Infodraw MRS Server Web Administration Interface

MRS Server is a TCP and UDP server that serves MRS device and monitor clients. Its most basic functionality and prime reason for its existence is to distribute video packets from cellular MRS client devices with limited bandwidth to a number of monitor clients observing the video stream. MRS Server under MS Windows OS takes form of a Windows Service. A Windows Service has no application-like user interface as does the MRS Monitor application, so it is instead configured using a Web Administration Interface. This document covers the web administration interface of MRS Server version 5.4.0.5.

The MRS Server responds to streams and packets coming in the following ports:
TCP: 12654
UDP: 12655
It is important to allow communication through these ports in the server machine's firewall. In Windows XP go to Windows Firewall settings, choose 'Advanced', select the network connection, click “Settings”, click “Add” and add TCP port 12654 (internal and external) if not already there, click “Add” and add UDP port 12655 (internal and external) if not already there.

The starting point for the web administration interface is the main menu page, reachable the following address (enter this address in your browser):
http://serverip:12654/admin
'serverip' is the IP address of the server. If the server is installed on the machine where the web browser is open, you may use 'localhost' as the address. If a secure connection is desired, use the following address:
https://serverip:12654/admin

Every time the server does not identify the browser as the administrator, it requests the user to enter the administrator's password. The initial password is mrs. The administrator is required to change this initial password to a different one.

Main Menu Page

The web administration interface (or WAI) contains the following configuration pages:

Title	Description
Login	Enter administrator password to allow administrator control.
Change Password	Change administrator password.
Server Authentication	Change how the server authenticates itself to the browser.
Files and Folders	Display the use of files and folders by the server.
Resource Limits	Control memory usage by the server.
Backup Settings	Allow to backup and restore the server's settings.

Internet Protocol	Display network information – use for debugging.
Logging: Latest Messages	Display the server's latest log messages – use for debugging.
Logging: Configure	Configure the server's logging parameters.
Logging: Latest Events	Displays the latest recorded events: connections and operations.
User/Device: Default Access	Configure default user and device's access to the server.
User/Device: Users	Control the users list.
User/Device: Devices	Control the devices list.
User/Device: Default Device Access	Control the default access permitted to devices.
User/Device: User Device Access	Control the access permitted to devices by specific users.
Clients: Management	Controls how the server manages clients.
Clients: Traffic Summary	Displays the incoming and outgoing data summary.
Clients: All Connections	Displays all connected clients.
Clients: Connected Devices	Lists the devices which are connected.
Clients: Connected Users	Lists the users which are connected.
Clients: User Device Calls	Lists the current calls made by users to devices.
Clients: File Uploads	Lists the files which are being uploaded from the server.
Clients: File Downloads	Lists the files which are being downloaded to the server.
Recordings: Configure	Configures the server's recording attributes.
Recordings: List	Lists the devices with video and audio channels that are recorded.
Recordings: Automatic device backups	Lists and configures automatic download of device recordings.
Software Updates: Configure	Configures the software updates folder path.
Software Updates: List	Lists the software update files for clients (devices only).
Software Updates: Upload	Enables uploading a software update file for clients (devices only).
User Area: Configure	Configures the user area folder path.
Sleep Management: Configure	Configures sleep states for devices that support sleeping for battery power conservation.
Licensing: List	Lists server software licenses and enables adding and removing licenses.

Login Page

Enter the correct administrator's password and click on “Login”. This will take you back to the main menu page.

Change Password Page

Type the current password where it says 'Old password', type a new password where it says 'New password', and retype the new password where it says 'Retype new password'. Then click on “Set”. This will take you back to the main menu page.

Server Authentication Page

Place an RSA certificate and private key for the server in order to have browsers connecting via SSL (HTTPS) authenticate the server successfully. The certificate must be digitally signed by a certificate authority known to the PC or browser.

Files And Folders Page

The “Data Folder” is the root folder where all other folders and files are used by the server.
The “Parameters File” contains all server parameters in XML format.
"Recordings” folder contains all server media recordings and device locations.
"Software Updates” folder contains all software update files to be sent to clients (devices only).

Resource Limits Page

The data that passes through the server is organized in packets, blocks of memory containing any data. Each packet contains about 1000 bytes of data and consumes roughly up to 1600 bytes of memory to compensate for differences between the data types. Open video streams and monitor connections using “Any” transport protocol all require storage of packets in memory. Use this page to control the number of allocated packets, take notice of the “Peak” to adjust the number after a while.

Backup Settings Page

This page will help you save the server parameters file someplace else for backup. Click where it says “Server Parameters” to display the XML parameters file. It is then possible to save it. Click on “Server Parameters (Compressed)” to download the parameters to a compressed file.

If necessary, upload the backup XML file using the “Browse” and “Upload” buttons. This action will restore back the settings to the ones when you just saved the XML file.

Network Information Page

This page lists the network interfaces and IP addresses which were discovered and are being used by the server.

Latest Log Messages Page

This page will let you view the server's latest log messages. It displays the time (and date), the message , and its parameters. Click on “Refresh” to refresh this page. Click on the “Main Menu” link to go back to the main menu page.

Logging Configuration Page

This page will let you change the logging parameters.
The maximal number of messages is the maximal number of messages to be kept in memory.
The minimal log severity is the minimal log severity to be displayed and kept in memory. Log messages less severe than this one will be ignored. Log severities are: Undefined, Status, Warning and Error.

Set Default User Device Access Page

This page will let you set how users and devices are permitted in the system when no other more specific rules apply. The default device access level decides what a user can do with a device if no other more specific rule was specified.

The following user/device access levels are defined as a relation between one user and one device:
Undefined: this level is not defined so it should not be used.
Forbidden: the user is not aware that the device is connected to the server and thus cannot do anything.
Searchable: the user may search a device, for Airself devices.
Aware: the user is aware that the device has connected to the server, but cannot do anything else.
Location Aware: the user is aware of the device's location, but cannot do anything else.
Passive: the user is aware that the device has connected to the server and may acquire media and location information from the device. For example: it can watch a video channel and play back a device recording.
Active: the user is aware of the device, may acquire passive data and may record on the device. It can also delete a device recording and manipulate switches and PTZ camera positions.
Advanced: the user may also change bitrate, frame-rate, sample-rate, etc.
Administrative: the user is aware of the device and can do anything with it, including device and channel renaming, setting time, packet size, enabling and disabling channels.

The “allow unlisted users” option, if checked, allows general access by any user not listed in the users list. This general access, however, is controlled by the default device access level. The “allow unlisted devices” option, if checked, allows general access to any device not listed in the devices list.

For secure server administration set the default device access level to “Forbidden”, uncheck the “allow unlisted users” and “allow unlisted devices” options. Then add users and devices and set user/device access levels in the relevant configuration pages.

Users Page

This page will list the users and allow adding users, deleting users and setting a user's password. Click “Add” to add a user to the list. In the “Edit User Details” page fill the user name and password, retype the new password and click “Apply”. Click on “Edit” to change a password of an existing user. Click on “Delete” to delete a user from the list.

Devices Page

This page will list the devices and allow adding devices, deleting devices and settings a device's password. Click “Add” to add a device to the list. In the “Edit Device Details” page fill the device ID and password, retype the new password and click “Apply”. The device ID is a positive number that uniquely identifies that device. A device ID is assigned to a device in the device configuration utility's “Device Identification” section. Click on “Edit” to change a password of an existing device. Click on “Delete” to delete a user from the list.

Default Device Access Page

This page will list the default device access permission to specific devices. Click “Add” to add a default device access directive to the list. In the “Set Default User Device Access” page select the device ID and default device access level. The device ID is selected from the devices list. You can read about device access level in page 4. Click on “Edit” to change the device ID or the access permission level for a certain entry in the list. Click on “Delete” to delete a specific entry from the list.

User Device Access Page

This page will list the specific device access levels certain users are permitted on certain devices. Click “Add” to add a user device access level directive. In the “Set User Device Access” page select the user, select the device ID and select the device access level. The user is selected from the users list. The device ID is selected from the devices list. You can read about device access level in page 4. Click on “Edit” to change the user, device ID or access permission level for a certain entry in the list. Click on “Delete” to delete a specific entry from the list.

Clients Management Page

This page will let you configure general settings with regards to connecting clients.
Check the “connect monitors with devices peer to peer” option to make monitor clients and device clients connect to each other directly, thus passing media such as video directly between them,

bypassing the server.

Traffic Summary Page

This page displays a summary of the general data that passes through the server. It gives information about the received data rate and the sent data rate for observing the server's currently consumed bandwidth. Click on the “Main Menu” link to return to the main menu.

All Connections Page

This page lists all connections to the server, including devices, users and browsers.

Connected Devices Page

This page lists the connected devices: their IP address as seen from the server, their numeric identifier, name and current data rate.

Connected Users Page

This page lists the connected users: their IP address as seen from the server, their name and current data rate.

User Device Calls Page

This page lists the calls made by users of the Airself Smartphone application to devices which are also AirSelf Smartphone Applications.

File Uploads Page

This page lists the active file uploads: downloading client's IP address as seen from the server, file path and progress information.

File Downloads Page

This page lists the active file downloads. These files are usually recordings being copied for backup purposes from capture devices to the server.

Recordings Configuration Page

This page lets you configure the server recording parameters.

Configuration Option	Description
Recordings Folder	The root path where server recordings are kept.
Downloads Folder	The root path where downloads to the server are kept.
File Size Limit	The maximal size of the media file.
Buffer Size	The size of buffer to be used between the network and the storage device for each recorded file.
Audio file format	Format of audio-only recorded file.
Video file format	Format of video-only recoded file.
Audio-Video file format	Format of combined video and audio recorded media file.
Automatic recording in motion detection	Automatically start a recording of the video channel where motion has been detected.
Delete old files to free space	Automatically delete old server recordings after the free space on the storage device drops below 10%.
Sign media files	Automatically generate a signature file for every recorded media file. A signature file contains an electronic signature that can be verified with the MRS AV Player application.
Use names in files	Generate media file names that contain the name of the device and recorded channel instead of their numbers.
Record device location	Automatically record all locations of devices on the server.
Record video on alarm	Automatically record a video channel which was associated with a general alarm, depending on the state of the alarm.
Record audio on alarm	Automatically record an audio channel which was associated with a general alarm, depending on the state of the alarm.
Record all media traffic	Automatically record on the server every channel being requested by any client.
Use separate device recording folder	Place files recorded from every device in the device specific recordings sub-tree.
Use separate device downloads folder	Place files downloaded from every device in the device specific downloads sub-tree.
Minimal event recording time	Set the extra time to be recorded after the event state which triggered the automatic recording turns back to idle.

Click on “Apply” to store modified settings, or “Main Menu” to return without making changes.

Recordings List Page

This page lists the active or scheduled recordings on the server. A recording is considered active if the

recorded capture device is connected to the server, or scheduled if the recorded capture device is disconnected from the server.

Automatic Device Backups Page

This page lists and enables adding and removing entries of devices to be automatically backed up in terms of media recordings. The following entry parameters determine the logic of actions to be taken by the server for backing up recordings from an online device:

Device	The device to be backed up.
Enable	Whether to enable (Yes) or disable (No) this entry.
Interface type	Limit the backup action for a specific network interface. For example: only backup files from a device if it connected to the server through its WiFi interface. In this case select “WiFi”.
Order	Download older files first or newer files first.

Software Updates Configuration Page

This page lets you configure the software updates parameters, particularly the software updates folder path.

Software Updates List Page

This page lists the update files to be sent to devices in order to upgrade their firmware. The software updates can generally be enabled or disabled. If enabled and a device connects to the server and there is a newer version of its firmware listed, then the server will send the relevant update to the device client, the device will upgrade itself, restart, and reconnect to the server with the updated version. Click “Enable” to enable software updates, “Disable” to disable them, “Main Menu” to return to the main menu, or “Upload” to upload a new software update file to the server.

Upload Software File Page

Use this page to upload a new software update file to the server. The types of supported files are:

File Type	Description
pmrs-A_B_C_D.tgz	MRS-100 (PMRS) device firmware
pmrs-101-A_B_C_D.tgz	MRS-101 (PMRS) device firmware
pmrs-102-A_B_C_D.tgz	MRS-102 (PMRS) device firmware
pmrs-202-A_B_C_D.tgz	MRS-201 (PMRS) device firmware
pmrs-103-A_B_C_D.tgz	MRS-103 (DOH) device firmware

pmrs-104-A_B_C_D.tgz	MRS-104 (PMRS) device firmware
pmrs-110-A_B_C_D.tgz	MRS-110 (PMRS) device firmware
pmrs-410-A_B_C_D.tgz	MRS-410 (PMRS) device firmware
MRS_BlackfinDeviceSystem.ldr	MRS-400 device firmware
Setup_MRS_Service.msi	Windows Service Software (self upgrade)

Click “Browse” to select the file on your local PC. Click “Upload” to start uploading the file to the server.

User Area Configuration Page

This page lets you configure where to place the root folder for user specific data files. User specific data files include device icons and exports of recordings that users created in the user area website of the server.

Sleep Management Configuration Page

PMRS-101, PMRS-102, PMRS-201, PMRS-410 and PMRS-110 devices versions 4.5.0.0 and above can be turned off (sleeping mode) to be woken up automatically when some programmable time arrives. While the device is off, it consumes a small amount of energy, around 30 micro-amperes. After the device is turned on automatically, it can also be turned off remotely (by an MRS Server). If the device is equipped with an additional specific electronic circuit, it can also be turned on by connecting a given special wire to the ground, or to a 12v input. It may be woken up also by an interrupt from an accelerometer or from a passive infrared sensor (PIR). The state of being turned on not by the ON/OFF switch and not by the internal timer is called “port wake-up”.

In order to send the device back to sleep after an automatic wake-up, the device must be configured to connect to the MRS Server. The server commands the device to go to sleep according to the specific device configuration in this page. If the device has no special configuration in this page, it will not be sent to sleep.

Click the “Add Device” to add a device that supports sleeping to the sleep control table. Alternately select a device already defined in the sleep control table for additional modifications. Three sleeping states are supported:

- Normal operation. This is the state in which the device is not required to sleep and has similar behavior to a device which is not listed in the sleep control table.
- Wake up every certain constant time frame. This is the state in which the device goes to sleep, to be woken up every certain defined time. Once woken up, the device connects to the server for an updated sleeping instruction if any.
- Wake up at a certain time. This is a temporary sleeping state until the defined time arrives.
- Indefinite sleep. Use this state for waking up by an external trigger only, not by a timer. The

device will go back to sleep according to the “limit port wakeup” setting, after all event states are idle.

The “validate wakeup within X minutes” option triggers an event in the server and in the monitors connected to the server if a device scheduled to wake up by a timer did not wake up within the input time. Configure the notifications of this event in the MRS Monitor under My Monitor->”Device Connection Status Indications” with Event Type:Device Oversleep.

The “Limit port wake-up” option deals with devices which were woken up by a port trigger: 12v, acceleration, infrared sensing, etc. Check this option to send the device back to sleep after the trigger events are idle, more accurately - when the contact alarms are all non-active. This option lets one configure a specific delay before sleeping. It can be set to zero for an immediate shutdown.

It is important to note that the PMRS device must be powered off using the power switch in order to be able to wake up automatically, either by a programmed time or by an input port. By default, the device is not programmed to come up automatically, so it can only be connected to the server when the power switch is on. After applying the first sleeping command on the server, wait for the device's lights to stop blinking and gently move the power switch to off, to allow it to wake up.

PMRS-110/201/410 devices can also be woken up by motion using a built-in acceleration sensor. Use the MRS Monitor Application to configure this sensor by double-clicking the “Accelerometer” tree item under the relevant device item in the online devices sub-tree. A browser will open with a configuration page. Choose an axis, threshold and check the “Run Accelerometer” box. Then click “Submit”. When the device moves beyond the threshold it will indicate the movement as the last dry contact input, and if the device is OFF, it will wake up and indicate “Sensor Wake-up” as a tree item under the online device item.

Licenses List Page

This page lists the server's licenses and indicates the number of allowed devices. A server without a license supports up to five concurrent devices. The license depends on the hard disk volume serial number as displayed in this page. To request a new license from Infodraw, click on “Request License” to send a license request by mail to info@infodraw.com indicating the type of license (server license) and number of devices required. Copy the license text from your mail client and paste in in the text area instead of “Enter license here”. Click on “Add License” to add the new license. Click on “Delete” to remove an old or non-relevant license.

Support

For any kind of support, please send email to info@infodraw.com or call our office at +972-3-6127434.