



Universal Hub User's Manual MA-2080-B

Functional meets simple

The Next Generation IoT and Telemetry Solution has arrived.
With a future-proof, expansion ready design, functional truly meets simple.

TABLE OF CONTENTS

DISCLAIMERS	4
RF EXPOSURE AND ELECTRICAL SAFETY	5
CONTACT INFORMATION	10
REVISION HISTORY	11
PRODUCT OVERVIEW.....	12
DEVICE INSTALLATION.....	15
Device Mounting	15
SIM Card	15
Antennas	16
Ethernet Interface	17
Serial Interface	17
Digital I/Os	17
Power Interface	18
LED Indication	20
Reset Button	21
DEVICE MANAGEMENT	22
DEVICE STATUS	24
Overview	24
Device.....	25
Connections.....	26
VPN & Tunnels.....	27
Service	28
I/O & Analogue.....	30
BASIC CONFIGURATIONS	31
WAN Interface.....	31
Cellular.....	33
Ethernet	37
Serial Interface	41
GNSS	45
SMS/Email	52
Contacts.....	56

Digital I/O.....	58
LED Display Control.....	63
ADVANCED NETWORKING.....	64
Dynamic DNS	64
Cloud Service.....	65
IP Routing.....	67
NAT.....	69
DMZ	70
Port Forwarding	71
Security	72
VPN & Tunnelling	78
X.509.....	99
VRRP.....	101
SNMP	102
DEVICE MANAGEMENT	103
System.....	103
Backup / Profiles.....	106
Clock.....	108
Ping Tool.....	109
System Logs	110
Firmware Upgrade	113
REBOOT / LOGOUT	114
SMS COMMANDS	115
DEVICE AT COMMAND SET	120

DISCLAIMERS

All data and information contained in or disclosed by this document are confidential and proprietary information of RF Industries, and all rights therein are expressly reserved. By accepting this material, the recipient agrees that this material and the information contained therein are held in confidence and in trust and will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of RF Industries. The information provided in this document is provided on an "as is" basis.

In no event will RF Industries be liable for any damages arising directly or indirectly from any use of information contained in this document. Information in this document is subjected to change without any notice.

Life support – This product is not designed for use in life support appliances or systems where malfunction of these products can reasonably be expected to result in personal injury.

RF Industries' customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify RF Industries for any damages resulting from such application.

Right to make change - RF Industries reserves the right to make changes, without notice, in the products, including circuits and software, described or contained herein in order to improve design and/or performance.

Some features outlined in this manual may require an updated firmware and/or GUI to work. Please contact RF Industries for more information.

RF EXPOSURE AND ELECTRICAL SAFETY

The use of this modem in any other type of host configuration that may not comply with the RF exposure requirements should be avoided. During operation, a minimum of 20 cm (8 inches) should be maintained between the antenna, whether extended or retracted, and the user's/bystander's body (excluding hands, wrists, feet, and ankles) to ensure RF exposure compliance in accordance with ARPANSA guidelines. The modem is not designed, nor intended, for use in applications within 20 cm (8 inches) of the body of the user. Continued operational compliance of the modem relies upon it being used with an AS/NZS 60950.1 approved SELV power supply.

Cautions

This modem has been tested and found to comply with the limits pursuant to relevant ACMA Standards. These limits are designed to provide reasonable protection against harmful interference in an appropriate installation. This modem generates, uses, and can radiate radio frequency energy and, if not used in accordance with instructions, can cause detrimental interference to other radio communication networks and devices. Use only the supplied or approved antenna. Unauthorized antennas, modifications, or attachments could impair performance, damage the modem, or result in violation of RF exposure regulations.

There is no guarantee that electromagnetic interference will not occur in a particular installation. If the modem does cause detrimental interference in radio and television reception, which can be verified by turning the modem on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving radio or TV antenna
- Increase the separation between the modem and thereceiver
- Contact RF Industries Maxon Technical Support for assistance.

Changes or modifications to the modem that are implemented without the express consent of RF Industries Pty. Ltd. void the product warranty and terminate the user's authority to use the modem.

General Safety

RF Interference Issues: Avoid possible radio frequency (RF) interference by carefully following safety guidelines below:

- Switch OFF the modem when in an aircraft. The use of cellular devices in an aircraft is illegal. It may endanger the operation of the aircraft and/or disrupt the cellular network. Failure to observe this instruction may lead to suspension or denial of cellular services to the offender, legal action, or both.
- Switch OFF the modem in the vicinity of gasoline or diesel fuel pumps or before filling a vehicle with fuel.
- Switch OFF the modem in hospitals and any other places where medical equipment may be in use.
- Respect restrictions on the use of radio equipment in fuel depots, chemical plants, or in areas of blasting operations.
- There may be hazards associated with the operation of your modem in the vicinity of inadequately protected personal medical devices such as hearing aids and pacemakers. Please consult the manufacturers of the medical device to determine if it is adequately protected.
- Operation of the modem in the vicinity of other electronic equipment may cause interference to the equipment if it is inadequately protected. Observe any warning signs and manufacturers' recommendations.
- The modem contains sensitive electronic circuitry. Do not expose the modem to any liquids, high temperatures or shock. The modem is not waterproof. Please keep it dry and store it in a cool, dry place.
- Only use original accessories or accessories that are authorized by the manufacturer. Using unauthorized accessories may affect your modem's performance, damage your modem and violate related national regulations.
- Always handle the modem with care. There are no user serviceable parts inside the modem. Unauthorized dismantling or repair of the modem will void the warranty.

NOTE:



- * The product needs to be supplied by a limited power source or the power supply provided. Otherwise, safety will not be ensured.
- * Do not affix the modem in an open area where it is liable to lightning-strike hazard.

Vehicle Safety

- Do not use the modem whilst driving.
- Respect national regulations on the use of cellular devices in vehicles. Road safety always comes first.
- If incorrectly installed in a vehicle, the operation of the modem could interfere with the correct functioning of vehicle electronics. To avoid such problems, ensure that the installation has been carried out by qualified personnel.
- Verification of the protection and interference-free performance of vehicle electronics should be a part of the installation procedure

Potentially Unsafe Areas

Posted Facilities: Turn off the modem in any facility or area when posted notices require you to do so.

Blasting Areas: Turn off the modem where blasting is in progress. Observe restrictions and follow any regulations or rules.

Potentially Explosive Atmospheres: Turn off the modem when you are in any area with a potentially explosive atmosphere. Obey all signs and instructions. Sparks in such areas could cause an explosion or fire, resulting in bodily injury or death.

Areas with a potentially explosive atmosphere are often but not always clearly marked. They

include:

- Fuelling areas such as gas or petrol stations
- Below deck on boats
- Transfer or storage facilities for fuel or chemicals
- Vehicles using liquefied petroleum gas, such as propane or butane
- Areas when the air contains chemicals or particles such as grain, dust or metal powders
- Any other area where you would normally be advised to turn off machinery of any kind

Concentrated Electromagnetic Activity: Avoid using the modem within areas of high electromagnetic wave activity or within enclosed metallic structures e.g. lifts.

CONTACT INFORMATION

In keeping with RF Industries' dedicated customer support policy, we encourage you to contact us.

TECHNICAL:

Hours of Operation: Monday to Friday 8.30am to 5.00pm*

Telephone: +61 2 8814 2300

Facsimile: +61 2 9630 0844

Email: iot.support@rfi.com.au / support@maxon.com.au * Public holidays excluded

SALES:

Hours of Operation: Monday to Friday 8.30am to 5.00pm*

Telephone: +61 2 8814 2300

Facsimile: +61 2 9630 0844

Email: orders@rfi.com.au * Public holidays excluded

WEBSITE: www.rfi.com.au

ADDRESS:

RF Industries Pty Ltd
99 Station Road
Seven Hills NSW 2147
Australia

POSTAL ADDRESS:

RF Industries Pty Ltd
Locked Bag 2007
Seven Hills NSW 1730
Australia

REVISION HISTORY

– Product Information

Product	Universal Hub Cellular Ethernet Modem Router
Model	MA-2080-B
Document Type	PDF
Current Revision	0.3
Status of the Document	Preliminary Release
Revision Date	May 2020
Total Number of Pages	128

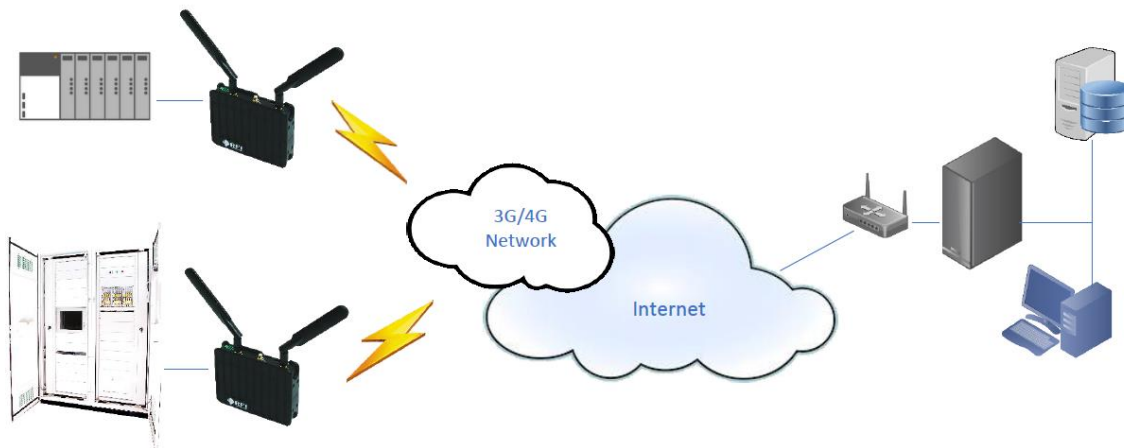
– Revision History

Level	Date	History
0.1	September 2019	Preliminary Release
0.2	November 2019	Added more information for digital I/Os Added AT Command Set, Ethernet Link Speed Options, SNMP MIB file, and updated Security Settings
0.3	May 2020	Added FTP Client, Radius Client, and Syslog FTP upload functions. Added newly supported AT commands for ClearSCADA. Added onboard measurements in features list. Updated descriptions for improved functions.

PRODUCT OVERVIEW

The RFI Universal Hub is a unique and intelligent fusion of 4G capabilities with advanced functionality of a modem/router, all encased in a durable & robust metal casing.

The Universal Hub Base Model features dual-SIM capabilities and wired WAN, providing advanced redundancy functionality. The LTE-Advanced connectivity with dual MIMO antennas means you can now have faster internet connections, and an array of connectivity options including RS232/RS485, 2 x Ethernet Ports and 4 x Digital IO's make the device a rugged cellular modem/router suitable for a diverse range of industrial networking and M2M applications.



Features and Benefits

- **Designed for Industrial Applications**
 - Powerful industrial grade ARM Cortex A8 processor and LTE-A cellular module
 - Industrial grade GNSS receiver
 - Industrial grade metal/plastic housing
 - Gigabit Ethernet ports with 1.5KV magnetic isolation protection
 - RS232/RS485/RS422 Interface 15KV ESD protection

- Dual SIM support with 15KV ESD protection
- Galvanic Isolated Digital IO ports
- On board input voltage and temperature monitoring
- 9~48VDC input voltage range with reverse-polarity and overvoltage protection

– **High-Performance and Function-Rich**

- FDD-LTE CAT6 LTE-Advanced cellular connectivity
- Up to 300 Mbps Downlink & 50 Mbps Uplink
- Supports 3G fallback with 6 Bands DC-HSPA+ CAT24
- Supports multiple WAN access methods, including Dual SIM backup and wired WAN interface (PPPOE, ADSL)
- SIM backup policies provide flexible data connection failover management
- GNSS function with GPS/GLONASS support
- Onboard input voltage and temperature measurements by built-in 12bit ADC
- Multiple VPN and tunnel protocols including PPTP, L2TP, IPSEC, OPENVPN and GRE
- Up to six(6) simultaneous VPN/Tunnel instances (Server/Client)
- Supported network protocols include PPPoE, TCP, UDP, DHCP, ICMP, NAT, Port Forwarding, DMZ, HTTP, HTTPS, FTP, SFTP, DNS, SNTP, TELNET, SSH, Static Routing, OSPF, VRRP, SNMPv3, QoS*, IGMPv3.0*
- Supports multiple DDNS services including Dyn, No-IP, Dynu, MS-DNS, as well as custom-defined.
- Comprehensive security features including firewall, anti-DDOS, SFTP, SSL/TLS secured socket connection and syslogs, and geo-fence, etc.
- Remote SMS commands and device status reporting
- Web-based user interface for local/remote device management
- System real time clock with SNTP support
- Local and over-the-air firmware upgrade

Device Interfaces

- 2x Mini USIM Card Slots
- 2x 10/100/1000Mbit RJ45 Ethernet Ports
- 1x RS232/RS485/RS422 Serial Interface over DB9F
- 2x Digital Inputs, 2x Digital Outputs

Display

- 6x Green LEDs: PWR, SIM, SIG, DAT, USR, and T/R



Package Contents

Standard Package:

Item	Quantity	Remark
Router MA-2080-B	1	
Cellular antenna	2	
Ethernet cable	1	
DB9 Serial cable	1	
3-way terminal block plug	1	
6-way Terminal Block Plug	1	
DIN rail clip	1	

Optional Accessories:

12VDC plugpack terminated with 3-way terminal block plug

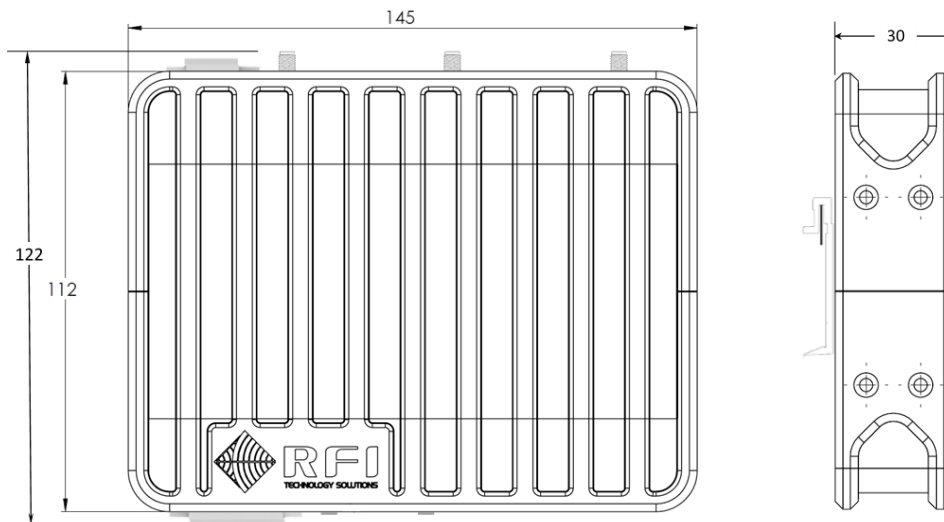
GNSS antenna

Optional Mounting Accessories

DEVICE INSTALLATION

IMPORTANT You should check the router configuration immediately after installation to ensure all settings are as desired. Failure to do so may result in unauthorized access to your equipment.

Device Mounting



Units: mm. with DIN Rail mounting option.

IMPORTANT The maximum clearance between device casing exterior to internal parts is 5mm. Please use proper length screws, e.g. M3x5, to attach the mounting accessories (DIN Rail Clip or Wall Mounting Plate) to avoid damaging the electronics inside.

SIM Card

Make sure the router is powered off the router. Holding the SIM card in the correct orientation based on the SIM slot to use (**Important!**) and carefully insert the card into desired SIM card slot.



SIM Card Slots

Antennas

Cellular Antennas

Attach the cellular antenna(s) with SMA male connector to the antenna connectors on the router, which are located at each side of the router housing.

The connector labelled “ANT” is the main antenna interface and must be connected properly for the router to operate over cellular network. For MIMO and Carrier Aggregation function, the “DRX” antenna must be used.



Antenna Connectors

GNSS Antenna

Attach the GNSS antenna with SMA male connector to the antenna connector on the router, which is located between the two cellular antenna connectors and labelled with “GNSS”.

Please avoid using excessive force when mounting the antennas as this may result in unnecessary damage to the housing that holds the antenna connectors.

Ethernet Interface

Connection of Ethernet interface is simple and straight forward. A minimum of CAT5E cable is required to achieve gigabit speed. A lit green LED on up-right corner of the each port indicates an active gigabit LAN connection, otherwise, the connection will be 10/100Mbps.

Serial Interface

RS-232

When configured as an RS-232 interface, the device follows the EIA/TIA definition as a DCE and can be directly connected to a DTE using off-the-shelf RS-232 DB9 cable.

RS-485/422

When configured as an RS-485/422 interface, special-made cable is required for connecting to other equipment with RS485/422 interface. Please refer the product hardware manual for pinouts when making the cables. The cable is also offered as optional accessory and can be ordered from RFI.

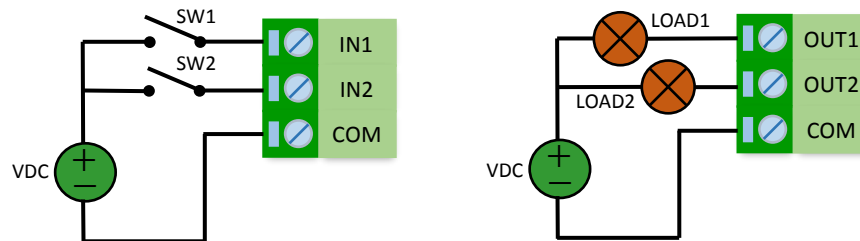
Digital I/Os

A 6-way terminal block for digital I/O connectivity is included in the standard package. Customer will have to carry out all the wirings If required. Inputs and outputs have separate common points to suit different application needs. COM terminal aside IN1 is used for inputs only and the other is for outputs, and they are not electrically connected.



Digital I/O Interface

A typical digital I/O wiring is illustrated below. Customers can design their own circuit connections to suit the application needs.



Typical Digital I/O Wiring

Please strictly follow the maximum rating of the I/O interfaces, which is specified in the product hardware manual. Otherwise damage to the internal electronics, as well as customer equipment, could occur.

Power Interface

The device is getting power through a 3-way terminal block socket/plug, which the 3rd pin ("E") is for protective earth connection and can be left floating if not used. The power source must be within the ratings specified in the product hardware manual, otherwise damage to the internal electronics, as well as customer equipment, could happen. It is recommended to use the 12VDC/1.5A power adaptor available from RFI, which can be ordered as an optional accessory.



Power Interface

The device is protected against reverse-polarity voltage input and will not be powered. However, please do NOT keep device supplied with improper power source for an extended period.

Always take extra cautions when trying to connect the protective earth, as different potential may exist in the electric wiring system and improper earth connection can cause loop current and risk of equipment damage. It is recommended to carry out a thorough review of the relevant electrical circuit/wiring in advance.

LED Indication

The router provides six LED indicators: "PWR", "SIM", "SIG", "DAT", "USR", and "T/R". The table below shows the details of the LED functions:

LED	Function Description
PWR	Router Status Indication: ON: the router is getting power BLINKING: the router is operating
SIM	SIM Status Indication: ON: SIM1 is in use BLINKING: SIM2 is in use OFF: No SIM is inserted
SIG	Cellular Signal Strength Indication. Please see the Signal Strength Indication Table for details.
DAT	WAN Data Indication. ON: WAN connection is active BLINKING: WAN data activity
USER	User Defined Function Indication. Can used for indication of status of GNSS, DDNS, VPN, and PPPoE.
T/R	Serial Interface Data Activity Indication. RED: Transmitting data GREEN: Receiving data

The cellular signal strength LED (SIG) follows the following display pattern:

Signal Strength	SIG LED
SIGNAL > -84dBm (or excellent RSSI setting)	SOLID ON
-91dBm < SIGNAL ≤ -84dBm	200ms OFF / 800ms ON
-98dBm < SIGNAL ≤ -91dBm	400ms OFF / 600ms ON
-105dBm < SIGNAL ≤ -98dBm	600ms OFF / 400ms ON
SIGNAL ≤ -105dBm	800ms OFF / 200ms ON
SIM Not Registered	OFF

Reset Button

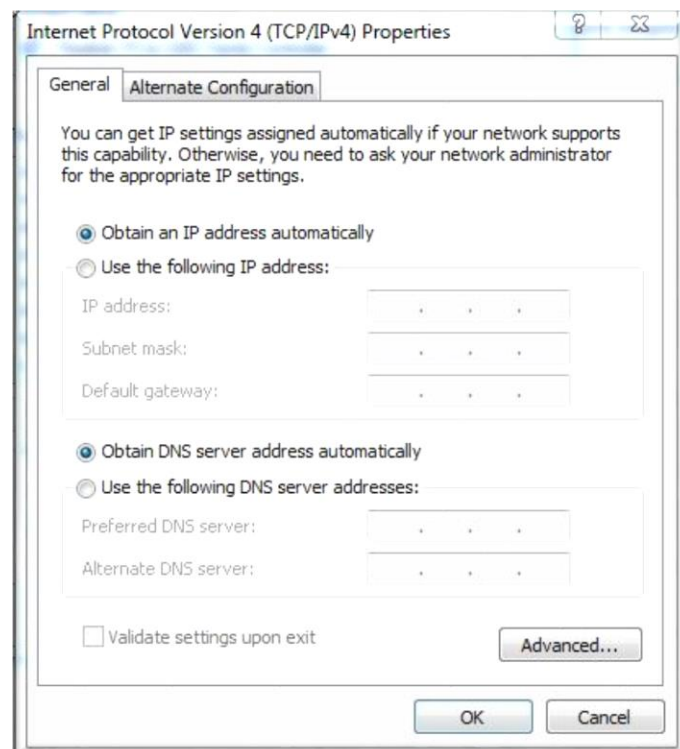
The “Reset” button is used to restart the device or restore the modem to its original factory default settings. To restart the device, press and hold the button for any time between 1s to 4s. If hold for more than 5s but less than 20 seconds, the router will restore a pre- saved profile and restart automatically. To restore the router to factory default settings, press and hold the button more than 20s, the router will then store its original factory default settings and restart.



Note that the reset button is recessed to prevent accidental resets – to press, use a small tool such as a ballpoint pen.

DEVICE MANAGEMENT

Universal Hub is managed via a web interface. To access the device web interface, users will need a computer with a spare Ethernet port. The Ethernet card configuration should have the Internet Protocol TCP/IP set to obtain an IP Address and DNS server address automatically (DHCP enabled). To check these settings, users need to go to Ethernet adaptor properties and check the Internet Protocol TCP/IP settings, which should look as below in a Windows OS:



Connection Steps:

1. Connect the Ethernet cable supplied with the router to the computer Ethernet port and one of the Ethernet port on the router
2. Computer will be able to acquire an IP address from the router's DHCP range.
3. In a web browser, type 192.168.0.1 (The factory default IP Address of the router) in the Address (URL) field. The router will prompt for login credentials and the default username and password are "admin" and "password".

RFI
TECHNOLOGY SOLUTIONS

**Universal-Hub
Wireless Router
Web Login**

Hello

Please enter Universal-Hub Wireless Router web management username and password.

Username

Password

Login

Copyright © 2018 RFI Industries Pty Ltd. All rights reserved.

For further help, please contact RFI Industries on +61 2 8814 2300 or via e-mail at iot.support@rfi.com.au.

The router can also be managed remotely if the device has a public accessible IP address and allows the web access from the WAN.

It is strongly recommended that users change the default login credentials, at least the password, before deploying the device in the field to avoid security risks. This is especially critical if the router has a public accessible IP address over the internet.

Once logging in successfully, Device Status Overview will be shown. The router configurations and features can all be viewed and managed via this web-based user interface.

There is a timeout for a login session if web page remains idle for 15 minutes. Re-login is required after timeout.

DEVICE STATUS

The Device Status pages display the device information (hardware & Software), and the status of the network, interfaces and services.

Overview

The overview page lists the key information of the router for the hardware, network, services and interfaces.

Status > Overview

Device

System Time : 2019-03-05 09:53:54
Up Time : 0day : 13h : 3m : 39s
Device FW Version : MMdm-1.0.8 [201902270002]
Module IMEI : 359075060490587

Cellular Network

Network Operator : Telstra Mobile Telstra
Registration : Local network registered
Signal Strength : -101 dBm

WAN Connection

WAN Links : Connected
IP Address : 123.210.238.121
Gateway : 123.210.238.122
Netmask : 255.255.255.252

Services

Socket Connection : Disconnected
Dynamic DNS : Registered
GNSS : Fixed(6) 33°58'23.2" South 151°44'43.8" East

Digital I/Os

Digital Inputs : OFF, OFF
Digital Outputs : OPEN, OPEN

Device

This page shows the device hardware related information and cellular network information.

Status > Device Info

System Time : 2019-03-05 12:47:16
Up Time : 0day : 0h : 5m : 17s
Online Time : 0day : 0h : 3m : 34s
Device Serial Number : RFIMA-1960936064
Device HW Version : 1.1
Device FW Version : MMdm-1.1.1 [201903050102]
Module FW Version : SWI9X30C_02.24.05.06 r7040 CARMD-EV-FRMWR2 2017/05/19 06:23:09
Module IMEI : 359075063478332

SIM IMSI : 505013413494908
SIM ID(ICCID) : 89610180001669657852
SIM PIN Status : PIN Deactivated

Network Operator : Telstra Mobile Telstra
Registration : Local network registered
Location Area Identification : 50501
Location Area Code : 2064
Cell Information : 7F31121
Operating RAT Band : E-UTRAN (B7)
Signal Strength : -71 dBm (22)

Board Temperature : 37.3 °C
Module Temperature : 38 °C
Input Voltage : 14.38 Volt

The input voltage, board and cellular module temperature will be displayed in this page.

Connections

This page shows the status of network connections of the device. It has two tabs: Interfaces, DHCP Clients, and Mobile Data. The Interfaces tab shows the information of the WAN and LAN connections, and the DHCP Client tab shows the DHCP clients that are currently connected to the device LAN interface.

Status > Connections

Interfaces		DHCP Clients	Mobile Data
WAN			
Connection Status :		Connected	
Interface Type :		Cellular(RNDIS)	
Active SIM :		SIM 0	
IP Address :		161.43.195.160	
Netmask :		255.255.255.192	
Gateway :		161.43.195.161	
Transmitted Bytes :		1,040,423	
Received Bytes :		601,343	
Eth0			
IP Address :		Bridged	
Netmask :		Bridged	
Transmitted Bytes :		874,856	
Received Bytes :		142,113	
MAC Address :		74:e1:82:80:92:00	
Eth1			
IP Address :		0.0.0.0	
Netmask :		0.0.0.0	
Transmitted Bytes :		0	
Received Bytes :		0	
MAC Address :		74:e1:82:80:92:02	

Status > Connections

Interfaces		DHCP Clients	Mobile Data
Client Lists			
MAC Address	IP Address	Name	Remaining Time
70:5A:0F:80:96:56	192.168.0.131	rfl-l-05bm0	1day 0:5:46

The Mobile Data tab shows the mobile data usage for each SIM.

Status > Connections

	Interfaces	DHCP Clients	Mobile Data
SIM0			<div>Billing Date : 1 Usage : DL: 740 KB, UL: 1 MB, UL+DL: 2 MB Quota : 0.19 % <div>Reset</div></div>
SIM1			<div>Billing Date : 1 Usage : DL: 92 KB, UL: 63 KB, UL+DL: 155 KB Quota : 0.02 % <div>Reset</div></div>

VPN & Tunnels

This page shows the status of VPN and tunnels that are configured to use within the router.

Status > VPN & Tunnels

IPSecG	Gateway : Listening
IPSecS2SG	Site to Site Gateway : Listening
IPSec 3	Not configured
Tunnel 1 (l2tps1)	L2TP Server : Connected(10.2.0.10)
Tunnel 2 (pptpsvr)	PPTP Server : Listening
Tunnel 3	Not configured
Tunnel 4	Not configured
Tunnel 5	Not configured
Tunnel 6	Not configured

Status > VPN & Tunnels

IPSec 1	Not configured
IPSec 2	Not configured
IPSec 3	Not configured
Tunnel 1 (l2tpc1)	L2TP Client : Connected(10.2.0.10)
Tunnel 2	Not configured
Tunnel 3	Not configured
Tunnel 4	Not configured
Tunnel 5	Not configured
Tunnel 6	Not configured

If an VPN tunnel is up and connected, the client IP (local or remote) will be shown.

Service

This page shows the status of Services provided by the router, including IP socket connect, dynamic DNS, GNSS, and VRRP.

Status > Service

Socket Connection

Socket Type : TCP Server
Remote IP & Port :
Connection Status : Listening
Connect Time : 0 Days 0:0:0

Dynamic DNS

Dynamic DNS Provider : NoIP
Domain Name : maxtest.ddns.net
Update Status : Updated(123.210.238.121)

GNSS

Last Fixed Time : Tue Mar 05 2019 11:34:09 GMT+1100
(Australian Eastern Daylight Time)
Geo Location : South 33°45'23.7", East 151°44'33.8"
Speed : 0 km/h

VRRP

Connection mode :
IP address :
MAC Address :
Gateway :

I/O & Analogue

This page shows the status of digital I/Os and analogue inputs of the device.

Status > Digital I/O & Status

Digital Input

Input 1 : OFF
Counter : 0
Input 2 : OFF
Counter : 0

Digital Output

Output 1 : OPEN
Output 2 : OPEN

Analogue Input

When a digital input is configured as a counter, the Clear button will be available to manually clear the counter value.

The state of the output ports can also be toggled by the buttons associated with the port.

Analogue inputs are not supported in the current model and will be available in the future products.

BASIC CONFIGURATIONS

Basic Configuration provides settings for WAN and LAN interfaces, Serial Port, GNSS, Contacts, Digital I/O functions, and LED controls.

WAN Interface

This page provides the settings for the device WAN interface and the connection check using ICMP protocol.

Basic Configurations > WAN Interface

Interface	
Primary Interface :	Cellular ▼
Backup Interface :	None ▼
Restart on WAN Failure :	Disable ▼

Ping Check	
Enable :	<input type="checkbox"/>
First Server(WAN) :	
Second Server(WAN) :	
First Server(LAN) :	
Second Server(LAN) :	
Interval :	Seconds
Timeout :	Seconds
Retries :	Times
Interface Reset :	<input type="checkbox"/>

Primary Interface: the primary WAN interface for the router. It can be either Cellular or Ethernet(ETH0). WiFi is not support in this model.

Backup Interface: the backup WAN interface for the router when the primary interface becomes unavailable. It can be either Cellular or Ethernet(ETH0) that is different from the primary interface.

Restart on WAN Failure: option to enable router to reboot in case of all WAN interfaces are failed. Disabled by default and the router will keep trying the selected WAN options in loop.

Ping Check - Enable: option to enable the ping check for the WAN connectivity. The Ping Check will try pinging two designated servers with pre-defined intervals.

First Server (WAN): the IP address of the first server for the ping check on WAN interface. Leave blank if not used.

Second Server (WAN): the IP address of the second server for the ping check on WAN interface. Leave blank if not used.

First Server (LAN): the IP address of the first server for the ping check on LAN interface. Leave blank if not used.

Second Server (WAN): the IP address of the second server for the ping check on LAN interface. Leave blank if not used.

Interval: the interval in seconds between two consecutive ping checks.

Timeout: the maximum time in seconds for a ping check to wait for response from a server.

Retries: maximum number of retries the router will undertake for unsuccessful ping checks to the two servers.

Interface Reset: option to allow router to reset the network interface after the ping check retries are exhausted.

Cellular

The Cellular settings allow to set up mobile network to be used, as well as those mobile network related configuration and dual SIM back up policies. The page has three tabs: General, SIM 0, and SIM 1.

General

This Tab is used to set up the dual SIM back up policies.

Basic Configurations > Cellular Connections

GeneralSIM 0SIM 1

Primary SIM

Slot : Auto

Network backup policy

Switch to Secondary SIM when connection fails : ☒

Switch to Secondary SIM when roaming is detected : ☐

Switch to Secondary SIM when data limit is exceeded : ☐

Primary SIM Recover

Switch to Primary SIM when connection fails : ☒

Switch to Primary SIM when roaming is detected : ☐

Switch to Primary SIM when data limit is exceeded : ☐

Switch to Primary SIM after timeout : ☒

Initial timeout (Minutes) : 60

Back Off

Reboot after Backoff Failed : ☒

Retries : 5 times

Primary SIM: the primary SIM card used by the router.

Auto: No primary SIM card if Auto is selected. Router will use whichever is available after start. If both SIM are presented, SIM0 will be used. If the current SIM connection is failed, the router will try the other SIM if available. Backup policy will not apply to Auto mode.

SIMx: SIMx is the primary SIM card. The router will switch to the secondary SIM if any of the Backup policy is met for the primary SIM.

SIM Back Policy: the conditions when router is to switch from primary SIM to the secondary SIM, which include

- Switch to Secondary SIM when connection fails
- Switch to Secondary SIM when roaming is detected
- Switch to Secondary SIM when data limit is exceeded

The data limit has three options: Uplink, Downlink, and Combined for each SIM and have to be activated to use this policy.

Primary SIM Recover: the conditions when router is to switch back to the primary SIM, which include

- Switch to Primary SIM when connection fails
- Switch to Primary SIM when roaming is detected
- Switch to Primary SIM when data limit is exceeded

The Data limit will have three options: Uplink, Downlink, and Combined.

- Switch to Primary SIM after timeout

Allow a maximum time in minutes for the router to operate on secondary SIM and will switch back to primary SIM after.

Reboot after Backoff Failed: enabled by default, the modem will perform reboot if unable to get WAN IP via cellular network after a number of pre-defined retries. The option is valid when the modem uses only cellular as the WAN interface. When disabled, the modem will keep trying to get WAN IP without rebooting. There are 20 seconds backoff time between retries.

Retries: the number of retries when doing backoff retries before rebooting.

SIM 0 / SIM 1

This Tab is used to set up the mobile network parameters for SIMs.

APN: Access Point Name for the mobile network.

Authentication: the authentication method used for the mobile network. Can be either PAP or CHAP depending on the network provider.

Username: the username for the mobile network access if applicable. Can be left blank if not required.

Password: the password for the mobile network access if applicable. Can be left blank if not required.

SIM 1

APN :	telstra.internet
Authentication :	PAP ▼
User name :	
Password :
Auto PIN :	Disable ▼
Auto PIN code :	
Band Frequency :	<div><input checked="" type="checkbox"/> Auto <input checked="" type="checkbox"/> WCDMA B1 <input checked="" type="checkbox"/> WCDMA B5 <input checked="" type="checkbox"/> WCDMA B6 <input checked="" type="checkbox"/> WCDMA B8 <input checked="" type="checkbox"/> WCDMA B9 <input checked="" type="checkbox"/> WCDMA B19 <input checked="" type="checkbox"/> LTE B1 <input checked="" type="checkbox"/> LTE B3 <input checked="" type="checkbox"/> LTE B5 <input checked="" type="checkbox"/> LTE B7 <input checked="" type="checkbox"/> LTE B8 <input checked="" type="checkbox"/> LTE B18 <input checked="" type="checkbox"/> LTE B19 <input checked="" type="checkbox"/> LTE B21 <input checked="" type="checkbox"/> LTE B28 <input checked="" type="checkbox"/> LTE B38 <input checked="" type="checkbox"/> LTE B39 <input checked="" type="checkbox"/> LTE B40 <input checked="" type="checkbox"/> LTE B41</div>

Data Limitation

Activate :	<input type="checkbox"/>
Day of the Month :	
Report when Remaining :	<input type="checkbox"/> 50% <input type="checkbox"/> 25% <input type="checkbox"/> 10%
Data Source :	
Maximum Data :	KB

Connections

Mode :	RNDIS ▼
--------	---------

Save **Cancel**

Auto PIN: option for the router to automatically apply PIN code if PIN request is enabled in the SIM card. A PIN code must be correctly entered in the field provided as wrong PIN code will lock the SIM card.

Band Frequency: option to select 3G and/or 4G bands used by the cellular module to access mobile network. Default is Auto, which means all the supported bands are allowed and automatically chosen via network negotiation. Users can use this option to select specific bands to lock in 3G or 4G connectivity.

(Data Limit) Activate: option to activate the SIM data limit settings. the option must be activated for the SIM to be able to use data limit backup

policy. The data usage information for each SIM can be found in the Connection status page.

Day of the Month: the day in a month that the SIM data usage is to reset. Range is from 1 to 30.

Report when Remaining: The router will send an SMS alert when the remaining data reaches 50%, 25%, or 10%. The contact group to receive the SMS is defined in the SMS commands settings.

Data Source: the data usage source, which is one of the following: DL (Download only), UL (Upload only), or DL+UL (both Download and Upload).

Maximum Data: the maximum data allowance for the SIM in kB. After maximum data allowance is reached, the SIM will not be used until the usage is reset by date

Connection Mode: the mobile network connection mode, which can be RNDIS, PPP, or Bridge.

RNDIS: Remote Network Driver Interface for cellular WAN connection. This is the default mode for most applications.

PPP: Point-to-Point Protocol to be used for the cellular WAN connection. Ability of using PPP is cellular module and network dependent and may not work in some situations.

Bridge: Bridge mode only works when PPP protocol is in use. By this mode, PPPoE protocol can be utilised through one of router's LAN port to get WAN IP from the mobile service provider.

Ethernet

Ethernet settings allows to set up router's Ethernet interface, include device IP and subnet, wired WAN interface over ETH0, DHCP service, and MAC binding.

ETH0

Ethernet Port 0 (ETH0) can be used as either a LAN port (in switch mode or separate LAN) or a Wired WAN interface.

Basic Configurations > Ethernet Configuration

The screenshot displays the 'Basic Configurations > Ethernet Configuration' page. At the top, there are two tabs: 'ETH 0' (active) and 'ETH 1'. Below the tabs, the 'Mode' section contains a 'Working As' field with two radio buttons: 'LAN' (selected) and 'WAN'. Below this is a 'Link Speed' dropdown menu currently set to 'Auto'. The 'LAN Mode' section features a 'Bridge' toggle switch which is turned on.

Mode: the working mode for ETH0: LAN or WAN.

Link Speed: each Ethernet interface can be configured with specific link speed for compatibility. The speed options include:

Auto: Auto-negotiation for 1000M/100M/10M

10BaseT/Half: 10M Half Duplex

100BaseT/Full: 10M Full Duplex

100BaseT/Half: 100M Half Duplex

100BaseT/Full: 100M Full Duplex

WAN Connection: the settings are for ETH0 as a WAN interface. Three connection types can be configured for the interface: DHCP, Static, and PPPoE.

ETH 0
ETH 1

Mode

Working As ☐ LAN ☒ WAN

WAN Connection

Connection Type : Static ▼

DHCP
Static
 PPPoE

Static

IP Address :

Netmask :

Gateway :

Primary DNS :

Secondary DNS :

DHCP: the WAN interface will be as a DHCP client and acquire WAN IP from a DHCP server.

Static: the WAN interface will use static IP settings defined, including device IP, netmask, gateway, and DNS.

PPPoE: the WAN interface will be established by PPP over Ethernet protocol. Authentication settings will be required for the connection.

LAN Mode: the working mode as a LAN port.

Bridge: in this mode, the router's Ethernet ports are acting as a 2-port switch. All LAN settings are configured in in ETH1. This is the default mode for ETH0.

Separate LAN: if Bridge mode is not selected, the ETH0 will be as a separate LAN interface with different subnet settings.

DHCP Server: Option to enable/disable DHCP sever function on the LAN port, and the configuration for a DHCP server, such as IP range, Lease Time, and Doman name.

DHCP MAC Binding: only available when DHCP server is enabled. This is to bind certain static IP addresses to specific clients based on their MAC addresses. Up to 20 clients can be added.

Mode

Working As ☒ LAN ☐ WAN

LAN Mode

Bridge ☐

LAN

IP Address : 192.168.11.1

Netmask : 255.255.255.0

DHCP Server : ☐ Disable ☒ Enable

DHCP Server

Range : 192.168.11.101 - 192.168.11.150

Lease : 3600

Domain : MModem2

DHCP MAC Binding

MAC Address	IP Address	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

ETH1

Ethernet Port 1 (ETH1) can only be used as a LAN port (in switch mode or separate LAN). The settings associated with ETH1 are similar to those for ETH0 except Multiple IP function.

Basic Configurations > Ethernet Configuration

ETH 0 **ETH 1**

LAN

IP Address : 192.168.0.1

Netmask : 255.255.255.0

Link Speed : Auto ▼

Multiple IP : ☒ Disable ☐ Enable

DHCP Server Activate : ☐ Disable ☒ Enable

DHCP Server

Range : 192.168.0.101 - 192.168.0.150

Lease : 86400

Domain : MModem

DHCP MAC Binding

MAC Address	IP Address	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

No.	MAC Address	IP Address	Del
-----	-------------	------------	-----

Multiple IP: Option to enable/disable multiple IP function on the LAN port. The function is available to ETH1 port only and supports one extra IP address.

(Multiple IP) IP Address: The second LAN IP address of the modem.

(Multiple IP) Netmask: the netmask for the second LAN IP segment.

Serial Interface

The Serial Interface contains those configurations for the applications of serial port in the router.

Common Settings

The general settings for the physical serial interface.

Basic Configurations > Serial Interface

Common	SMS	Notification	Socket
---------------	-----	--------------	--------

Serial Common

Mode :	RS232 ▼
Baudrate :	115200 ▼
Flow Control :	None ▼
Data Bits :	8 ▼
Parity :	None ▼
ECHO :	0 ▼
&D :	0 ▼
&C :	0 ▼

Mode: the working mode for the serial interface. Three working mode are supported: RS232, RS485, and RS422.

Baudrate: the baudrate of the serial port. Supported options include: 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200.

Flow Control: supports None, RTS/CTS, and DTR/DSR.

Data Bits: supports 5, 6, 7, and 8 bits.

Parity: supports None, Even, and Odd.

Echo: 0 – no echo, 1 - with echo

&C: options for DCD signal:

0, 1 – DCD signal is always ON.

- 2 – DCD signal is always OFF
- 3 – DCD will be ON when WAN is connected, otherwise stay OFF.
- 4 – DCD will be ON when socket is connected, otherwise stay OFF.

&D: options for DTR signal:

- 0 – DTR signal is ignored.
- 1 – When there is an active socket connection, the serial interface will be into AT command mode when ON-OFF transition is detected and be back to data mode when DTR is back to ON state.
- 2 – When there is an active socket connection, the connection will be dropped when ON-OFF transition is detected and back to server listening mode when DTR is back to ON state. Hardware flow control need to be set for this option.

SMS

This is to set up serial port input reporting via SMS.

Delimiter: the character that used to indicate separate messages received from serial port and send by SMS. Can be one of *None*, *<CR>*, *<LF>*, *<CR><LF>*, and *<LF><CR>*. If *None*, the message length will be the serial interface buffer size.

Phone Group: the group of phone numbers that the SMS will be delivered to. If disabled, the function is deactivated.

Notification

The settings are to configure whether the router will send out bootup and IP Stack messages over the serial interface.

Common	SMS	Notification	Socket
--------	-----	---------------------	--------

Notification

Boot message :	<input checked="" type="checkbox"/>
IPStack message :	<input checked="" type="checkbox"/>
TCP connection message :	Disable ▾

Boot message: option to enable/disable boot up messages over the serial interface.

IPStack message: option to enable/disable IP stack connection messages over the serial interface.

TCP connection message: the option to allow device to send a customisable message to the remote device once a socket connection is established.

Socket

This page is to configure the socket connection over serial interface.

Common	SMS	Notification	Socket
--------	-----	--------------	---------------

Socket

Mode :	Server ▾
Protocol :	TCP ▾
Primary Server Address :	
Secondary Server Address :	
Port :	30000
IDLE timeout :	<input checked="" type="checkbox"/>
IDLE timeout interval :	3600 Seconds

Secure Socket

SSL :	Disable ▾	X.509 1 ▾
-------	-----------	-----------

Mode: socket mode, either Server (default) or Client, or can be Disabled.

Protocol: the socket protocol in use, either TCP or UDP.

Primary Server Address: the IP/URL of the primary socket server when acting as set as a client.

Secondary Server Address: the IP/URL of the secondary socket server when set as a client.

Port: the port number used for the socket connection.

IDLE Timeout: the option to enable/disable IDLE timeout function. IDLE means no incoming traffic from remote device.

IDLE Timeout Interval: the maximum time in seconds for a socket connection to stay in idle before being terminated.

Secure Socket: the Universal Hub supports secured TCP socket when enabled. Two encryption modes are supported: SSLv3 and TLSv1. The certificates to be used are defined in the X.509 Configuration under Advanced Networking. The certificates required, as an example, are:

CA certificate, e.g. ca.crt

local certificate, e.g. sever.crt (or client.crt)

local key, e.g. server.key (or client.key)

The requirement of CA certificate is depending on the server and is optional.

Network Dormant Period: the time interval in seconds for the router to send a null data packet over the mobile network to avoid the connection going into dormancy in case of no data activity during the period. For UDP protocol only.

Keep Alive: when enabled, the router will send a dummy UDP packet to the remote device to avoid dormancy in the remote device. For UDP protocol only.

Wake Up: the time interval in seconds for the router to send Keep Alive dummy packet. Only available when Keep Alive is enabled.

FTP Client

The FTP Client function allows the device to upload peripheral information to a remote FTP server on a regular basis or manually via an AT command from Serial Interface.

FTP Client

The FTP Client settings configure the options required by the remote FTP server, time intervals, and the file name to be uploaded.

Basic Configurations > FTP Client

FTP Client	
Interval :	Hourly ▼
Interval timeset :	1
Secure FTP :	<input checked="" type="checkbox"/>
Server Address :	172.16.0.9
Server Port :	22
User Name :	maxon
User Password :	*****
File Name :	RFIMAX
File Size :	4000 Bytes
Log Interval :	5 Minutes ▼

Interval: to enable and set up FTP upload interval. Time options include Manual, Minutes, Hourly, Time of Day, and Day of Month. When set up as Manual, the FTP upload will be triggered by AT command AT\$\$\$FTPSC via serial interface or AT over IP.

Interval timeset: the time interval value associated with Interval setting: 0-60 for Minutes, 0-24 for Hourly and Time of Day, 0-30 for Day of Month.

Secure FTP: the option to enable the SSH-FTP protocol.

Server Address: the IP address or URL of the remote FTP server.

Server Port: the port number used for the FTP server.

User Name/ User Password: the log in credentials for the FTP server.

File Name: this is to define the filename to begin with. The file will always contain time stamp and will be in the format of “filenameyyyymmddhhmmss.csv”.

File Size: the maximum file size in bytes for a log file. Once the file reaches the size limit, a new log file will be created.

Log Interval: the time interval for the device to record the selected information(content) to the log file. The options include Continue, 1, 5, 10, 15, 30, and 60 minutes. Please note that, when in Continue mode, the device will record the information only when a delimiter is received over the serial interface. For delimiter setting, please see configurations for Serial Interface.

Content

The Content settings define the information to be recorded in the log file that is to be uploaded via FTP.

Contents

Timestamp :	<input checked="" type="checkbox"/>
Serial :	<input type="checkbox"/>
Digital I/O :	<input checked="" type="checkbox"/>
Analogue :	<input checked="" type="checkbox"/>
Counter :	<input checked="" type="checkbox"/>
Temperature :	<input checked="" type="checkbox"/>
Input Voltage :	<input checked="" type="checkbox"/>

Time Stamp: the time stamp for the record. The format of the time stamp is YYYY/MM/DD HH:MM:SS.

Serial: the message received from the serial interface, separated by the defined delimiter.

Digital I/O: the status of the digital I/Os.

Analogue: the values of the analogue inputs. Not supported in the base model.

Counter: the counter values.

Temperature: the temperature values of the device and cellular module.

Input Voltage: the device input voltage value.

The log file will record the contents in the following format:

Timestamp,IN0,IN1,OUT0,OUT1,AN1,AN2,AN3,AN4,AN5,CNT0,CNT1,DeviceTemp,ModuleTemp,VIN

GNSS

Universal Hub support location services provided by GPS and GLONASS.

General Settings

The General settings page configures the GNSS receiver functions.

General Network Geo-Fence

GNSS Information

Activation : Disable ▾

Output Interface : ☒ Network ☐ Serial

Update Interval : Seconds

Device ID : ☒ Append the device ID

Satellite System : GPS ▾

Contents : ☒ RMC ☒ VTG ☒ GGA
☒ GSA ☒ GSV ☒ GNS

I/O Status Reporting : Disable ▾

Activation: to enable/disable the GNSS function in the device.

Output Interface: the interface that the GNSS information (NMEA sentences) will be sent through. Can be serial interface, IP socket, or both.

Update Interval: the time interval in seconds for updating the GNSS information over the output interface. Minimum time interval is 5 seconds.

Device ID: if enabled, the Site ID set in SMS settings will be added to the beginning of the GNSS information.

Satellite System: option to select the GNSS system to use. Currently supports GPS and GLONASS.

Contents: Up six types of NMEA sentences can be selected from for the GNSS information to be sent over the interface. "GNS" is for GLONASS only.

IO Status Reporting: option to enable the status of the router's I/O peripherals to be appended to the GNSS information. The information will have the following format:

\$DIO:Index,TimeStamp,OUT1,OUT2, IN1,IN2

\$ANA:*,*,*,*,*,*,BoardTemperature,VIN

\$NET:WANIP,UpTime,,RSSI

For example:

\$DIO:62,2019/03/07,12:56:23,Open,Open,Off,Off

\$ANA:2730,749,1870,1149,989,1307,1530,36.50,12.24

\$NET:123.209.64.105,00:05:51,, -103

Ignition Input

Activation :	Disable ▼
Input :	
Message Interval for On State :	
Message Interval for Off State :	

(Ignition Input) Activation: the option allows different GNSS location updating frequency based on a digital input status, e.g. the ignition status of a vehicle. The updating intervals will overwrite the setting in GNSS Information. Disabled by default.

Input: option to select the digital input for controlling the GNSS location updating frequency.

Message Interval for ON State: the GNSS location updating interval in seconds when the input is ON state.

Message Interval for Off State: the GNSS location updating interval in seconds when the input is OFF state.

Additional Settings

Initial Location Fix Message :	
String send with GNSS Location Update :	

Initial Location Fix Message: the message to be sent after the initial location fix.

String send with GNSS Location Update: the extra customised messages to be appended to the location messages.

Network

This page configures the IP socket connection for the GNSS information reporting.

The screenshot shows a web interface with three tabs: 'General', 'Network' (which is selected and underlined), and 'Geo-Fence'. Below the tabs, the 'Network' section is titled. It contains four configuration fields: 'Protocol' is a dropdown menu set to 'TCP'; 'Primary GNSS Center Address' is a text box containing 'maxon01.dynu.net'; 'Secondary GNSS Center Address' is a text box containing '0.0.0.0'; and 'Port' is a text box containing '30000'.

Protocol: the IP protocol to be used for socket connection.

Primary GNSS Center Address: the IP/URL of the primary GNSS centre.

Secondary GNSS Center Address: the IP/URL of the secondary GNSS centre.

Port: the port number used for the socket connection.

Geo-Fence

The Universal Hub has the function to send warning messages (SMS or email) in case the device is outside of its pre-defined location.

General	Network	Geo-Fence
Geo-fence		
Activation :	Enable ▼	
Mode :	Radius ▼	
Update Interval :	30	Seconds
Current NMEA : S 3359.3855 , E 15104.7256		
Option Radius		
GNSS Coordinate of Center :	S ▼	0.0000 °
	W ▼	0.0000 °
Distance Limit :	10	Meters
Phone Group and Message		
Phone Group :	Disable ▼	
Message :		

Activation: to enable/disable the GNSS function in the device.

Mode: define the scope of the designated geographic boundary, either a circle by radius or a rectangle by two coordinates.

Update Interval: the time interval in seconds to check if the current location is within the pre-defined area.

Current NMEA: the current geolocation of the device in NMEA DMM format.

Option Radius/Rectangle: the centre/radius or two coordinates of the designated geographic boundary. The coordinators entered here need to be DD format. To transfer a NMEA DMM value to DD format, take out the Minutes in DMM value and transfer it to Degree and add the result back to the Degree value from the DMM value.

For example, a DMM value 15104.7256 has the Degree value of 151 and Minute value of 4.7256. The Minute 4.7256' gives a Degree value of 0.07876. Therefore, the DD value will be $151 + 0.07876 = 151.07876$.

Contact Group: the contact group who the geo-fence alert messages will be sent to.

Message: the content of the alert message.

SMS/Email

The SMS/Email Settings manage the SMS and Email functions that are supported by the router. The functions include SMS commands, alarms by SMSs and Emails, and Email account used by the device.

SMS Settings

The SMS Settings manage the SMS commands and alarms, as well as the contact group who can send/receive SMSs.

SMS Email

Site ID :

SMS Commands : ☒

Contact Group : Disable ▾

Allow WANIP, APN and REBOOT Commands when no Contacts : ☒

General Notification

SMS on power up : ☐

SMS on WAN connected : ☐

SMS on WAN disconnected : ☐

Device Alarms

SMS on Board Temperature : ☐ THD: °C, RNG: °C

SMS on Input Voltage : ☐ THD: V, RNG: V

SMS on Module Temperature : ☐ THD: °C, RNG: °C

Allow sending alarm every hour when alarms persist : ☒

Site ID: the site name of the device that will be added to the start of each SMS messages sending from the device.

SMS Commands: option to allow the device to receive and execute the SMS commands sent from a specified contact group. It is enabled by default.

Contact Group: the contact group who can send SMS commands and get SMS alarms.

Allow WANIP, APN and REBOOT Commands when no Contacts: the option to allow the device to receive and execute certain SMS commands from any numbers when no contacts are defined and SMS commands are disabled. It is enabled by default. Only the following three SMS commands are allowed: WANIP inquiry, APN Setup, and Reboot command. The option is useful when device is in the field and has undergone a factory reset. It is strongly recommended that the option is disabled after the device is properly configured for SMS functions.

SMS on Power UP: when enabled, an SMS will be sent to the specified contact(s) when the device is powered up/restarted. Disabled by default.

SMS on WAN Connected: when enabled, an SMS will be sent to the specified contact(s) when the device is getting a WAN IP. Disabled by default.

SMS on WAN Disconnected: when enabled, an SMS will be sent to the specified contact(s) when the device has lost WAN connection. Disabled by default.

SMS on Board Temperature: when enabled, an SMS will be sent to the specified contact(s) when the device internal temperature in °C exceeds the THD value or below the (THD-RNG) value. For example, if THD is set to 60°C and RNG is 60°C, an alarm SMS when device internal temperature is over 60°C or below 0°C. Disabled by default.

SMS on Input Voltage: when enabled, an SMS will be sent to the specified contact(s) when the device input voltage in Volt exceeds the THD value or below the (THD-RNG) value. Disabled by default.

SMS on Module Temperature: when enabled, an SMS will be sent to the specified contact(s) when the device cellular module temperature in °C exceeds the THD value or below the (THD-RNG) value. Disabled by default.

Allow sending alarm every hour when alarms persist: when enabled, an SMS will be sent once per hour to the specified contact(s) when the alarms persist more than an hour. Enabled by default.

Email Settings

The Email Settings manage the Email account that device uses and the device alarms via emails.

SMS

Email

Subject :

Contact Group :

Disable ▾

General Notification

Email WAN connected :

☐

Device Alarms

Email on Board Temperature :

☐

THD: °C, RNG: °C

Email on Input Voltage :

☐

THD: V, RNG: V

Email on Module Temperature :

☐

THD: °C, RNG: °C

Allow sending alarm every hour when
alarms persist :

☒

Email Account

SMTP Server :

SMTP Server Port :

465

SSL/TLS :

None ▾

STARTTLS :

☐

User Name :

Password :

Subject: the email subject content that will be included in the emails sending from the device.

Contact Group: the contact group who can receive Email alarms.

Email on WAN Connected: when enabled, an Email will be sent to the specified contact(s) when the device is getting a WAN IP. Disabled by default.

Email on Board Temperature: when enabled, an SMS will be sent to the specified contact(s) when the device internal temperature in °C exceeds the THD value or below the (THD-RNG) value. For example, if THD is set to 60°C and RNG is 60°C, an alarm SMS when device internal temperature is over 60°C or below 0°C. Disabled by default.

Email on Input Voltage: when enabled, an SMS will be sent to the specified contact(s) when the device input voltage in Volt exceeds the THD value or below the (THD-RNG) value. Disabled by default.

Email on Module Temperature: when enabled, an SMS will be sent to the specified contact(s) when the device cellular module temperature in °C exceeds the THD value or below the (THD-RNG) value. Disabled by default.

Allow sending alarm every hour when alarms persist: when enabled, an SMS will be sent once per hour to the specified contact(s) when the alarms persist more than an hour. Enabled by default.

SMTP Server: the SMTP server address for Email account use by the device.

SMTP Server Port: the port number used by the SMTP server.

SSL/TLS: SSL or TLS security options used by the Email account server.

STARTTLS: enable this option if the Email account server requires STARTTLS.

User Name: the user name of the Email account.

Password: the password of the Email account.

Contacts

The Contacts Settings manages the contacts used by the router to deliver SMSs and emails. The functions with SMS/Email alert capability will send the messages based on groups, which will have one or more contacts with phone numbers and email addresses.

Contacts

The Contacts page is for storing all the required individual contact information including phone numbers and email addresses. Up to 20 contacts can be setup in the device.

Group

Contacts

Add

Name :

Phone Number :

Email :

Add

No.	Name	Phone Number	Email	Delete
1	test1	+614123456	sbc@rfi.com.au	Del
2	test2	+6140023456	abb@rfi.com.au	Del
3	test3	+614323432432	ccc@abc.com	Del

Name: the name of the contact.

Phone Number: the phone number of the contact. Please use international format for proper functions.

Email: the email address of the contact. Leave blank if not used.

Group

The Group page is for set up groups for different reporting purposes. The router will use group to deliver alert SMS and/or emails.

Add

Group Name :	<input type="text"/>
Contacts List :	<input type="checkbox"/> test1 <input type="checkbox"/> test2 <input type="checkbox"/> test3 <input type="checkbox"/> test4 <input type="checkbox"/> test5 <input type="checkbox"/> adm1 <input type="checkbox"/> adm2
	<input type="button" value="Add"/>

No.	Group Name	Contacts	Del
1	grp1	test2, test3	<input type="button" value="Del"/>
2	admin	adm1, adm2	<input type="button" value="Del"/>

Group Name: the name of the group.

Contact List: a list of contacts that have been set up in the router and can be selected for the new group.

Digital I/O

The Digital I/O settings manage the digital inputs and outputs functions that are provided in the router. The functions currently supported by the device include:

- Input state change alarm, input counter and alarm,
- Output control by SMS and scheduling, pulsed output
- Local and remote I/O automation

INPUT 0 / 1

The Input page provides the configuration options for the digital inputs.

INPUT 0

INPUT 1

OUTPUT 0

OUTPUT 1

Alarm

ON Alarm Message :

OFF Alarm Message :

Report SMS Group :

Disable ▾

Report Email Group :

Disable ▾

Input De-bouncing Time :

20

 milliseconds

Input Counter

Counter Function :

☐

Trigger Mode :

BOTH ▾

Counter Alarm Threshold :

9999

Counter Clear when reaches Threshold :

☐

Report SMS Group :

Disable ▾

Report Email Group :

Disable ▾

I/O Automation

Automation Mode :

Local ▾

Site Address :

Secured Remote Control :

☐

ON Action :

Output 0 ▾

☒ CLOSE ☐ OPEN ☐ PULSE

OFF Action :

Output 0 ▾

☒ CLOSE ☐ OPEN ☐ PULSE

Add+

No.	Address	IN No.	ON	OFF	Delete
1	Local	0	OUT0 CLOSE	OUT0 OPEN	Del

ON Alarm Message: the content of SMS and Email to be sent when input state changes from OFF to ON.

ON Alarm Message: the SMS content to be sent when input state changes from ON to OFF.

Report SMS Group: the contact group that the alarm SMSs will be sent to. Disabled by default.

Report Email Group: the contact group that the alarm Emails will be sent to. Disabled by default.

Input De-bouncing Time: the de-bouncing time in milliseconds to avoid noises over the input. Default value is 20ms.

Counter Function: option to enable the counter function for the digital input. Maximum input frequency for counting is 1KHz. The function is disabled by default.

Trigger Mode: the trigger mode for the counter:

ON: counted OFF-ON change only

OFF: counted ON-OFF change only

BOTH: counted on both OFF-ON and ON-OFF changes (default).

Counter Alarm Threshold: an alarm SMS and/or Email will be sent when the counter reaches the defined threshold value. The maximum value is 9999. The Counter will automatically roll back to "0" after reaching the maximum value.

Counter Clear when reaches Threshold: option to enable clearing the counter after the counter reaches the threshold. Disabled by default.

Report SMS Group: the contact group that the counter alarm SMSs will be sent to. Disabled by default.

Report Email Group: the contact group that the counter alarm Emails will be sent to. Disabled by default.

Automation Mode: Universal Hub supports automatic output control by an input either on the same device (Local Mode) or on a remote device with the same function (Remote Mode). Default mode is Local.

The IO automation is achieved by executing automation rules saved in the rules table. Each rule will have Site Address, Input Index, ON Action, and OFF action. Up to ten(10) rules can be set up for each input.

Site Address: the IP or URL of the remote device whose output is to be controlled by the input.

Secured Remote Control: the option to enable the secured communication for the IO automation if the remote device requires it. A pre-shared key will be required. Disabled by default.

ON/OFF Action: the action to take when input is in ON and OFF state. The output index and action (OPEN, CLOSE, or PULSE) will be defined in the action and saved in the rule table below.

OUTPUT 0 / 1

The Output page provides the configuration options for the digital outputs.

INPUT 0	INPUT 1	OUTPUT 0	OUTPUT 1
SMS Control			
Power On State :		OPEN ▾	
Function :		Disable ▾	
CLOSE Message :			
OPEN Message :			
PULSE Message :			
Report Group :			
Remote Control/Automation			
Function :		Disable ▾	
Secured Remote Control :		<input type="checkbox"/>	
Pre-Shared Key :		presharedkey	
Output Scheduler			
Function :		Disable ▾	
Scheduler Table :			
Pulse Output			
Number of Pulses :		0	
Delay :		10	(x 100ms)
Width :		10	(x 100ms)

Power On State: defines the output state after powerup or reboot:

OPEN: output is open after powerup/reboot

CLOSE: output is close after powerup/reboot

LAST: keep the previous state after powerup/reboot

Please be aware that a device reboot will affect the output state because output will become open during booting process.

(SMS Control) Function: the option to enable the SMS control of the output. Disabled by default.

CLSOE Message: User-defined SMS command to close the output.

OPEN Message: User-defined SMS command to open the output.

PULSE Message: User-defined SMS command to output a pulse.

Report Group: the contact group that can send output control SMS commands. Disabled by default.

(Remote Control) Function: the option to allow the output to be controlled by a remote device. Disabled by default.

Secured Remote Control: the option to require a secured IP communication for the remote IO control/automation. The TLS with a pre-shared key is used to encrypt the communication.

Pre-shared Key: the pre-shared key used for the secured remote control.

(Output Scheduler) Function: the option to enable the function that only allows the device output to be controlled (locally or remotely) during a pre-defined period. Outside the time frame, the output state will remain the last state unchangeable until the next schedule time.

A Cron expression with five(5) space-separated fields is used for the schedule settings. The definitions of each field are:

Minute Hour DayofMonth Month DayofWeek

For example, if the output is to be controlled during 8AM to 6PM in a day from Monday to Friday, a Cron expression can be set as:

* 8-18 * * 1-5 *

Users can go to <https://crontab.guru> for more help on Cron expressions. Please note that only "*" "," "-" and numbers are currently supported in the Cron expression settings.

Schedule Table: the Cron expression for the output scheduler.

Number of Pulse: the number of pulses to generate when the output is configured for pulse output. Range is from 0 – 100.

Delay: the time delay in unit of 100 milliseconds before the output is sending a pulse (OPEN-CLOSE-OPEN). Default values is 10 (1 second).

Width: the width of the pulse (the time of output staying in CLOSE state) in unit of 100 milliseconds. Default values is 10 (1 second).

LED Display Control

The SIG and USR LED display in Universal Hub can be customised by users.

Basic Configurations > LED Display Control

RSSI LED

Excellent Signal : - 83 dBm

USER LED

Activate : Disable ▼

Disable

GNSS

DDNS

VPN

PPPoE

Save

RSSI LED: this is to define the excellent signal strength for the SIG LED to be solid ON.

USER LED: this is the define which function will drive the USR LED. The available functions include GNSS, DDNS, VPN, and PPPoE. If selected, the LED will be blinking if the function is active. For example, the LED will be blinking if VPN is selected and the designated tunnel is connected successfully.

ADVANCED NETWORKING

Advanced Networking provides the settings for advanced network routing, VPN tunnels, dynamic DNS, and network securities. Comprehensive network and system knowledge will be necessary for properly managing some of these configurations.

Dynamic DNS

Dynamic DNS, also known as DDNS is a method of automatically updating a name server in the Domain Name System (DNS), often in real time. It solves the problem of having a dynamic IP address by associating the address with a consistent domain name, eliminating the need of a static IP.

Advanced Networking > Dynamic DNS

Configurations

Enable :	No-IP ▼
Service Provider :	
Host :	hostname.ddns.net
User Name :	username
Password / Key :	*****

Enable: option to disable/enable the DDNS function and select the dynamic DNS service provider. Currently support Dyn, No-IP, Dynu, MS-DNS, and customer defined.

Service Provider: the server IP/URL of the DDNS service provider. Only needed if using customer-defined provider.

Host: the URL to be assigned to the router IP address.

User Name: the username for the DDNS account.

Password/Key: the password or key for the DDNS account.

Cloud Service

Cloud Services provide in Universal Hub are provided to allow device management and data collection/presentation/analysis over a cloud-based server platform.

maXconnect

The maXconnect Remote Management portal allows you to manage, control and monitor this device on a web-based portal. The settings below are used to configure the Universal Hub to communicate with the maXconnect Remote Management portal. The maXconnect FTP server is needed to perform FOTA via the portal.

Max Connect

maXconnect

Remote Management : ☒

Server URL : portal.maxconnect.c

Port Number : 120

Update Interval : 120 Seconds

FTP Server URL : updates.maxconnec

Save **Cancel**

Remote Management: option to enable the maXconnect remote management function in the device.

Server URL: the server IP/URL of the maXconnect server. It must be "portal.maxconnect.com.au" by default. If maXwan is used for the WAN connection, it should use IP address of 10.0.0.1.

Port Number: the port number used for the service. It must be 120 by default.

Update Interval: the time interval in seconds for the router to update its status to the server.

FTP Server URL: the URL of the maXconnect FTP server. It must be "updates.maxconnect.com.au". If maXwan is used for the WAN connection, it should use IP address of 10.0.0.32.

IP Routing

The IP Routing settings provide system routing information as well as adding extra static routing policies and using OSPF protocol.

System Route

The page shows the current system routing table.

Advanced Networking > IP Routing

<div>System Route Static Route OSPF</div>				
System Routing Table				
No.	Dest. Network	Gateway	Subnet Mask	Intfance
1	192.168.0.0	0.0.0.0	255.255.255.0	br0
2	172.16.0.8	0.0.0.0	255.255.255.248	eth2
3	0.0.0.0	172.16.0.13	0.0.0.0	eth2

Static Route

The page allows to manually add extra static routing rules to the default system routing table. This is useful when a routing policy cannot be automatically created by the router system.

System Route	Static Route	OSPF
--------------	---------------------	------

Add Static Route

Destination IP Address :	<input type="text"/>
Subnet Mask :	<input type="text"/>
Default Gateway :	<input type="text"/>
Interface :	<div>LAN ▾</div>
	<div>Add</div>

Current Static Route

No.	Dest. Network	Subnet Mask	Gateway	Interface	Delete

Save

Cancel

Destination IP Address: the destination IP/subnet of the static route.

Subnet Mask: the subnet mask for the static route.

Default Gateway: the default gateway for the static route.

Interface: the interface the static route is applied to.

The created static route will be listed in a table and loaded to the system routing table every time the router restarts.

OSPF

OSPF (Open Shortest Path First) is a routing protocol for IP network used to find the best path for packets as they pass through a set of connected networks.

System Route

Static Route

OSPF

Open Shortest Path First

Destination IP Address :

Subnet Mask :

Add

Current OSPF

No.	Dest. Network	Subnet Mask	Delete
-----	---------------	-------------	--------

Destination IP Address: the destination IP for the OSPF protocol.

Subnet Mask: the subnet mask for the OSPF protocol.

The created OSPF route will be listed in a table and loaded every time the router restarts.

NAT

The NAT setting provides option to disable the IP Masquerade (one-to-many NATing) services in the router.

Advanced Networking > NAT

MASQUERADE

Enable : ☒

Save

Cancel

Once disabled, the LAN device will not be able to access WAN if the LAN devices are with private IPs. This service should be enabled in most applications unless the function is specifically required to be turned off.

DMZ

Demilitarized Zone (DMZ) is a subnet that separates an internal LAN from other untrusted networks, usually the internet. DMZ is primarily implemented to secure an internal network from interaction with and exploitation and access by external nodes and networks.

Advanced Networking > DMZ

DeMilitarized Zone

Enable :	<input checked="" type="checkbox"/>
Local IP Address :	<input type="text" value="192.168.11.100"/>
Exclude Remote Web Access :	<input type="checkbox"/>

Enable: option to enable the DMZ function.

Local IP Address: the local destination that all the external data traffic will be passed to.

Exclude Remote Web Access: Option to exclude the remote access to the web GUI of the router from the DMZ function.

Port Forwarding

Port forwarding, or port mapping is a network application that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

A port forwarding rule contains protocol, source IP/port, and destination IP/port. Up to 20 rules can be set up in the router.

Advanced Networking > Port Forwarding

Inbound Port Forwarding

Protocol :	TCP ▾
Source IP Address :	Any ▾
Source Port :	1 - 65535
Destination IP Address :	0.0.0.0
Destination Port :	1 - 65535
Add+	

Protocol: the IP protocol allowed for the port forwarding rule. Can be TCP, UDP, or both.

Source IP Address: the source IP address of the communication request. Can be any or a specific IP address.

Source Port: the port number used in the communication request from the source.

Destination IP Address: the local destination for the communication request to be redirected to.

Destination Port: the destination port number for the communication request to be redirected to.

Security

The Universal Hub offers comprehensive security settings that allow users to have broad control over incoming or outgoing IP traffics. The features include firewall related functions such as Anti-DoS, Access Control List and IP Traffic Filtering.


The security features provided by the device are grouped into four menu sections: Firewall, Service List, Access Rules List, and Content Filtering.

Firewall


The Firewall page provides settings for Anti-DoS and ICMP Controls.

Advanced Networking > Security > Firewall

Anti DoS

Activate : 

Drop Remote Access

ICMP Response : 

Anti DoS: Option to activate Anti-DoS function. When in use, TCP SYN packets, TCP/UDP New Connections and ICMP requested can be filtered to avoid DoS attacks.

Drop Remote Access: option to restrict certain access over the WAN(Internet). Currently supports restrictions for ICMP (Ping) response.

Service List

This Service List allows user to set up a list of IP services using TCP and/or UDP that need to be controlled via the Security Access Rules. Users can define the service name, protocol(s) to be used, and the port number(s).

Add Service

Service Name :

Protocol : BOTH ▼

Port Range : 0 to 0

[Add+](#)

Service Name: the name of the service to be defined.

Protocol: the IP protocol to be used for the service, currently supports TCP and/or UDP.

Port Range: the port range used by the service. If only one port is used, put the same port number in the range fields.

Once defined, the service will be added to a table that shows all the services that have been set up in the device as below.

Service Table

No.	Prot.	Port	Service Name	Delete
1	BOTH	1:65535	All traffic	
2	UDP	53	DNS	Del
3	TCP	80	HTTP	Del
4	TCP	443	HTTPS	Del
5	UDP	161	SNMP	Del
6	TCP	1701	L2TP	Del
7	TCP	1723	PPTP	Del
8	BOTH	1194	OpenVPN	Del
9	UDP	500	IPSec	Del
10	TCP	12521	AToverIP	Del
11	BOTH	20000	DNP3	Del
12	TCP	30000	IPSTACK	Del
13	TCP	23	TELNET	Del
14	TCP	22	SSH	Del

Services that are required by the features supported by the modem have been pre-defined using the default setting values. Those services can be removed and re-added if default values need to be changed.

Access Rules List

The Access Rules are a set of rules to control the IP access via the device LAN and WAM interfaces, which is called Access Control List (ACL). Four groups of

access rule can be defined in the device: LAN to WAN, WAN to LAN, Local to WAN, and WAN to Local.

LAN to WAN: Rules that control the IP traffic from LAN devices to WAN.

WAN to LAN: Rules that control the IP traffic from WAN to LAN devices.

Local to WAN: Rules that control the device resources access of WAN.

WAN to Local: Rules that control the access of device resources from WAN.

Each rule group has its own configuration page with similar configuration set ups. A WAN to LAN configuration page is shown below:

WAN to LAN

Default Policy : Denied ▼

Add Rule

Service : All traffic[1:65535] ▼

Policy : Denied ▼

Add+

WAN to LAN Table

No.	Service	Policy	Delete
-----	---------	--------	--------

Save

Cancel

Default Policy: the group policy applied to all the IP traffic by default. For LAN to WAN and Local to WAN, the default rule is Allowed, while for WAN to LAN and WAN to Local, it is Denied.

Service: define a service that need to be controlled. The service is selected via the drop-down menu that lists all the services that pre-defined.

Policy: the policy that applies to the service selected, either Allowed or Denied. Once defined, the rule will be added to the access rules table below by clicking Add+ button.

Access Rule Table: the access rule table that lists all the rules defined for the group.

Content Filtering

The Content Filtering provides settings for restricting certain IP traffic based on the content of the IP package. Three types of content filtering are supported by the modem: Pattern, URL, and Keyword.

– Pattern

The Pattern filtering provides settings to block those IP traffic that containing certain binary patterns, either originated from WAN (Inbound) or from LAN (Outbound), in a selected service.

Advanced Networking > Security > Content Filtering

The screenshot shows the 'Pattern' tab of the 'Content Filtering' configuration page. At the top, there are three tabs: 'Pattern' (selected), 'URL', and 'Keyword'. Below the tabs is the 'Add Pattern' section, which contains three input fields: 'Service' (a dropdown menu showing 'All traffic[1:65535]'), 'Direction' (a dropdown menu showing 'Inbound'), and 'Pattern' (a text input field). An 'Add+' button is located below the 'Pattern' field. Below the 'Add Pattern' section is the 'Pattern Filtering' section, which contains a table with the following columns: 'No.', 'Service', 'Direction', 'Pattern', and 'Delete'.

No.	Service	Direction	Pattern	Delete
-----	---------	-----------	---------	--------

Service: define a service that needs to be controlled with Pattern filtering. The service is selected via the drop-down menu that lists all the services that pre-defined.

Direction: the direction of the IP traffic that needs be controlled. Either Inbound or Outbound.

Pattern: a string of binary in HEX format that is used for pattern matching.

Pattern Filtering Rule Table: multiple rules can be set up for the Pattern filtering and all the rules defined will be listed in a table.

– URL

The URL filtering provides settings for restricting access to certain internet sites by their URLs.

Advanced Networking > Security > Content Filtering

Pattern

URL

Keyword

Add URL

URL :

Add+

URL Filtering

No.	URL	Delete
-----	-----	--------

URL: the URL (Uniform Resource Locator) need to be blocked from access by the LAN devices. Once saved, the address will be listed in the URL Filtering Table.

URL Filtering Rule Table: multiple rules can be set up for the URL filtering and all the rules defined will be listed in a table.

– Keyword

The Keyword filtering provides settings for restricting access to certain internet sites by the keywords.

Advanced Networking > Security > Content Filtering

Pattern	URL	Keyword
---------	-----	----------------

Add Keyword

Keyword :	<input type="text"/>
	Add+

Keyword Filtering

No.	Keyword	Delete
-----	---------	--------

Keyword: the WAN (Internet) sites containing the defined keyword will be blocked from access by the LAN devices. Once saved, the keyword will be listed in the Keyword Filtering Table.

Keyword Filtering Rule Table: multiple rules can be set up for the Keyword filtering and all the rules defined will be listed in a table.

VPN & Tunnelling

This page allows users to configure PPTP server and PPTP client. Users can remotely access the device behind the modem using this VPN.

GRE Tunnel

GRE (Generic Routing Encapsulation) is a simple IP packet encapsulation protocol used to establish a direct, point-to-point connection between network nodes over an Internet Protocol network.

Once a GRE protocol is select for a VPN tunnel, the following set up page will be shown:

GRE Tunnel ▼

Parameters

Tunnel name :	<input type="text" value="GRETNL"/>
Remote IP Address :	<input type="text" value="172.16.0.15"/>
Remote Subnet :	<input type="text" value="192.168.0.1"/>
Remote Subnet Mask :	<input type="text" value="255.255.255.0"/>
All Traffic :	<input checked="" type="checkbox"/>
Enable NAT :	<input type="checkbox"/>

Save

Cancel

Tunnel name: a name of the tunnel used for identifying tunnels.

Remote IP Address: the WAN IP address of the remote device on the other end of the GRE tunnel.

Remote Subnet: the LAN subnet or virtual IP of the remote device, e.g. 192.168.0.1.

Remote Subnet Mask: the LAN subnet mask used by the remote device, e.g. 255.255.255.0

All Traffic: by enabling this option, all the IP traffic will be forced via this VPN tunnel.

Enable NAT: by enabling this option, ...

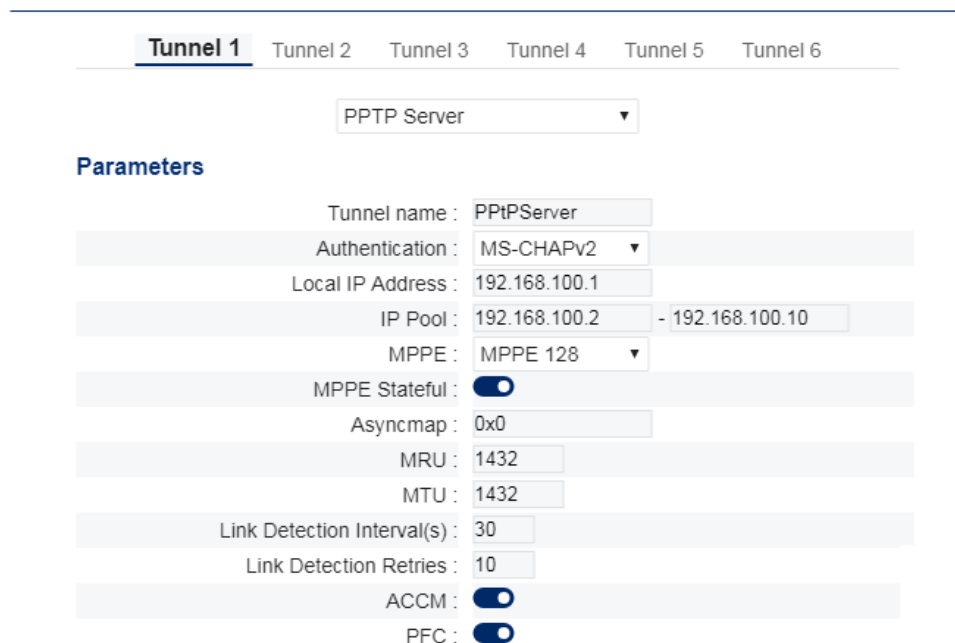
PPTP VPN

PPTP stands for Point-to-Point Tunneling Protocol, operating on TCP port 1723. It is one of the oldest VPN protocols still in use, which was developed by Microsoft to encapsulate PPP (Point-to-Point Protocol).

PPTP is an easy to use VPN protocol but is not recommended in cases where security is essential since it has serious security vulnerabilities.

PPTP Sever

The Universal Hub can be configured as a PPTP server. When PPTP Sever is selected for a VPN tunnel, the following settings will be shown:



The screenshot displays the configuration interface for a PPTP Server. At the top, there are tabs for Tunnel 1 through Tunnel 6, with Tunnel 1 currently selected. Below the tabs is a dropdown menu labeled 'PPTP Server'. Under the 'Parameters' section, the following settings are visible:

- Tunnel name : PPtPSever
- Authentication : MS-CHAPv2
- Local IP Address : 192.168.100.1
- IP Pool : 192.168.100.2 - 192.168.100.10
- MPPE : MPPE 128
- MPPE Stateful : ☒
- Asyncmap : 0x0
- MRU : 1432
- MTU : 1432
- Link Detection Interval(s) : 30
- Link Detection Retries : 10
- ACCM : ☒
- PFC : ☒

Tunnel name: a name of the tunnel used for identifying tunnels.

Authentication: the authentication method used by the PPTP VPN. The options include: PAP, CHAP, MS-CHAPv1, and MS-CHAPv2. The option cannot be left as NONE.

Local IP Address: the local IP address of the PPTP Tunnel. It has to be different from the device LAN IP, e.g. 192.168.100.1.

IP Pool: This is to define the range of IP addresses for the PPTP client(s) that connect to the sever, e.g. 192.168.100.2 – 192.168.100.10.

MPPE: Microsoft Point-to-Point Encryption (MPPE) for PPTP data. The options include NONE, MPPE 40, and MPPE 128. Default is NONE.

MPPE Stateful: to use MPPE Stateful Mode by enabling this option. Otherwise, Stateless Mode is in use. The option is disabled by default.

Asynctmap: a 32-bit Asynchronous Control Character Map for LCP control in hex format. For example, 0xffffffff will escape all control characters. Set as 0x0 by default.

ACCM: Option to enable/disable the use of Asynctmap (Asynchronous Control Character Map) setting.

MRU: Maximum Receive Unit. Use 1450 as default.

MTU: Maximum Transmission Unit. Use 1450 as default.

Link Detection Interval(s): the interval in seconds between link checks.

Link Detection Retries: the number of retries if PPTP link detection is failed. If all retries are exhausted, the device will restart the VPN tunnel.

PFC: Protocol Field Compression. Disabled by default

Client Credentials and IP Address Table: the client(s) to connect need to be set up with log in credentials and their associated IP addresses. Up to 10 clients can be added.

Assign IP address		User Name	Password	Add
<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
No.	IP Address	User Name	Password	Delete
1	192.168.100.3	user	*****	<input type="button" value="Del"/>
2	192.168.100.4	user4	*****	<input type="button" value="Del"/>

The client will be assigned with the IP address that is associated with the login credential.

PPTP Client

If the Universal Hub needs to be as a PPTP client, the PPTP client protocol needs to be selected for a VPN tunnel and the following settings will be shown:

The screenshot shows the configuration interface for a PPTP Client. At the top, there are tabs for Tunnel 1, Tunnel 2 (selected), Tunnel 3, Tunnel 4, Tunnel 5, and Tunnel 6. Below the tabs is a dropdown menu set to 'PPTP Client'. Under the 'Parameters' section, the following settings are visible:

- Tunnel name : PPTPClient
- User name : test
- Password :
- Remote IP Address : 172.16.0.15
- Authentication : MS-CHAPv2
- All Traffic : ☐
- MPPE : MPPE 128
- MPPE Stateful : ☒
- Asyncmap : 0x0
- MRU : 1450
- MTU : 1450
- Link Detection Interval(s) : 30
- Link Detection Retries : 10
- ACCM : ☒
- PFC : ☒

At the bottom, there are 'Save' and 'Cancel' buttons.

Tunnel name: a name of the tunnel used for identifying the tunnels.

User name / Password: the log in credentials set by the PPTP server.

Remote IP Address: The IP address or URL of the PPTP server.

Authentication: the authentication method used by the PPTP server.

All Traffic: by enabling this option, all the IP traffic will be forced via this VPN tunnel.

MPPE: Microsoft Point-to-Point Encryption (MPPE) for PPTP data. Must use the option that matches the PPTP server setting.

MPPE Stateful: to use MPPE Stateful Mode by enabling this option. Otherwise, Stateless Mode is in use. Must use the option that matches the PPTP server setting.

Asyncmap: a 32-bit Asynchronous Control Character Map for LCP control in hex format. For example, 0xffffffff will escape all control characters. Must use the option that matches the PPTP server setting.

ACCM: Option to enable/disable the use of Asyncmap (Asynchronous Control Character Map) setting. Must use the option that matches the PPTP server setting.

MRU: Maximum Receive Unit. Use 1450 as default.

MTU: Maximum Transmission Unit. Use 1450 as default.

Link Detection Interval(s): the interval in seconds between link checks

Link Detection Retries: the number of retries if PPTP link detection is failed. If all retries are exhausted, the device will restart the VPN tunnel.

PFC: Protocol Field Compression. Must use the option that matches the PPTP server setting.

L2TP VPN

Layer Two Tunneling Protocol (L2TP) is an extension of the PPTP protocol used to enable a virtual private network (VPN) over the Internet. L2TP combines the best features of PPTP from Microsoft and L2F from Cisco Systems. The L2TP itself does not provide any encryption or confidentiality but can rely on an encryption protocol that it passes within the tunnel, such as IPSec, to provide security.

L2TP Sever

The Universal Hub can be configured as a L2TP server. When L2TP Sever is selected for a VPN tunnel, the following settings will be shown:

L2TP Server ▼

Parameters

Tunnel name :	l2tps1	
Authentication :	CHAP ▼	
Local IP Address :	10.2.0.1	
IP Pool :	10.2.0.10	- 10.2.0.20
Port :	1701	
Asyncmap :	0x0	
MRU :	1500	
MTU :	1500	
Link Detection Interval(s) :	30	
Link Detection Retries :	5	
ACCM :	<input type="checkbox"/>	
PFC :	<input type="checkbox"/>	

Tunnel name: a name of the tunnel used for identifying tunnels.

Authentication: the authentication method used by the L2TP VPN. The options include: PAP, CHAP, MS-CHAPv1, and MS-CHAPv2. The option cannot be left as NONE.

Local IP Address: the local IP address of the L2TP Tunnel. It has to be different from the device LAN IP, e.g. 10.2.0.1.

IP Pool: This is to define the range of IP addresses for the L2TP client(s) that connect to the sever, e.g. 10.2.0.10 – 10.2.0.20.

Port: the UDP port used by the L2TP VPN. The port 1701 is the commonly used one for L2TP VPN.

Asynccmap: a 32-bit Asynchronous Control Character Map for LCP control in hex format. For example, 0xffffffff will escape all control characters. Set as 0x0 by default.

ACCM: Option to enable/disable the use of Asynccmap (Asynchronous Control Character Map) setting.

MRU: Maximum Receive Unit. Use 1450 as default.

MTU: Maximum Transmission Unit. Use 1450 as default.

Link Detection Interval(s): the interval in seconds between link checks.

Link Detection Retries: the number of retries if PPTP link detection is failed. If all retries are exhausted, the device will restart the VPN tunnel.

PFC: Protocol Field Compression. Disabled by default.

Client Credentials and IP Address Table: the client(s) to connect need to be set up with log in credentials and their associated IP addresses. Up to 10 clients can be added.

Assign IP address		User Name	Password	Add
<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
No.	IP Address	User Name	Password	Delete
1	10.2.0.10	user1	*****	<input type="button" value="Del"/>
2	10.2.0.11	user2	*****	<input type="button" value="Del"/>
3	10.2.0.13	luser3	*****	<input type="button" value="Del"/>
4	10.2.0.14	user4	*****	<input type="button" value="Del"/>
5	10.2.0.15	luser5	*****	<input type="button" value="Del"/>

L2TP Client

If the Universal Hub needs to be as a L2TP client, the L2TP client protocol needs to be selected for a VPN tunnel and the following settings will be shown:

L2TP Client ▼

Parameters

Tunnel name :	<input type="text" value="l2tpc1"/>
User name :	<input type="text" value="user1"/>
Password :	<input type="password" value="....."/>
Remote IP Address :	<input type="text" value="maxon01.dynu.net"/>
Authentication :	<div>CHAP ▼</div>
All Traffic :	<input checked="" type="checkbox"/>
Port :	<input type="text" value="1701"/>
Asyncmap :	<input type="text" value="0x0"/>
MRU :	<input type="text" value="1500"/>
MTU :	<input type="text" value="1500"/>
Link Detection Interval(s) :	<input type="text" value="30"/>
Link Detection Retries :	<input type="text" value="3"/>
ACCM :	<input checked="" type="checkbox"/>
PFC :	<input checked="" type="checkbox"/>

Tunnel name: a name of the tunnel used for identifying tunnels.

User name / Password: the log in credentials set by the L2TP server.

Remote IP Address: The IP address or URL of the L2TP server.

Authentication: the authentication method used by the L2TP server.

All Traffic: by enabling this option, all the IP traffic will be forced via this VPN tunnel.

Port: the UDP port used by the L2TP server. The port 1701 is the commonly used one for L2TP VPN.

Asyncmap: a 32-bit Asynchronous Control Character Map for LCP control in hex format. For example, 0xffffffff will escape all control characters. Set as 0x0 by default.

ACCM: Option to enable/disable the use of Asyncmap (Asynchronous Control Character Map) setting.

MRU: Maximum Receive Unit. Use 1450 as default.

MTU: Maximum Transmission Unit. Use 1450 as default.

Link Detection Interval(s): the interval in seconds between link checks.

Link Detection Retries: the number of retries if PPTP link detection is failed. If all retries are exhausted, the device will restart the VPN tunnel.

PFC: Protocol Field Compression. Disabled by default.

IPSec: the encryption protocol used by the L2TP VPN server. If selected, an IPSec tunnel matching the server settings must be configured and selected here. By default, no IPSec is in use.

IPSec

IPSec (Internet Protocol Security) is a set of protocols that provides security for Internet Protocol, through authentication and encryption of IP network packets.

Site-to-Site IPSec VPN

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g. offices or branches). The Universal Hub can be configured as a router for an IPSec Site to Site VPN. To do this, go to Advanced Networking -> IPSec settings and select Site to Site Gateway for one of the IPSec tunnels if used as a server, or Site to Site Client if as a client.

When the tunnel is selected as a gateway, the following settings will be shown:

The screenshot shows the configuration interface for IPSec 1. It has tabs for IPSec 1, IPSec 2, and IPSec 3. The 'Basic' section includes fields for Number (0), Mode (Site to Site Gateway), and Name (IPSecS2SG). The 'Local Group' section includes (USER) FQDN (Local), Security Type (Subnet), IP Address (192.168.0.1), and Subnet Mask (255.255.255.0). The 'Remote Group' section includes (USER) FQDN (Remote), Security Type (Subnet), IP Address (192.168.11.1), and Subnet Mask (255.255.255.0). The 'IPSec' section includes Preshared Key (masked), Aggressive Mode (disabled), IKE DH Group (1024 bits), IKE Encryption (AES_CBC), IKE Hash (SHA2 256), ESP Encryption (AES 128), ESP Authentication (MMAC SHA2 256), and Perfect Forward Secrecy (disabled).

IPSec 1	
Basic	
Number :	0
Mode :	Site to Site Gateway ▼
Name :	IPSecS2SG
Local Group	
(USER) FQDN :	Local
Security Type :	Subnet ▼
IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
Remote Group	
(USER) FQDN :	Remote
Security Type :	Subnet ▼
IP Address :	192.168.11.1
Subnet Mask :	255.255.255.0
IPSec	
Preshared Key :
Aggressive Mode :	<input type="checkbox"/>
IKE DH Group :	1024 bits ▼
IKE Encryption :	AES_CBC ▼
IKE Hash :	SHA2 256 ▼
ESP Encryption :	AES 128 ▼
ESP Authentication :	MMAC SHA2 256 ▼
Perfect Forward Secrecy :	<input type="checkbox"/>

Mode: the working modes of the IPSec Tunnel including:

Site to Site Gateway, Site to Site Client, Gateway, Client

The Site to Site Gateway/Client options are used for creating a site-to-site VPN tunnel, while the Gateway/Client are for a VPN connection between two end devices, e.g. to use along with L2TP protocol for enhanced security.

Name: a name of the tunnel used for identifying tunnels.

(USER) FQDN: a Fully Qualified Domain Name (FQDN) selected for the devices in the VPN Tunnel. Both the local and remote devices have to be set with a unique name.

Security Type: the option to define how the IP address(es) are managed within the IPsec tunnel. It can be one of the three options: Subnet, IP, or IP Range. Each option comes with its associated IP settings. Both local and remote devices have to be configured.

Preshared Key: the secret key pre-set for the IPsec Tunnel and used by both server and client.

Aggressive Mode: the VPN tunnel will use Aggressive mode instead of Main mode when enabled. Disabled by default.

IKE DH Group: the Diffie-Hellman (DH) group used in the Internet Key Exchange (IKEv2) protocol.

IKE Encryption: defines the encryption algorithm used in the IKEv2 protocol.

IKE Hash: defines the Hash function used in the IKEv2 protocol.

ESP Encryption: defines the encryption algorithm used in the Encapsulating Security Payload (ESP).

ESP Authentication: defines the cryptography function used in the ESP authentication.

Perfect Forward Secrecy: option to enable the Perfect Forward Secrecy (PFS) in the IPsec VPN. A PFS DH group will be needed if PFS is enabled.

A Site to Site Client set up is very similar to that of a Gateway, with additional setting of a Remote Server IP address.

IPSec 1	IPSec 2	IPSec 3
Basic		
Number : 0		
Mode : Site to Site Client ▼		
Name : IPSecS2SC		
Server IP : maxon01.dynu.net		
Local Group		
(USER) FQDN : Remote		
Security Type : Subnet ▼		
IP Address : 192.168.11.0		
Subnet Mask : 255.255.255.0		
Remote Group		
(USER) FQDN : Local		
Security Type : Subnet ▼		
IP Address : 192.168.0.1		
Subnet Mask : 255.255.255.0		
IPSec		
Preshared Key :		
Aggressive Mode : <input type="checkbox"/>		
IKE DH Group : 1024 bits ▼		
IKE Encryption : AES_CBC ▼		
IKE Hash : SHA2 256 ▼		
ESP Encryption : AES 128 ▼		
ESP Authentication : MMAC SHA2 256 ▼		
Perfect Forward Secrecy : <input type="checkbox"/>		

All the client settings must match those used in the gateway (server), such as FQDN, Security Types, Keys, and Encryption Functions.

L2TP/IPSec

Since L2TP itself does not provide any encryption or confidentiality, IPSec encryption can be used to secure the data packet that passes within the tunnel, which is call L2TP/IPSec.

To set up L2TP/IPSec VPN, an IPSec tunnel needs to be created for L2TP VPN, either a server or client. Go to Advanced Networking -> IPSec and select IPSec Gateway (for L2TP Server) or IPSec Client (for L2TP Client) in one of the IPSec tunnels.

For gateway settings:

The screenshot shows the configuration interface for an IPSec tunnel, specifically for 'IPSec 1'. The interface has two tabs: 'Basic' and 'IPsec'. The 'Basic' tab is active, showing the following settings:

- Number : 0
- Mode : Gateway (dropdown menu)
- Type : ☐ Tunnel ☒ Transport
- Name : IPSecG

The 'IPsec' tab is also visible, showing the following settings:

- Preshared Key :
- Aggressive Mode : ☐
- IKE DH Group : 1024 bits (dropdown menu)
- IKE Encryption : AES_CBC (dropdown menu)
- IKE Hash : SHA2 256 (dropdown menu)
- ESP Encryption : AES 128 (dropdown menu)
- ESP Authentication : MMAC SHA2 256 (dropdown menu)
- Perfect Forward Secrecy : ☒
- PFS Group : 2048 bits (dropdown menu)

Mode: the working modes of the IPSec Tunnel, must be Gateway when used with a L2TP server.

Type: the type of the IPSec tunnel - Tunnel Mode or Transport Mode. If a L2TP/IPSec client is Linux based device, Transport Mode should be used.

Name: a name of the tunnel used for identifying tunnels.

Preshared Key: the secret key pre-set for the IPSec Tunnel and used by both gateway and client.

Aggressive Mode: the VPN tunnel will use Aggressive mode instead of Main mode when enabled. Disabled by default.

IKE DH Group: the Diffie-Hellman (DH) group used in the Internet Key Exchange (IKEv2) protocol.

IKE Encryption: defines the encryption algorithm used in the IKEv2 protocol.

IKE Hash: defines the Hash function used in the IKEv2 protocol.

ESP Encryption: defines the encryption algorithm used in the Encapsulating Security Payload (ESP).

ESP Authentication: defines the cryptography function used in the ESP authentication.

Perfect Forward Secrecy: option to enable the Perfect Forward Secrecy (PFS) in the IPSec VPN. A PFS DH group will be needed if PFS is enabled.

For client settings:

The screenshot displays the configuration interface for IPsec 1. It is divided into two main sections: 'Basic' and 'IPSec'. The 'Basic' section includes fields for 'Number' (0), 'Mode' (Client), 'Type' (Tunnel/Transport), 'Name' (IPSecC), and 'Server IP' (maxon01.dynu.net). The 'IPSec' section includes a 'Preshared Key' field, an 'Aggressive Mode' toggle, and several dropdown menus for 'IKE DH Group' (1024 bits), 'IKE Encryption' (AES_CBC), 'IKE Hash' (SHA2 256), 'ESP Encryption' (AES 128), 'ESP Authentication' (MMAC SHA2 256), 'Perfect Forward Secrecy' (toggle), and 'PFS Group' (2048 bits).

Section	Field	Value
Basic	Number	0
	Mode	Client
	Type	Tunnel / Transport
	Name	IPSecC
	Server IP	maxon01.dynu.net
IPSec	Preshared Key
	Aggressive Mode	Off
	IKE DH Group	1024 bits
	IKE Encryption	AES_CBC
	IKE Hash	SHA2 256
	ESP Encryption	AES 128
	ESP Authentication	MMAC SHA2 256
	Perfect Forward Secrecy	On
PFS Group	2048 bits	

Mode: the working modes of the IPsec Tunnel, must be Client when used with a L2TP client.

Type: the type of the IPsec tunnel. Must be Transport Mode if the device is set up as a client, and so does the gateway in this case.

Name: a name of the tunnel used for identifying tunnels.

Server IP: The IP address or URL of the L2TP server.

Preshared Key: the secret key pre-set for the IPsec Tunnel and used by both server and client.

Aggressive Mode: the VPN tunnel will use Aggressive mode instead of Main mode when enabled. Disabled by default.

IKE DH Group: the Diffie-Hellman (DH) group used in the Internet Key Exchange (IKEv2) protocol.

IKE Encryption: defines the encryption algorithm used in the IKEv2 protocol.

IKE Hash: defines the Hash function used in the IKEv2 protocol.

ESP Encryption: defines the encryption algorithm used in the Encapsulating Security Payload (ESP).

ESP Authentication: defines the cryptography function used in the ESP authentication.

Perfect Forward Secrecy: option to enable the Perfect Forward Secrecy (PFS) in the IPsec VPN. A PFS DH group will be needed if PFS is enabled.

No specific setups are required for L2TP VPN server or client for it to operate properly once the IPsec is setup correctly.

OPENVPN

OpenVPN is an open-source implementation of Virtual Private Network (VPN) for creating a secure point-to-point or site-to-site connections. The project was started by James Yonan and is published under the GNU General Public License (GPL). The OpenVPN in Universal Hub utilises certificate-based authentication.

OpenVPN Server

The Universal Hub can be configured as an OpenVPN server. When OpenVPN Sever is selected for a VPN tunnel, the following settings will be shown:

Tunnel 1

Tunnel 2

Tunnel 3

Tunnel 4

Tunnel 5

Tunnel 6

OpenVPN Server ▼

Parameters

Tunnel Name :	ovpns1
Protocol :	TCP ▼
Port :	1194
Interface :	tun ▼
OpenVPN Auth :	X.509 cert ▼
Virtual IP :	10.7.0.0
Virtual Netmask :	255.255.255.0
Client Subnet :	192.168.0.0
Client Subnet Mask :	255.255.255.0
Renegotiation Interval(s):	60
Max Clients:	5
Enable Default Gateway :	<input type="checkbox"/>
Enable NAT :	<input type="checkbox"/>
Ping Interval Seconds :	10
Ping Timeout Seconds :	60
Compression :	LZO ▼
Encryption :	AES-256-CBC ▼
Hash :	SHA1 ▼
MTU :	1500
Max Frame Size :	1500
Expert Options :	
Enable Client to Client :	<input checked="" type="checkbox"/>
Enable Dup Client :	<input checked="" type="checkbox"/>
Certificates :	X.509 2 ▼

Tunnel Name: a name of the tunnel used for identifying tunnels.

Protocol: the IP protocol used for the OpenVPN tunnel, either UDP or TCP.

Port: the port number used for the VPN tunnel. 1194 is the default port number used for the OpenVPN.

Interface: the interface of the tunnel, either TUN (routing device) or TAP (bridging device).

OpenVPN Auth: the authentication method used by the OpenVPN. Currently only supports X.509 certificates.

Virtual IP: the virtual IP subnet of the VPN tunnel.

Virtual Netmask: the IP netmask of the tunnel.

Client Subnet: the subnet of the OpenVPN client LAN.

Client Subnet Mask: the IP netmask of the OpenVPN client LAN.

Renegotiation Interval (s): the interval in seconds for the server to periodically renegotiate the session key.

Max Clients: the maximum number of clients that can connect.

Enable Default Gateway: option to force the router using the VPN server as its default gateway.

Enable NAT: option to enable

Ping Interval (s): the interval in seconds for the periodical tunnel connection check using ICMP.

Ping Timeout (s): the timeout in seconds for every PING response. The values must be at least 2 times longer than Ping Interval.

Compression: option for packet compression, either NONE or LZO.

Encryption: defines the encryption algorithm used for the VPN.

Hash: defines the Hash function used in the VPN.

MTU: defines the Maximum Transmission Unit. Use 1500 as default.

Max Frame Size: defines the Maximum Frame Size for transmission. Use 1500 as default.

Expert Options: extra PPP initialization strings that may be useful. Multiple strings can be separated by a space. Default is Null. Valid strings include:

nodeflate, nobsdcomp, novj, novjccomp, noccip

Enable Client to Client: option to enable communications between clients within the VPN tunnel.

Enable Dup Client: option to allow clients to use duplicate certificates with the VPN tunnel.

Certificate: define the set of X.509 certificates to be used for the VPN. The certificates are set up in the X.509 settings page.

OpenVPN Client

If the Universal Hub is to be an OpenVPN client, OpenVPN Client needs to be selected for a VPN tunnel and the following settings will be shown:

The screenshot shows the configuration interface for an OpenVPN client, specifically for Tunnel 2. At the top, there are tabs for Tunnel 1, Tunnel 2 (selected), Tunnel 3, Tunnel 4, Tunnel 5, and Tunnel 6. Below the tabs is a dropdown menu set to 'PPTP Client'. Under the 'Parameters' section, the following settings are visible:

- Tunnel name : PPTPClient
- User name : test
- Password : ****
- Remote IP Address : 172.16.0.15
- Authentication : MS-CHAPv2
- All Traffic : ☐
- MPPE : MPPE 128
- MPPE Stateful : ☒
- Asyncmap : 0x0
- MRU : 1450
- MTU : 1450
- Link Detection Interval(s) : 30
- Link Detection Retries : 10
- ACCM : ☒
- PFC : ☒

Tunnel Name: a name of the tunnel used for identifying tunnels.

Protocol: the IP protocol used for the OpenVPN tunnel, either UDP or TCP.

Port: the port number used for the VPN tunnel. 1194 is the default port number used for the OpenVPN.

Interface: the interface of the tunnel, either TUN or TAP that is used by the OpenVPN server.

OpenVPN Auth: the authentication method used by the OpenVPN. Currently only supports X.509 certificates.

Remote IP: the IP or URL of the OpenVPN server.

Enable NAT: option to enable

Ping Interval (s): the interval in seconds for the periodical tunnel connection check using ICMP

Ping Timeout (s): the timeout in seconds for every PING response. The values must be at least 2 times longer than Ping Interval.

Compression: option for packet compression. Must match the option used in the server.

Encryption: defines the encryption algorithm used in the OpenVPN server.

Hash: defines the Hash function used in the OpenVPN server.

MTU: defines the Maximum Transmission Unit. Use 1500 as default.

Max Frame Size: defines the Maximum Frame Size for transmission. Use 1500 as default.

Expert Options: extra PPP initialization strings that may be useful. Multiple strings can be separated by a space. Default is Null. Valid strings include:

nodeflate, nobsdcomp, novj, novjccomp, noccip

Certificate: define the set of X.509 certificates to be used for the VPN. The certificates are set up in the X.509 settings page.

X.509

An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate. Universal Hub uses X.509 certificates as its OpenVPN authentication method. A set of X.509 certificates must be set up correctly for the OpenVPN service to be working properly.

All the necessary certificate and key files must be generated in advance. The easiest way to achieve this is to use Easy-RSA software tool, which is available in both Linux and Windows OS (users can search online or refer to relevant RFI/Maxon Application Notes for more details).

The files request by an OpenVPN server include:

- ca.crt
- dh2048.pem
- server.crt,
- server.key
- ta.key - only required if TLS protocol is in use

The certificates for an OpenVPN client must be created based on the server CA and the files include:

- ca.crt
- client.crt,
- client.key
- ta.key - only required for TLS protocol is in use

Certificate Revocation Lists (CRL) can also be part of certificates but is optional.

Once all the files are generated properly, they can be imported into the device via the X.509 set up page. Maximum 10 set of certificates can be imported into the router and each of them can be used by one of the OpenVPN tunnel depending on its VPN type (server or client).

Advanced Networking > X.509

Add

Number :	1	
Title :	CA certificate	
	<input type="button" value="Choose file"/> No file chosen	<input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Delete"/>

X.509 List

No.	CA	Cert	Key	CRL	DH	TLS-Auth
1	OK	OK	OK	-	-	OK
2	OK	OK	OK	-	OK	OK
3	OK	OK	OK	-	-	OK
4	-	-	-	-	-	-
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-	-	-	-
10	-	-	-	-	-	-

The imported certificates can also be exported for backup or other devices if required.

VRRP

The Virtual Router Redundancy Protocol (VRRP) is a networking protocol to provide enhanced availability and reliability of routing paths via automatic default gateway selections from a set of routers in an IP subnetwork.

Advanced Networking > VRRP

Virtual Router Redundancy Protocol	
Enable :	<input checked="" type="checkbox"/>
Group ID :	<input type="text" value="1"/>
Priority :	<input type="text" value="100"/>
Interval :	<input type="text" value="10"/>
Virtual IP :	<input type="text" value="192.168.0.1"/>

Enable: option to activate the VRRP protocol in the router.

Group ID: specify the VRRP group the router belongs to.

Priority: the priority of the router within the VRRP group. Valid from 1 to 255. The larger value has the higher priority.

Interval: the interval in seconds at which the master router (with the highest priority) sends keepalive packets to the backup routers.

Virtual IP: a Virtual IP address shared among the VRRP group routers as the gateway IP in the LAN. A router with the same LAN IP as the virtual IP is the master router and the rest are backups. In case the master fails, the virtual IP address is mapped to a backup router's IP address according to its priority and this backup router becomes the gateway.

SNMP

Simple Network Management Protocol (SNMP) is a set of protocols for network management and monitoring and used for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour.

The device behaviour that can be changed via SNMP protocol currently includes digital output status, active SIM card, and device reset.

Simple Network Management Protocol

Enable :	<input checked="" type="checkbox"/>
System Name :	<input type="text" value="RF Industries"/>
Read Community Name :	<input type="text" value="public"/>
Write Community Name :	<input type="text" value="private"/>
System Contract :	<input type="text" value="support@rfi.com.au"/>
Trap 1st Server IP :	<input type="text" value="192.168.0.20"/>
Trap 2nd Server IP :	<input type="text" value="192.168.0.21"/>
Trap 3rd Server IP :	<input type="text" value="192.168.0.22"/>
Version 3 :	<input type="checkbox"/>

Enable: option to activate the SNMP function in the router.

System Name: the system name of the router.

Read Community Name: the public community name for read-only.

Write Community Name: the private community name for read and write.

System Contact: the contact information of the router.

Trap Server IP: the SNMP trap server's IP address. Up to three trap servers can be set in the router.

Version 3: option to enable the SNMP v3 support.

MIB file: the MIB (Management Information Base) file is built-in and can be retrieved by clicking the "MIB" button and save the content to a file.

DEVICE MANAGEMENT

The Device Management settings provide configurations for the router itself, including management of device access, user account, system clock, debug tools, and firmware upgrade.

System

The system settings provide configurations for the device access controls.

System

The System settings manages the device access via the LAN or WAN interfaces and reboot scheduling.

System

User Management

Device Access

HTTP :

☒

80

HTTPS :

☐

SSH Terminal :

☐

Telnet Terminal :

☒

23

AT over IP :

☒

12521

AT over IP Auth :

☒

Signal Log

Active :

☒

Device Reboot

Reboot :

☒ Periodic ☐ Scheduled

Periodic Reboot :

24

hours

Scheduled Reboot :

59 23 * * *

HTTP: option to allow device access via HTTP protocol. Default port is 80 and customisable.

HTTPS: option to allow device access via HTTPS protocol. Default port is 443 and customisable.

SSH Terminal: option to allow device access via SSH protocol.

Telnet Terminal: option to allow device access via Telnet protocol. Default port is 23 and customisable.

AT over IP: option to allow AT over IP via TCP protocol. Username and password are required to access the function. Default port is 12521 and customisable.

AT over IP Auth: the option to enable/disable authentication to access AT over IP function.

Signal Log: option to allow cellular signal strength logging. When enabled, the RSSI value will be logged with timestamp in case of level changes. The log can be downloaded from the System Log page.

Periodic Reboot: the settings for the device to perform a periodic reboot at a pre-defined interval (0 – 26 hours). "0" means periodic reboot is disabled.

Scheduled Reboot: the settings for the device to perform a reboot on a specific time defined by a Cron expression in a format of:

Minute Hour DayofMonth Month DayofWeek.

For example, to make the device to reboot at 11:59PM every Sunday, the Cron expression should be: 59 23 * * 7

User Management

The User Management provides account settings for device access via Web GUI and other management interfaces, such as Telnet/SSH.

Device Management > System

System	User Management
--------	------------------------

User Management

Current User Name :	<input type="text"/>
Current User Password :	<input type="password"/>
New User Name :	<input type="text"/>
New User Password :	<input type="password"/>
Confirm New User Password :	<input type="password"/>

Both username and password can be configured with correct entries of current login credentials. It is strongly recommended that users change the default login credentials, at least the password, before deploying the device in the field to avoid security risks.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management. Universal Hub has built-in RADIUS client function to allow the device using AAA from a remote RADIUS server.

Device Management > RADIUS

Server	
Activate :	<input checked="" type="checkbox"/>
NAS ID :	MA-2080
Primary :	172.16.0.9
Secondary :	
Port Number :	1812
Shared Secret :	*****
Timeout :	3 Seconds

Activate: option to enable the RADIUS client function.

NAS ID: the NAS identifier for the device.

Primary: the IP/URL of the primary RADIUS sever.

Secondary: the IP/URL of the secondary RADIUS sever. Leave blank if not used.

Port Number: the port number used for RADIUS protocol and 1812 is the default port defined by RFC2865.

Shared Secret: the password for client to connecting the RADIUS sever.

Timeout: the timeout limit in seconds when negotiating with the RADIUS server. Valid range is 1 to 60 seconds.

Backup / Profiles

Backup / Profiles settings provide device configuration backup and restore function, as well as factory default reset.

System > Backup / Profiles

Save Settings to File :	Backup		
Load Settings from File :	Choose File	No f...osen	Restore
Restore to Factory Default :	Reset		
Load Profile Setting :	1	2	3
Set Profile Settings :	1	2	3

Save Settings to File: option to save the current device configuration to an encrypted binary file. Note that the X.509 certificates saved in the device will not be saved into backup file. Users need to save them separately if required.

Load Settings from File: option to load a device configuration from a previously save file. Device will automatically reboot after loading for the new settings to take effect.

Restore to Factory Default: option to restore the device to its factory default configuration. The device will automatically reboot after loading the default settings.

Load Profile Setting: the device can store three (3) profiles locally. User can load the pre-saved profile by clicking the numbered button. Device will automatically reboot after loading for the new settings to take effect.

Set Profile Settings: save the current settings to one of the three local stored profiles by clicking the numbered button. The existing X.509 certificates will be saved to profile as well. It is recommended to take down notes for each profile for future reference.

Clock

The Clock settings is to control the real time clock source in the router.

Clock Setting

Time Sync :	Cellular Network ▼
NTP Server :	au.pool.ntp.org
Time Zone :	Australia/Sydney ▼
Current Date & Time :	2019 / 9 / 25 (yyyy/mm/dd) 12 : 11 : 31 (hh:mm:ss)
Get PC time :	<input type="button" value="Sync"/>

Time Sync: option to specify the source that the router uses to synchronise its internal system clock. The source can be Cellular Network, NTP Server, or Manually Input.

NTP Server: the IP/URL of the NTP server if using NTP server for clock source.

Time Zone: option to specify the time zone the router is located.

Current Date & Time: The current date & time information. User can also manually enter a time here if Time Sync is set to Manual.

Get PC Time: the device can be synchronised with a connected PC by click the Sync button when Time Sync is set to Manual.

Ping Tool

The Ping Tool page provides the ping check function over the Web interface for some debugging purposes.

Device Management > Ping Tool

Ping

IP Address/Host Name :

More useful debugging tools may be available in further firmware releases.

System Logs

The System Logs page allow users to config device logs for diagnostic purposes. The device logs are stored locally and can be pushed to the remote server by either syslog protocol or FTP.

Syslog

The Syslog displays the current system logs that may be helpful for some trouble shooting. The logs can be downloaded locally via the download button. There are also settings for remote syslog function.

Enable Logs: option to enable the System log functions. Enabled by default.

Remote Syslog: option to activate the remote syslog function. Disabled by default.

Server Address: the IP/URL of the remote syslog server.

X.509: the CA certificate (ca.crt) to be used for secured Syslog server and is defined in the X.509 Configuration under Advanced Networking. Disabled by default.

Download Syslog: Click the button to download the device system log as a ZIP file.

Download RSSI Log: Click the button to download the device RSSI log.

Syslog

Enable : ☒Remote Syslog : ☐

Server Address :

x509 :

Apply

```

,,,,,,N*53\n"}
2020-01-15T16:10:32.405238+11:00 Modular Modem root: sh /etc/init.d/log_signal.sh 71 59
115 &
2020-01-15T16:10:54.650721+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/status, {"uptime": "0day : 3h : 22m : 33s\n", "modem_firmware_version":
"MMdm-1.2.2 [202001140521]\n", "system_time": "1579065054\n", "signal_level_n": -69,
"network_registration": "Telstra", "battery_value_n": 13.366711984940387, "area_info":
"LAI(50501), LAC(2064), CellID(07f31117)\n", "temperature_n": 37.221476957755293}
2020-01-15T16:10:54.719996+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/wan, {"ip_address": "172.16.0.22", "sent_packets": 1671337,
"received_packets": 1424618}
2020-01-15T16:10:54.720179+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/io, {"digital_input/1/value": false, "digital_input/2/value": false,
"digital_output/1/value": false, "digital_output/2/value": false}
2020-01-15T16:10:54.819514+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/firmware, {}
2020-01-15T16:10:55.141718+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/gps, {"nmea_sentence": "$GPRMC,V,,,,,,,,,N*53\n"}
2020-01-15T16:11:12.312128+11:00 Modular Modem root: sh /etc/init.d/log_signal.sh 65 59
115 &
2020-01-15T16:11:22.503260+11:00 Modular Modem root: sh /etc/init.d/log_signal.sh 71 59
115 &
2020-01-15T16:11:25.214594+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/status, {"uptime": "0day : 3h : 23m : 3s\n", "modem_firmware_version":
"MMdm-1.2.2 [202001140521]\n", "system_time": "1579065085\n", "signal_level_n": -69,
"network_registration": "Telstra", "battery_value_n": 13.415734156034301, "area_info":
"LAI(50501), LAC(2064), CellID(07f31117)\n", "temperature_n": 37.221476957755293}
2020-01-15T16:11:25.246912+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/wan, {"ip_address": "172.16.0.22", "sent_packets": 1673727,
"received_packets": 1427409}
2020-01-15T16:11:25.247095+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/io, {"digital_input/1/value": false, "digital_input/2/value": false,
"digital_output/1/value": false, "digital_output/2/value": false}
2020-01-15T16:11:25.319758+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/firmware, {}
2020-01-15T16:11:25.622706+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/gps, {"nmea_sentence": "$GPRMC,V,,,,,,,,,N*53\n"}
2020-01-15T16:11:55.688837+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/status, {"uptime": "0day : 3h : 23m : 34s\n", "modem_firmware_version":
"MMdm-1.2.2 [202001140521]\n", "system_time": "1579065115\n", "signal_level_n": -69,
"network_registration": "Telstra", "battery_value_n": 13.464756327128217, "area_info":
"LAI(50501), LAC(2064), CellID(07f31117)\n", "temperature_n": 37.14077262830974}
2020-01-15T16:11:55.721766+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/wan, {"ip_address": "172.16.0.22", "sent_packets": 1675964,
"received_packets": 1430359}
2020-01-15T16:11:55.721949+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/io, {"digital_input/1/value": false, "digital_input/2/value": false,
"digital_output/1/value": false, "digital_output/2/value": false}
2020-01-15T16:11:55.862025+11:00 Modular Modem publisher: sending mosquitto topic & msg:
359075063478696/d/firmware, {}
2020-01-15T16:11:56.103100+11:00 Modular Modem publisher: sending mosquitto topic & msg:

```

Refresh

Download Syslog

Download Sysnal Log

FTP

The FTP settings under Syslog allow users to set up FTP client function to regularly push the system logs to a remote FTP server.

Activate: option to enable the FTP client function for system logs. Disabled by default.

Schedule: the FTP upload scheduling set up using a Cron expression in a format of:

Minute Hour DayofMonth Month DayofWeek..

Secure: the option to enable SSH-FTP protocol.

Server Address: the IP address or URL of the remote FTP server.

Server Port: the port number used for the FTP server.

User Name/ User Password: the log in credentials for the FTP server.

Syslog

FTP

FTP Upload

Activate :	<input checked="" type="checkbox"/>
Scheduled :	10 * * * *
Secure :	<input type="checkbox"/>
Server Address :	172.16.0.9
Server Port :	21
User Name :	maxon
User Password :	*****

Apply

Firmware Upgrade

The Firmware Upgrade page is used for upgrading the router firmware via LAN or WAN interface.

Device Management > Firmware Upgrade

Choose F/W

When “Choose F/W” is clicked, the Web GUI will pop up windows asking for the binary firmware image (.BIN file). Once selected, the router will upload the file into its internal memory and perform firmware upgrade.

Device Management > Firmware Upgrade

MMdm-1.1.1[201903120047].bin

Upload

Cancel

25% uploaded

The router will start internal reflash process once upload successfully. It will take at least 3 minutes and then the device will reboot itself and come back operating with the new firmware in place.

Device Management > Firmware Upgrade

MMdm-1.1.1[201903120047].bin

Upload

Cancel

Unit will automatically reboot in 144.3 seconds

REBOOT / LOGOUT

Two buttons are provided in the router Web GUI for quit the user interface or manually reboot the device.

Universal-Hub Wireless Router

Model No. MA-2080XX

Status > Overview

Device

System Time : 2019-03-12 11:53:25
Up Time : 0day : 1h : 18m : 44s
Device FW Version : MMdm-1.1.1 [201903060239]
Module MAC : 950075000470000

[Logout](#)[Reboot](#)

Logged in as: admin

SMS COMMANDS

Universal Hub provides a comprehensive SMS command set for user to easily carry out remote diagnostics and some important settings. Follow are the list of SMS commands that are currently built-in.

- **WAN Status**

Syntax:

RFIM.SMS.WANIP

Return:

siteID,SIM-x IP-x.x.x.x APN-xxxxxxx ID-xxxxxxx Auth-PAP Reg-1 Sig-xx

- **SIM Switch**

Syntax:

RFIM.SMS.SIMSWITCH <SIM No.>

<SIM No.>: 0 or 1

Return:

SIM SWITCH TO SIM<SIM No.>

- **Reboot**

Syntax:

RFIM.SMS.REBOOT

Return:

siteID,REBOOTING

- **Restore Factory Default Settings**

Syntax:

RFIM.SMS.FACTORY

Return:

siteID,FACTORY DEFAULT and REBOOTING

– **I/O and Analogue Status**

SMS Syntax:

RFIM.SMS.IOSTATUS

Return:

siteID,IN0-stat,IN1-state,OUT0-stat,OUT1-stat,BT-xx.xx,BV-xx.xx,MT-xx.xx, P0-xxxx, P1-xxxx

IN0, IN1: INPUT

OUT1, OUT1: OUTPUT

BT: Board temperature

BV: Board supply voltage

MT: Module temperature

P0, P1: Pulse counter (only when function configured)

– **Signal Strength (RSSI)**

Syntax:

RFIM.SMS.RSSI

Return:

RSSI -xxdBm(xx)

– **Last Data received via Serial Port**

SMS Syntax:

RFIM.SMS.SERIAL

Return:

Last messages received from serial port.

– **APN setting**

SMS Syntax:

RFIM.SMS.APN=SIM-<SIM No.>,APN-<APNname>,AUTH-<Authentication>,ID-<Username>,PASSWD-<Password>

<SIM No.>: 1 or 2

<Authentication>: 0 – None, 1- PAP, 2 - CHAP

Return:

siteID,SIM-<SIMNo.>,APN-<APNname>,AUTH-<Authentication>,ID-<Username>,PASSWD-****

– **Current GNSS data**

Syntax:

RFIM.SMS.GNSS

Return:

<SatelliteNumber>,Degree,minutes,seconds,<NORTH/SOURTH>,
Degree,minutes,seconds,<EAST/WEST>

or

LOCATION NOT FIXED

– **SIM Data Usage Check (in future release)**

Syntax:

RFIM.SMS.SIMUSAGE <SIM No.>

Return:

SIM <SIM No.> DATA UL-xxx, DL-xxx, TOL-xxx

– **SIM Data Usage Clear**

Syntax:

RFIM.SMS.CLEARUSAGE <SIM No.>

Return:

CLEAR SIM <SIM No.> DATA USAGE

– **WAN Connect / Disconnect**

Syntax:

RFIM.SMS.WANCONNECT

RFIM.SMS.WANDISCONNECT

Return:

No message return for the commands. Instead, user can use SMS settings for notifications.

Please note that, after the SMS command, the WAN connection state will persist even if the modem is re-powered.

– **Input Counter Settings**

Syntax:

RFIM.SMS.COUNTER <INx.> <option> TM-<Mode>,AT-<threshold>

<INx>: 1 or 2

<Mode>: trigger mode, one of ON, OFF, or BOTH

<threshold>: counter alarm threshold.

Return:

COUNTER <INx> <DISABLE/ENABLE/CLEAR>

Examples:

RFIM.SMS.COUNTER 1 DISABLE
RFIM.SMS.COUNTER 1 ENABLE TM-BOTH,AT-9000
RFIM.SMS.COUNTER 2 CLEAR

DEVICE AT COMMAND SET

The Universal Hub supports a set of AT commands for device status and configurations via its physical serial interface or AT over IP connections.

AT Command Password Protection

When enabled, the device will be protected from changing or monitoring by any AT command unless the interface password is entered first. Otherwise, any AT command will return an "ERROR" response.

```
AT$$$SERIALPWD=<0,1>,<PWD>
```

<0, 1> : 0 - disable, 1- enable
<PWD> : set password

Once the command has been entered, a save (AT&W) and reboot (AT\$\$\$RESET) is required. To de-activate the password protection for a session, enter the following command and this will persist until the modem reboots:

```
AT$$$PWD=<PWD>
```

Query Command:

```
AT$$$SERIALPWD?
```

```
$$$SERIALPWD: 1,****  
OK
```

Device Information

– Device Information

```
ATI
```


Manufacturer: RFI Technology Solutions
Model Number: MA-2080
Product Name: UNIVERSAL-HUB
F/W Revision: MMdm-1.2.1 [201907120140]
H/W Version: 1.0
Module F/W Revision: SWI9X30C_02.24.05.06 r7040 CARMD-EV-FRMWR2
2017/05/19 06:23:09
LAI: 50502
LAC: 7EFC
Cell ID: 0BBEDAE8
IMEI: 359075063478696

OK

– **Manufacturer Information**

AT+CGMI

RF Industries Pty Ltd
OK

– **Firmware version**

AT+CGMR

+CGMR: MMdm-1.2.1 [201907120140]
OK

– **IMEI number**

AT+CGSN

359075063478696
OK

– **Device Date & Time**

AT\$\$DATE

\$\$DATE: 11/19/2019 11:18:44.854456
OK

AT+CCLK?

+CCLK: [19/11/19,12:24:10]
OK

– **Device Up Time**

AT\$\$UPTIME

\$\$UPTIME: 0day : 21h : 45m : 17s
OK

– **Device WAN IP**

AT\$\$WAN

\$\$WAN: 10.97.163.190
OK

– **Device Cellular Signal Strength**

AT\$\$RSSI

\$\$RSSI: -69
OK

AT+CSQ

+CSQ: 22,99
OK

– **Device SIM PIN Status**

AT+CPIN?

+CPIN: READY
OK

Cellular WAN Setup

AT\$\$\$WANS= <IPStack>,<APN>,<auth>,<userid>,<password>,<dialnum>,<SIMPIN>,<SIMCode>.<PReset>,<TCPListening>,<TCPConnect>,<ResetonTime>,<HH:MM>,<LCPIInterval>,<LCPFail>

<IPStack>: IP Stack Mode. 0 (Auto Mode) Only

<APN>: Access Point Name

<auth>: Network authentication 1-PAP, 2-CHAP

<userid>: Username for Cellular Network authentication

<password>: Password for Cellular Network authentication

<dianum>:

Dialup number for PPP connection under 3G network. Always put *99# here. Can't leave it blank

<SIMPIN>: Disable/Enable Auto PIN, 0 - disable, 1- enable

<SIMCode>: SIM PIN code used for auto PIN function

<PReset>:

Periodic reset schedule setting. 0 ~ 26 Hours, 0 – disable periodic reset.

<TCPListening>:

1 - allow scheduled or periodic reset only when TCP server in listening state;

0 – device reset regardless of TCP server state

<TCPConnect>:

1 - allow scheduled or periodic reset only when TCP client is not in connecting state;

0 – device reset regardless of TCP client state

<ResOnTime>: Disable (0) / Enable (1) Reset at scheduled Time

<HH:MM>: the time for scheduled reset in 24-hour format

Battery Level for Module Deregistration (12.3 volts ON, 11.9 volts OFF)

0, 1~20 LCP Echo Interval (seconds)

0, 1~10 LCP Echo Failure (counts)

Example:

\$\$\$WANS: 0,telstra.corp,1,userid,password,*99#,0,,24,0,0,0,00:00,0,20,10
OK

Short Messages (SMS)

Universal Hub supports SMS function using AT commands via its serial interface. Only TEXT mode is supported (+CMGF=1) and using "GSM" Character Set (+CSCS='GSM').

– Send SMS

`AT+CMGS="mobile number"<CR>`

`> message body <SUB>`

">" is prompted by the modem after mobile number is entered. Serial terminal device should wait ">" coming out before entering message body and terminated with <SUB>, which is keyboard combination of "CTRL+Z" or "0x1A" in HEX. Maximum length of message is 150 characters.

The modem will return OK and message reference number as below when SMS is successfully sent:

`+CMGS: <num>`

`OK`

`AT+MMC SMSMO <Phone number> <message>`

This is a single line SMS sending command that eliminates the waiting of modem prompt before the message input. Maximum length of message is 150 characters.

Some characters are not supported: \, [,], ^, ~, `. The command will return same message as AT+CMGS

– List SMS

`AT+CMGL=<status>`

<status>: ALL – List all messages.

REC UNREAD – List the messages with status "received unread". It is the default value".

REC READ – List the messages with status "received read".

– **Read SMS**

`AT+CMGR=<index>`

<index>: the location index of the message stored.

– **Delete SMS**

`AT+CMGD=<index>,<flag>`

<index>: the location index of the message stored.

<flag>: 0 – Delete only the message stored at the location index. This is the default value.

1 – Ignore the value of index and delete all SMS messages that the status is "received read".

4 – Ignore the value of index and delete all SMS messages from the message storage area.

– **Unsolicited Result Code (URC)**

Modem can be configured to output an unsolicited message or URC via its serial interface when receives an SMS. The settings cannot be permanently saved and will need re-set after modem reboot.

`AT+CNMI=<mode>,<mt>`

<mode>: 0 – SMS related URCs are buffered and will not be forwarded to the serial interface.

1 – SMS related URCs are forwarded to the serial interface only when the interface is not in socket data mode

2 – SMS related URCs are forwarded to the serial interface regardless of serial interface status

3 – Same as mode 2 for compatibility purpose.

<mt>: 0 – No SMS-DELIVER indications are routed to the serial interface.

1 – An indication of the memory location of the SMS is routed to the serial interface via URC:

+CMTI: <mem>.<index>

<index>: the location index of the message stored.

<mem>: SMS memory location. Can be either "SM" or "ME".

2 – SMS details and message body are routed to the serial interface via URC:

+CMT: <sender>.,<timestamp>

<message body>

– **Show SMS text mode parameters**

The command sets whether or not extra information is shown in SMS result codes. The setting cannot be permanently saved and will need re-set after modem reboot.

AT+CSDH=<show>

<show>: 0 – Do not show the extra information in SMS result codes.

1 – Show the extra information in SMS result codes.

Device Reset

– **Device Reboot**

AT\$\$RESET

When entered, the device will perform a software reset.

– Periodic Reset

AT\$\$RESET=<num>

<num>: the number of hours for periodic rest. 0 – disable periodic reset.

Query Command:

AT\$\$RESET?

\$\$RESET: <num>
OK

– Factory Reset

AT\$\$FACTORY

When entered, the device will restore its factory default configurations and perform a software reset. The saved profile will also be lost.

– Profile Save

AT\$\$PFSET

When entered, the current device configurations will be saved to local Profile 1.

– Profile Restore

AT\$\$PFRST

When entered, the local Profile 1 will be loaded to the device configuration.

Other Supported AT Commands

Universal Hub also supports following AT commands for query and compatibility purpose only and will not affect the cellular module behaviour:

AT+CMEE?

AT+CMEE=<n>

AT+CMGF?

AT+CMGF=1

AT+CSCS?

AT+CSCS='GSM'

AT+CSMP=17,167,0,8

AT+CSMP=17,167,0,0

AT+MOV1E0H0S0=0