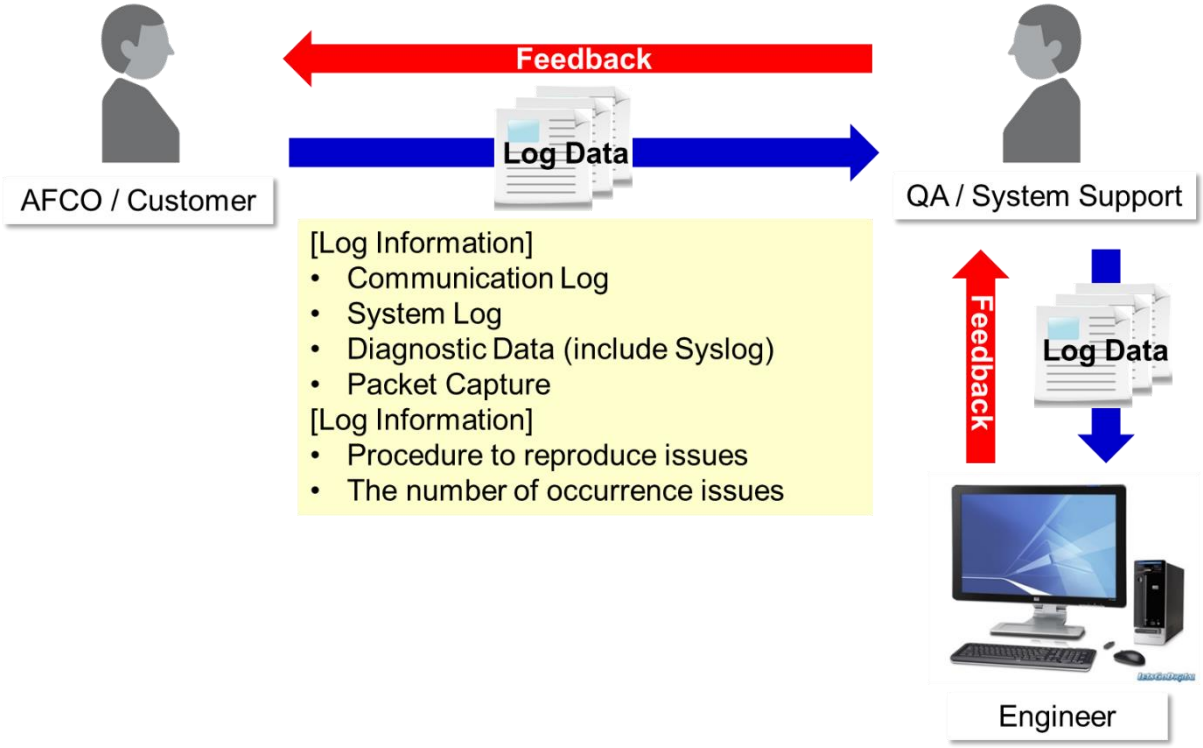
Communication Test

Register Radio configuration file to KPG-180AP, then Execute OTAP.
If OTAP is succeeded, Status is changed to Programmed.



4. Trouble Shooting

IP gateway has logging functions for trouble shooting. Communication log, System log and Diagnostic Data can be stored in IP gateway and downloaded at Maintenance menu. These log functions are always active. There is no configuration for storage. Moreover, Field Support function is available when a system operator does login as “admin” user. Packet Capture/Syslog can be downloaded at Field Support menu. Set of log information is very useful to look into a system issue by QA/Engineer. The Trouble Shooting flow is as follows.



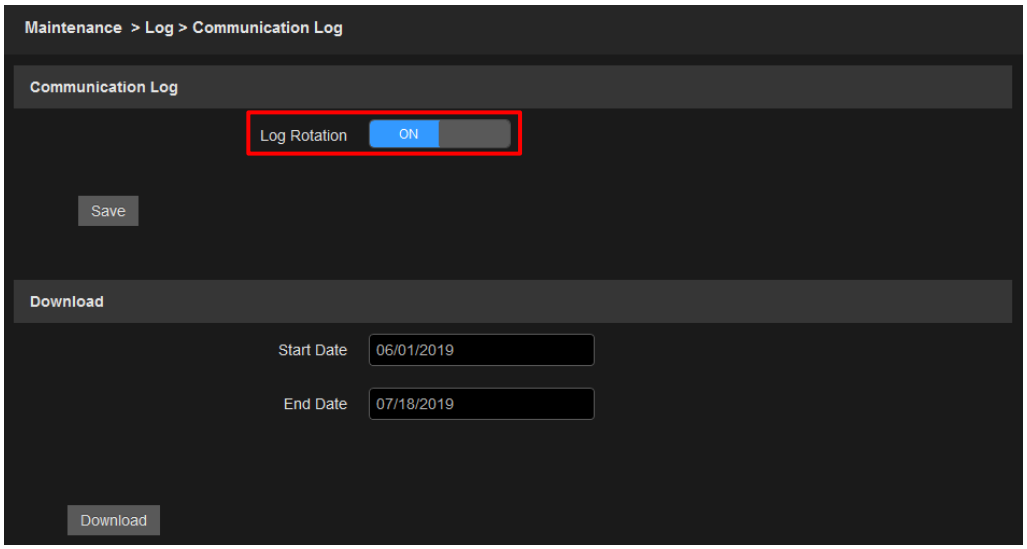
4.1. Log

Communication log, System log and Diagnostic Data can be stored in IP gateway. These log information are very useful to look into a system issue by QA/Engineer.

4.1.1. Communication Log

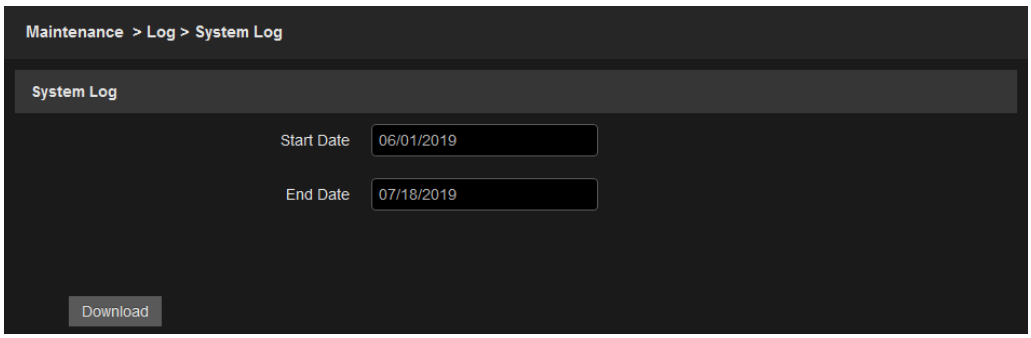
IP gateway can store a Communication Log used voice call and data communication with DMR System. The communication log is downloaded in the CSV format. The period of a log to be downloaded can be configured by set Start Date or End Date. The log of the configured period downloads by a click of the “Download” button. Log Rotation describes below.

[Log Rotation]
ON: The old logs are overwritten when the log storage area is more than 95%.
OFF: The new logs are deleted when the log storage area is more than 95%.



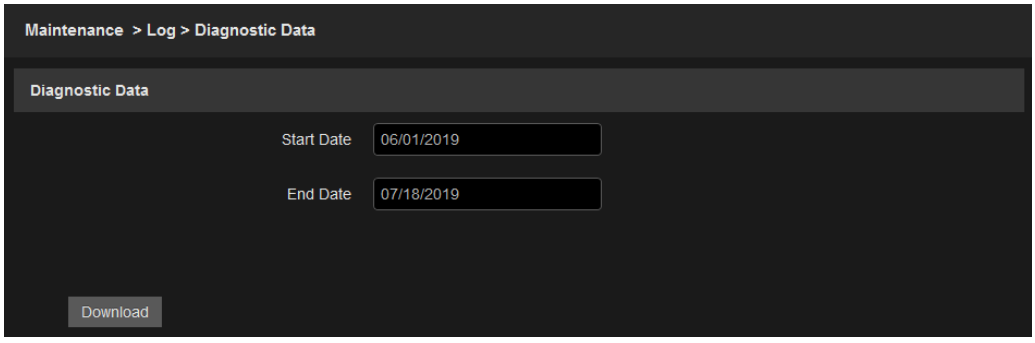
4.1.2. System Log

Acquiring the system log can be confirmed the system condition and user operation and find the cause of an unusual behavior by system's fault and wrong configuration. The System Log is downloaded in the CSV format. The period of a log to be downloaded can be configured by set Start Date or End Date. Number of storable system logs are 200000. The old logs are overwritten when the number of records exceeds 200000. System log is deleted by Factory Reset.



4.1.3. Diagnostic Data

Diagnostic Data includes internal information of system and used for issue investigation. Only HQ Engineer can confirm the Diagnostic Data. The user cannot open and analyze the data file. After download, the data must be shared with HQ engineer. The period of a log to be downloaded can be configured by set Start Date or End Date. Syslog is included in Diagnostic Data. The syslog is described in 4.2.2 Syslog.

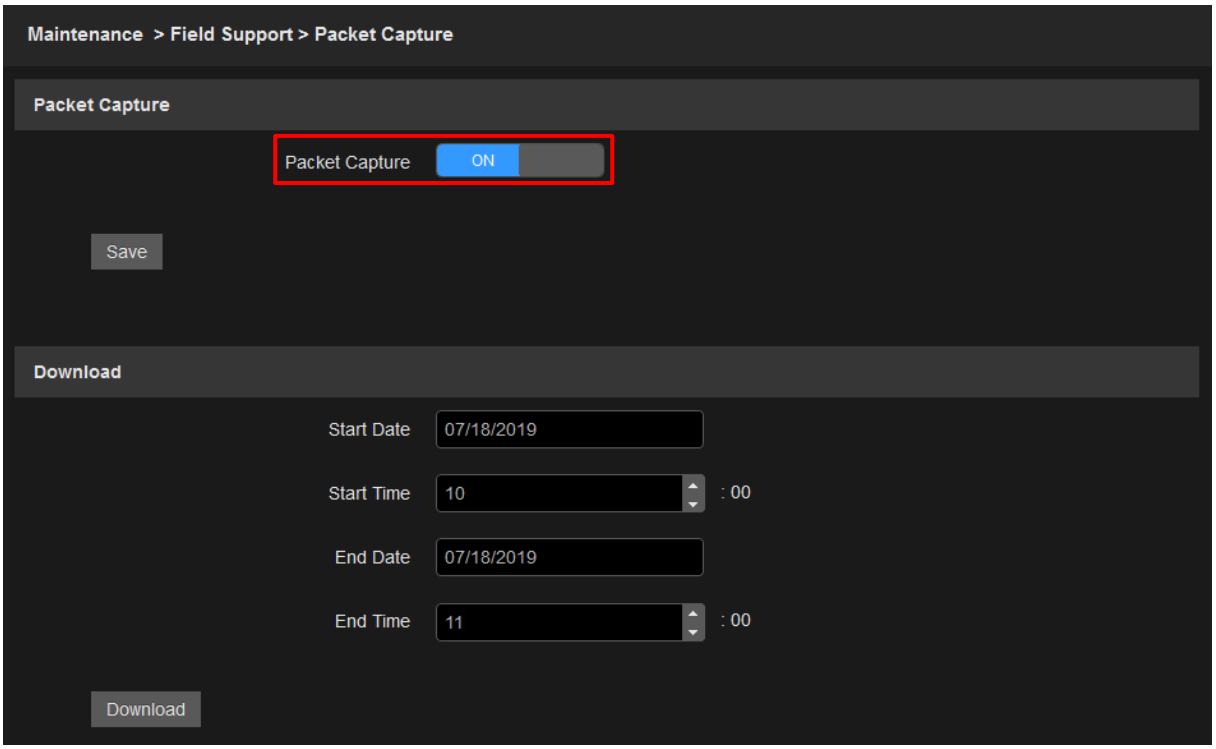


4.2. Field Support

Field Support feature is available when a system operator login as “admin” user. Packet Capture and Syslog can be downloaded by Field Support function.

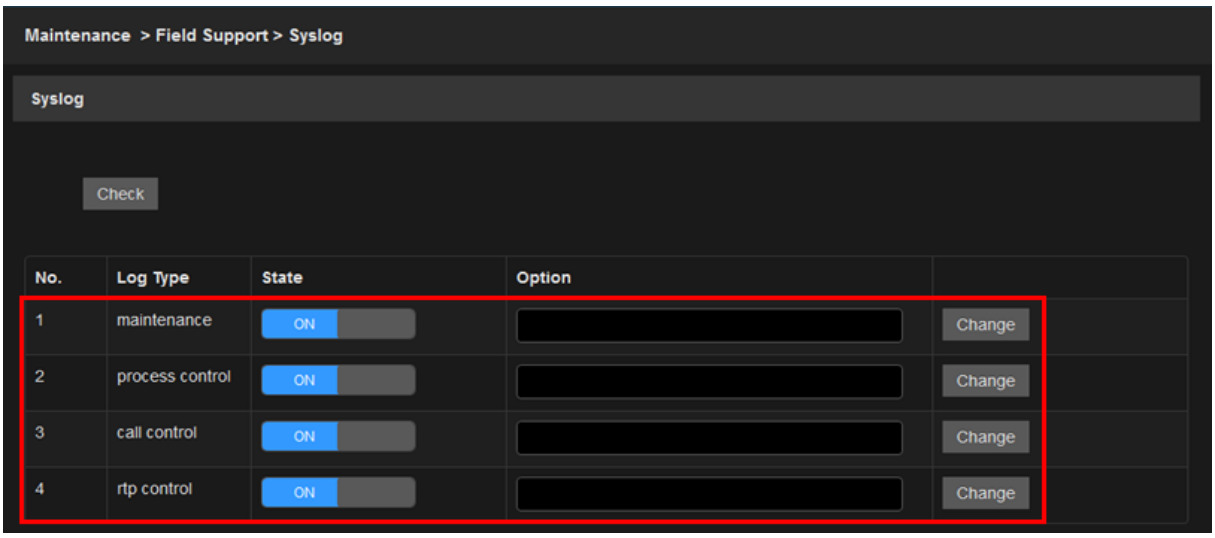
4.2.1. Packet Capture

Packet Capture is function to capture a packet data that IP Gateway sends/receives. By enabling Packet Capture function, it can be stored/downloaded the internal packet data of IP Gateway and among external devices. If IP Gateway is restarted/rebooted, Packet Capture function continues. Only HQ Engineer can confirm the Packet Capture. The user cannot open and analyze the data file. The period of a log to be downloaded can be configured by set Start Date/Time and End Date/Time.



4.2.2. Syslog

Syslog is function to output debug log file of IP Gateway. Syslog is included in Diagnostic Data. To output the log must be enabled the following functions. After click “Check”, select “Log Type” and input “Option”. “Log Type” means a type of internal process of the IP Gateway. Because “Option” is able to decide output level of the log, it’s used to output a detailed log information. “Log type” and “Option” configuration is specified by QA/Engineer. After QA/Engineer investigate a customer’s issue report, QA/Engineer announce to system operator the proper configuration for “Log type” and “Option”.



Note:

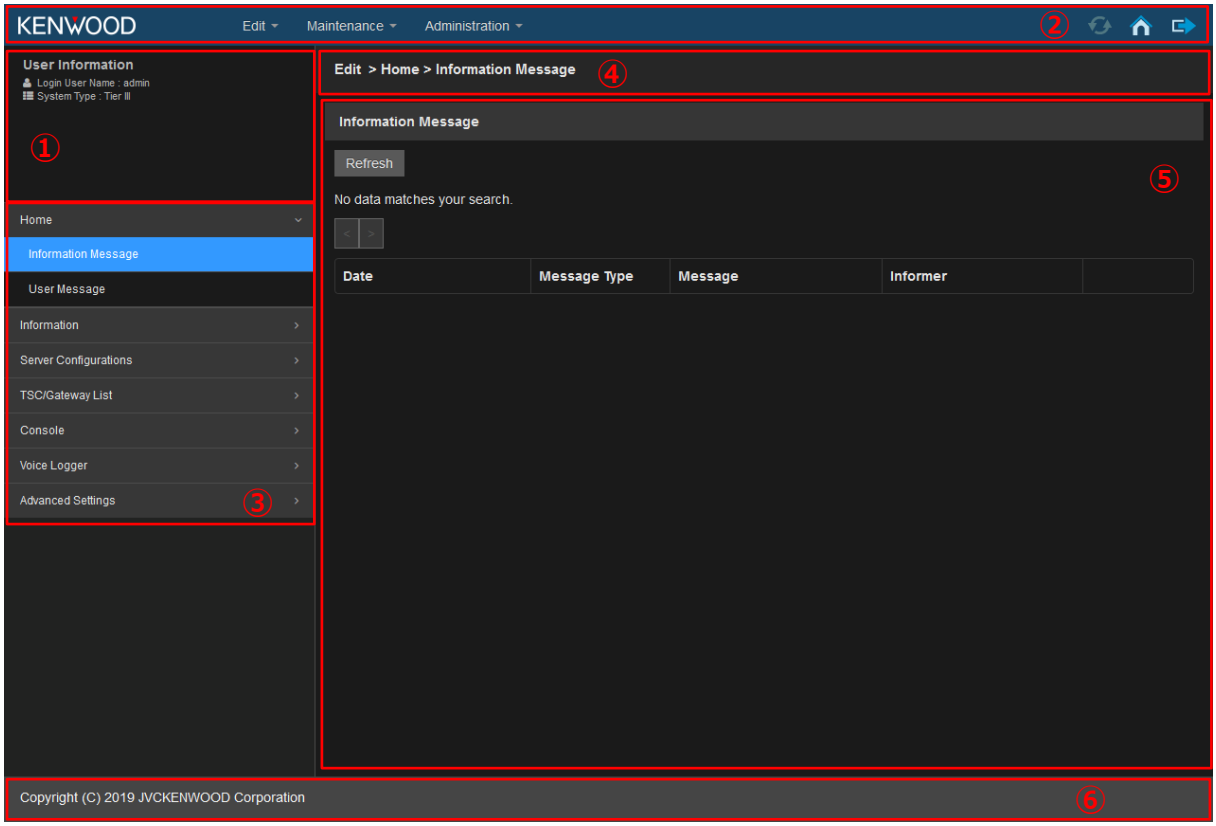
- The server PC performance for IP Gateway might be lower during enabling Syslog function because the PC consumes a system resource by activation Syslog function. It's not recommended to use this function other than issue investigation.

5. Appendix

Appendix describes basic functions for web interface.

5.1. Home

Main window is below.



No.	Name	Description
①	User Information Pane	The login information and the update information of each configuration screen are displayed.
②	Header	This field is displayed in common on every screen. Links to the main configuration screens, etc. are displayed.
③	Navigation pane	Links to detailed configuration screens related to the displayed screen are displayed.
④	Screen Hierarchy Pane	The hierarchy is displayed sequentially from the top screen to the currently displayed screen.
⑤	Configuration Pane	This field displays the configuration items of each screen.
⑥	Footer	This field is displayed in common on every screen. The copyrights appear.

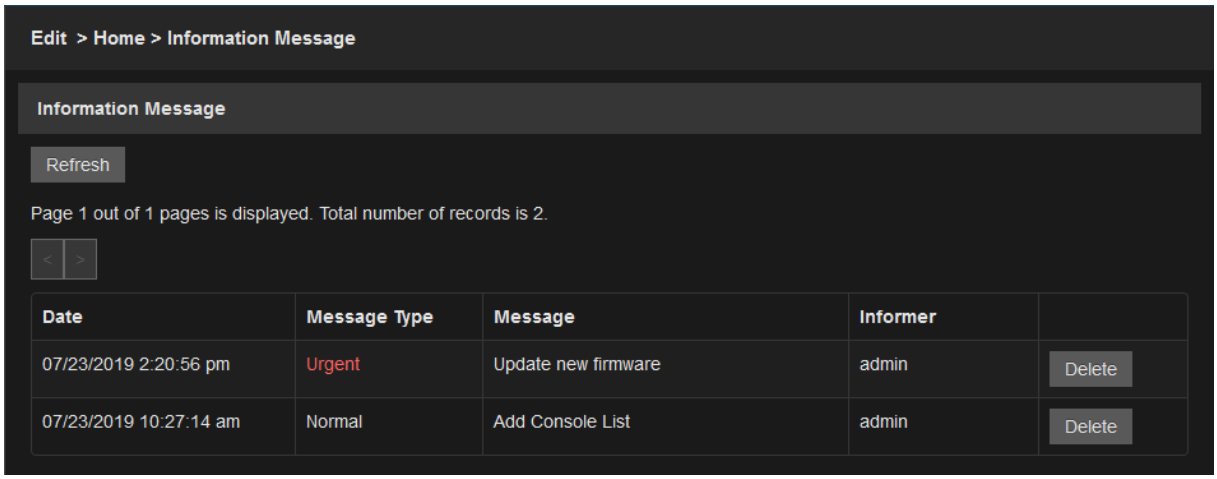
Note

In Header, there is “Update” button. Clicking the “Save” button on the configuration screen of the each menu saves the configuration data on web interface. If writing the configuration data to the IP Gateway, click the “Update” button.

5.1.1. Information Message

Information Message is function to share an information between users. The users can confirm modified configuration and notified information by using User Message function. The message is stored Max. 1000 messages. New message is displayed on top.

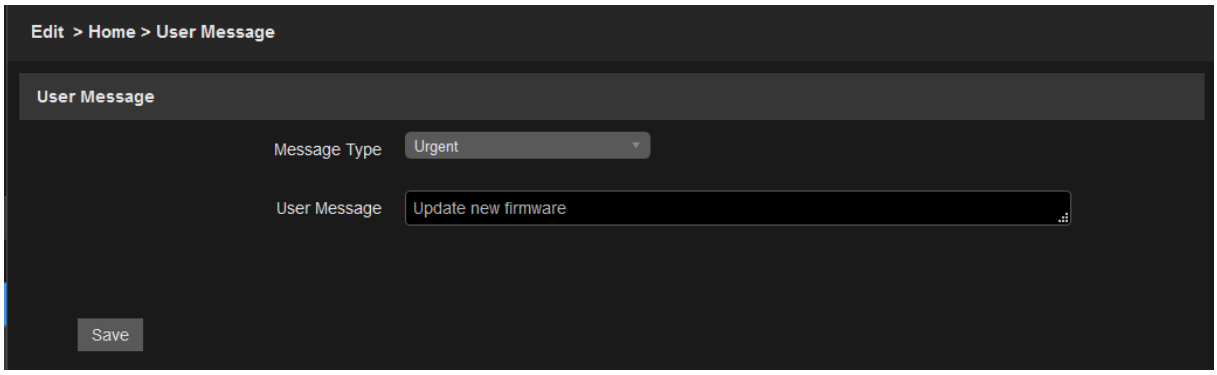
Edit > Home > Information Message



5.1.2. User Message

The users can type in modified configuration and notified information. Message Type can assign priority of the message. The message typed in is displayed on Information Message.

Edit > Home > User Message



5.2. System

System menu has Remote Control, Firmware Update, Backup & Restore, Factory reset, Import & Export and IP Configuration.

5.2.1. Remote Control

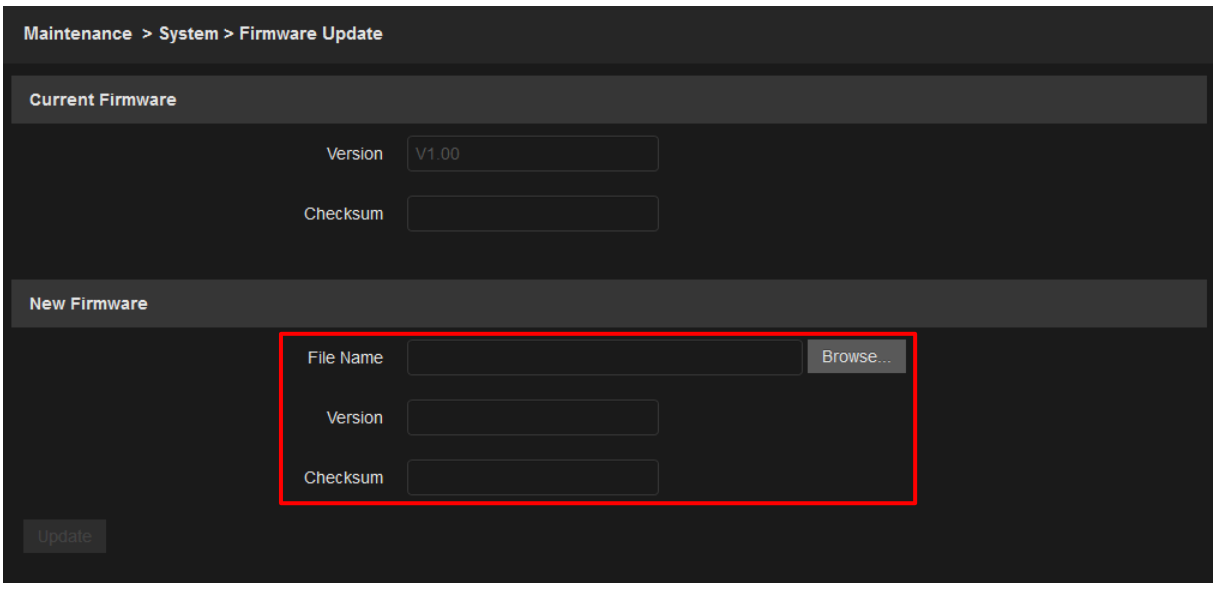
Press “Reboot” button to restart the IP Gateway. Rebooting the IP Gateway can restore it to the same state as when the IP Gateway is turned on. The IP Gateway cannot be used while rebooting.
Press “Restart” button to stop a behavior of the IP Gateway and then restarts the behavior. The behavior can be resumed in shorter time than Reboot. However, the status may not be improved depending on the status of the IP Gateway.

Maintenance > System > Remote Control

5.2.2. Firmware Update

Update firmware for IP Gateway in New Firmware.
Current Firmware displays the firmware version and checksum that has already written.

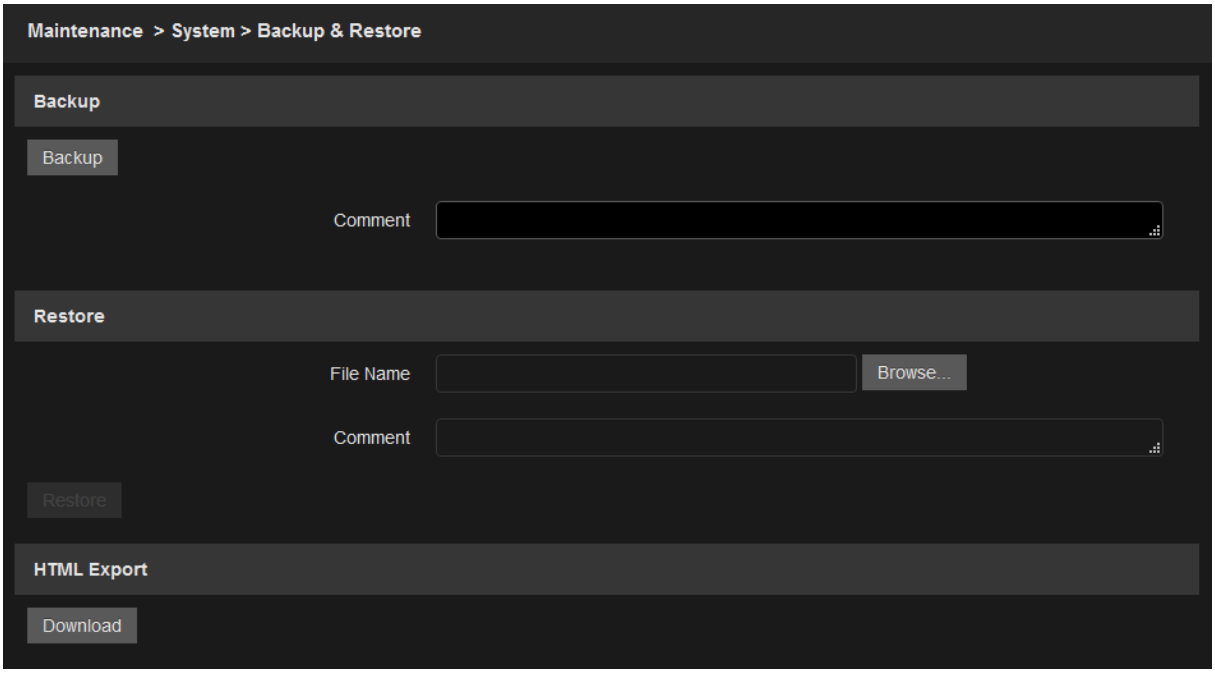
Maintenance > System > Firmware Update



5.2.3. Backup & Restore

Press “Backup” button to save the configuration data. By saving configuration data as a file, the data can be restored. Press “Restore” button to write the configuration data saved by backup to IP Gateway.

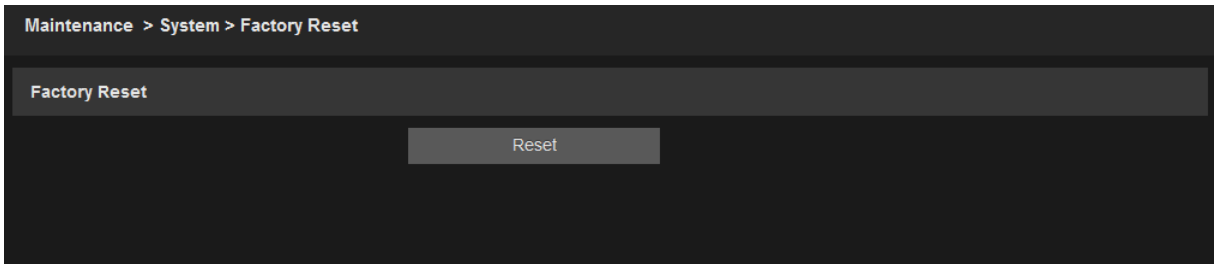
Maintenance > System > Backup & Restore



5.2.4. Factory Reset

Factory Reset is the function to reset the configurations of the IP Gateway to the initial state. By Factory Reset, communication log and system log that stored in IP Gateway are deleted. The activated license and IP Configuration never delete. The factory reset can be performed only by a user with Administrative privileges.

Maintenance > System > Factory Reset



5.2.5. Import & Export

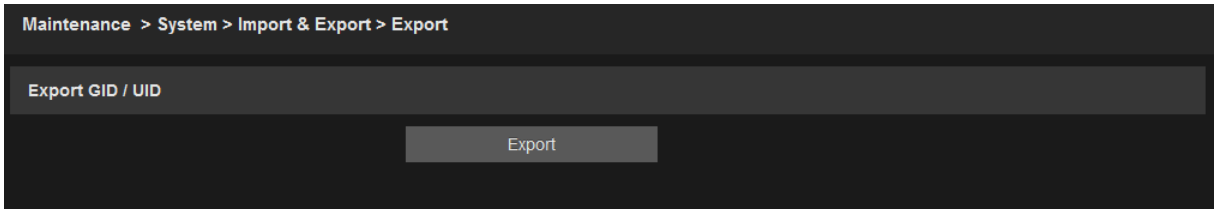
The data of UID List and GID List of console configured by web interface can be exported as a CSV file. Also, the exported CSV file can be imported to web interface. By editing the exported CSV file, the UID and GID of console can be added and deleted. By importing the CSV file to web interface after each data is changed, the configuration contents can be applied to web interface.

Export

The file name of an exported CSV file is “IPGW_id_export_yyyy-mm-dd.csv” for Export.
The information exported is below.

- System Type
- Console List (UID, UID Name, Valid, Comment, Home TSC/Gateway)
- GID List (GID, GID Name Valid)

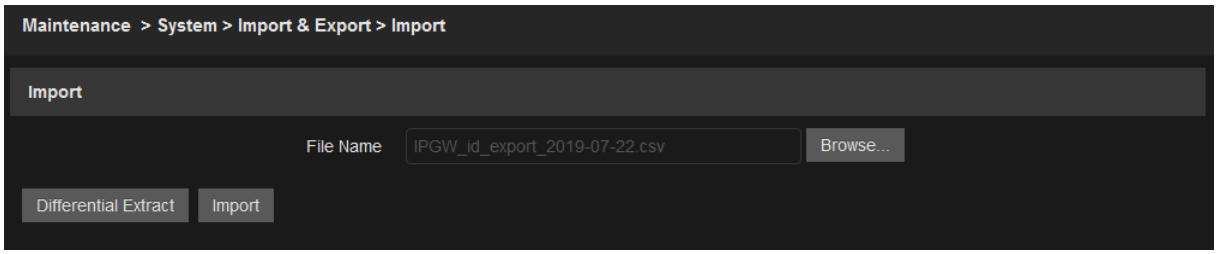
Maintenance > System > Import & Export > Export



Import

Clicking the “Browse” button to select the CSV file to import and then clicking the “Import” button executes import. Write the read data to an IP Gateway by clicking the “Update” button after importing completes. Up to 2,000 items can be imported at (the total number of addition, deletion, and changes) at one time.
By clicking the “Differential Extract” button after the “Browse” is clicked and the CSV file to import is selected, the configuration to be applied when importing is executed can be exported to the CSV file and confirmed. The function is very useful to confirm the importing results beforehand.
The file name of an exported CSV file is “DifferentialExtract_IPGW_id_export_yyyy-mm-dd.csv” for Export.

Maintenance > System > Import & Export > Import



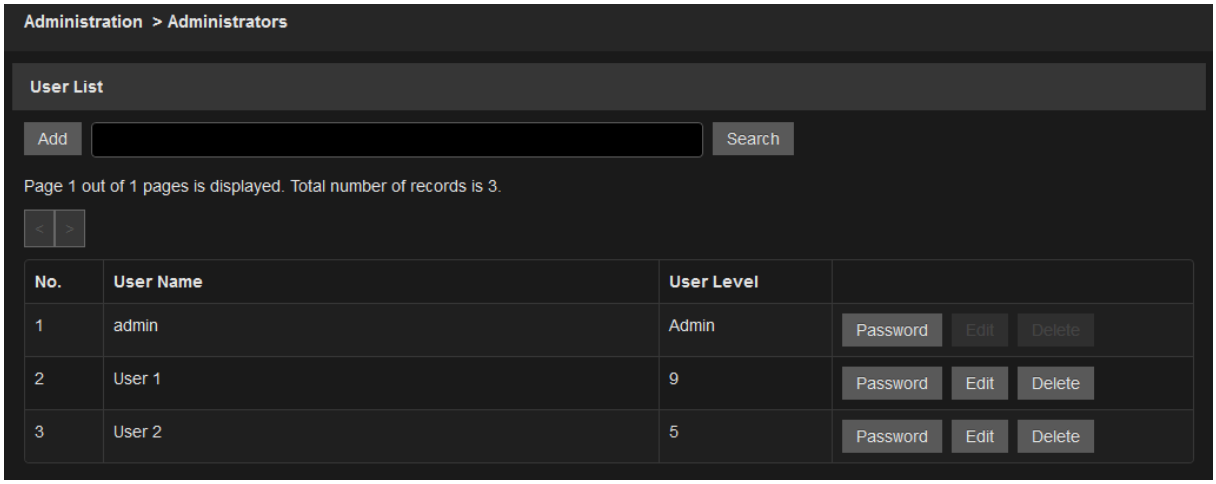
5.3. Administration

Using the web interface, the configuration of an IP Gateway and the administrative users to operate the system can be registered beforehand. Multiple administrative users can be registered and the function restrictions that can be operated on the web interface can be configured. Only permitted administrative users can configure and operate an IP Gateway.

5.3.1. Administrators

In User List, it is registered users to configure and operate IP Gateway using web interface. The password of the account can be entered or changed. The maximum number of registration account is 1000 users.

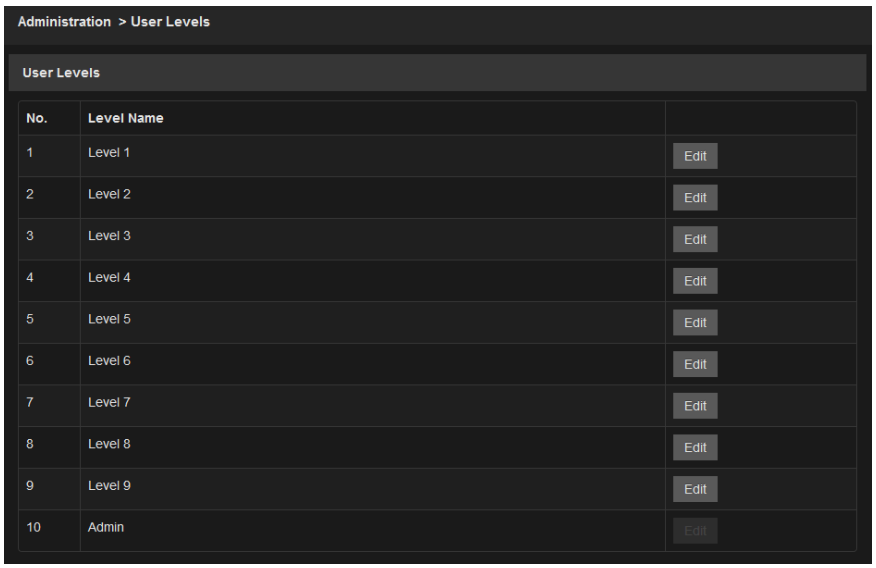
Administration > Administrators



5.3.2. User Levels

In User Levels, it is configured user privileges to configure and operate IP Gateway. User Level is nine steps and configured for each user. The privilege is configured in each function. The user level of admin never changes.

Administration > User Levels



The following table is the configuration of User Levels.

Item		Description
User Level	Level Name	Level Name allows a system administrator to configure the name of the user level. A maximum of 32 alphanumeric characters and symbols can be entered.
Access Permission (Edit)	Information	Configures the Information configuration privileges.
	Server Configurations	Configures the Server Configurations configuration privileges.
	TSC/ Gateway List	Configures the TSC/ Gateway List configuration privileges.
	Channel List	Configures the Channel List configuration privileges.
	Console List	Configures the Console List configuration privileges.
	GID List	Configures the GID List configuration privileges.
	Voice Logger List	Configures the Voice Logger List configuration privileges.
	Target GID	Configures the Target GID configuration privileges.
	Target UID	Configures the Target UID configuration privileges.
	Advanced Settings	Configures the Advanced Settings configuration privileges.
Access Permission (Maintenance)	Communication Log	Configures the Communication Log privileges.
	System Log	Configures the System Log privileges.
	Diagnostic Data	Configures the Diagnostic Data privileges.
	Remote Control	Configures the Remote Control privileges.
	Firmware Update	Configures the Firmware Update privileges.
	Backup	Configures the Backup privileges.
	Restore	Configures the Restore privileges.
	HTML Export	Configures the HTML Export privileges.
	Factory Reset	Configures the Factory Reset privileges.
	Time Settings	Configures the Time Settings privileges.
	Import	Configures the Import privileges.
	Export	Configures the Export privileges.
	IP Configuration	Configures the IP Configuration privileges.
	Formats	Configures the Formats privileges.
	Theme	Configures the Theme privileges.
	Packet Capture	Configures the Packet Capture privileges.
	Syslog	Configures the Syslog privileges.
Access Permission (Administration)	Administrators	Configures the Administrators privileges.
	User Levels	Configures the User Levels privileges.