AXIOMTEK

ICO300-MI

Robust Din-rail Fanless Embedded System as an Intel® IoT Gateway Solution

User's Manual

RoHS

Disclaimers

This manual has been carefully checked and believed to contain accurate information. Axiomtek Co., Ltd. assumes no responsibility for any infringements of patents or any third party's rights, and any liability arising from such use.

Axiomtek does not warrant or assume any legal liability or responsibility for the accuracy, completeness or usefulness of any information in this document. Axiomtek does not make any commitment to update the information in this manual.

Axiomtek reserves the right to change or revise this document and/or product at any time without notice.

No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Axiomtek Co., Ltd.

Safety Precautions

Before getting started, please read the following important safety precautions.

1. The ICO300-MI does not come equipped with an operating system. An operating system must be loaded first before installing any software into the computer.

2. Be sure to ground yourself to prevent static charge when installing the internal components. Use a grounding wrist strap and place all electronic components in any static-shielded devices. Most electronic components are sensitive to static electrical charge.

3. Disconnect the power cord from the ICO300-MI before making any installation. Be sure both the system and the external devices are turned OFF. Sudden surge of power could ruin sensitive components. Make sure the ICO300-MI is properly grounded.

4. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.

5. Turn OFF the system power before cleaning. Clean the system using a cloth only. Do not spray any liquid cleaner directly onto the screen.

6. Do not leave this equipment in an uncontrolled environment where the storage temperature is below -45℃ or above 85℃. It may damage the equipment.

7. Do not open the system's back cover. If opening the cover for maintenance is a must, only a trained technician is allowed to do so. Integrated circuits on computer boards are sensitive to static electricity. To avoid damaging chips from electrostatic discharge, observe the following precautions:

   ▪ Before handling a board or integrated circuit, touch an unpainted portion of the system unit chassis for a few seconds. This will help to discharge any static electricity on your body.

   ▪ When handling boards and components, wear a wrist-grounding strap, available from most electronic component stores.

Classification

1.   Degree of production against electric shock: not classified

2.   Degree of protection against the ingress of water: IP40

3.   Equipment not suitable for use in the presence of a flammable anesthetic mixture with air or with oxygen or nitrous oxide.

4.   Mode of operation: Continuous

5.   Type of protection against electric shock: Class I equipment

General Cleaning Tips

You may need the following precautions before you begin to clean the computer. When you clean any single part or component for the computer, please read and understand the details below fully.

When you need to clean the device, please rub it with a piece of dry cloth.

1.   Be cautious of the tiny removable components when you use a vacuum cleaner to absorb the dirt on the floor.

2.   Turn the system off before you start to clean up the component or computer.

3.   Never drop the components inside the computer or get circuit board damp or wet.

4.   Be cautious of all kinds of cleaning solvents or chemicals when you use it for the sake of cleaning. Some individuals may be allergic to the ingredients.

5.   Try not to put any food, drink or cigarette around the computer.

Cleaning Tools

Although many companies have created products to help improve the process of cleaning your computer and peripherals users can also use household items to clean their computers and peripherals. Below is a listing of items you may need or want to use while cleaning your computer or computer peripherals.

Keep in mind that some components in your computer may only be able to be cleaned using a product designed for cleaning that component, if this is the case it will be mentioned in the cleaning.

- Cloth: A piece of cloth is the best tool to use when rubbing up a component. Although paper towels or tissues can be used on most hardware as well, we still recommend you to rub it with a piece of cloth.

- Water or rubbing alcohol: You may moisten a piece of cloth a bit with some water or rubbing alcohol and rub it on the computer. Unknown solvents may be harmful to the plastics parts.

- Vacuum cleaner: Absorb the dust, dirt, hair, cigarette particles, and other particles out of a computer can be one of the best methods of cleaning a computer. Over time these items can restrict the airflow in a computer and cause circuitry to corrode.

- Cotton swabs: Cotton swaps moistened with rubbing alcohol or water are excellent tools for wiping hard to reach areas in your keyboard, mouse, and other locations.

- Foam swabs: Whenever possible it is better to use lint free swabs such as foam swabs.

Note: We strongly recommended that you should shut down the system before you start to clean any single components.

Please follow the steps below:

1. Close all application programs
2. Close operating software
3. Turn off power
4. Remove all device
5. Pull out power cable

Scrap Computer Recycling

If the computer equipments need the maintenance or are beyond repair, we strongly recommended that you should inform your Axiomtek distributor as soon as possible for the suitable solution. For the computers that are no longer useful or no longer working well, please contact your Axiomtek distributor for recycling and we will make the proper arrangement.

Trademarks Acknowledgments

Axiomtek is a trademark of Axiomtek Co., Ltd. IBM, PC/AT, PS/2, VGA are trademarks of International Business Machines Corporation.

Intel$^®$ and Pentium$^®$ are registered trademarks of Intel Corporation.

MS-DOS, Microsoft C and QuickBASIC are trademarks of Microsoft Corporation.

VIA is a trademark of VIA Technologies, Inc.

SST is a trademark of Silicon Storage Technology, Inc.

UMC is a trademark of United Microelectronics Corporation.Other brand names and trademarks are the properties and registered brands of their respective owners.

Table of Contents

CHAPTER 1
INTRODUCTION

This chapter contains general information and detailed specifications of the ICO300-MI. The Chapter 1 includes the following sections:

■ General Description
■ System Specification
■ Dimensions
■ I/O Outlets

1.1   General Description

ICO300-MI, an intelligent industrial Intel® Atom-based IoT (Internet of Things) gateway solution. With din-rail, fanless and rugged design, delivering high performance at competitive price. The reliable ICO300-MI is a perfect embedded solution for IoT, industrial and embedded applications such as power plant automation, facility monitoring systems, intelligent transportation systems and other harsh environment.

The application-ready machine to machine platform ICO300-MI supports Intel® IoT Gateway Solution. Customers could connect their widely distributed systems via wireless network such as 3G/GPRS. It also avails users to manage a variety of systems effortlessly with a wide range of industrial interfaces for both new and existing installation into the Internet of Things environment. It simplifies the development process and deployment ofIoT gateways and achieves accelerated business transformation.

● **Features**

  ■ Fanless design
  ■ Wide temperature operation of -20℃ - +70℃ (-40℃ - +70℃ for optional)
  ■ Supports 2 10/100/1000 Base-T Ethernets with Magnetic Isolated Protection
  ■ 4 COM Ports support RS-232/422/485
  ■ Wireless (3G/GPRS)
  ■ Support one 2.5" SATA SSD (or HDD) and one CompactFlash™ (or mSATA)
  ■ Wide range 12–24V DC-in with terminal block
  ■ Din-rail mounting
  ■ Wall mounting (optional)
  ■ Passed CE with FCC testing
  ■ Supports Intel® IoT Gateway Solution.

Wind River Intelligent Device Platform Overview

The Wind River Intelligent Device Platform XT (IDP XT) packages a commercial-grade Wind River Linux development platform with security and management tools for gateways.

IDP XT provides integrated development and management support for distributed systems that utilize smart services with cloud computing. It includes secure remote management layer for cloud-based smart services, including automated customer interaction and support.
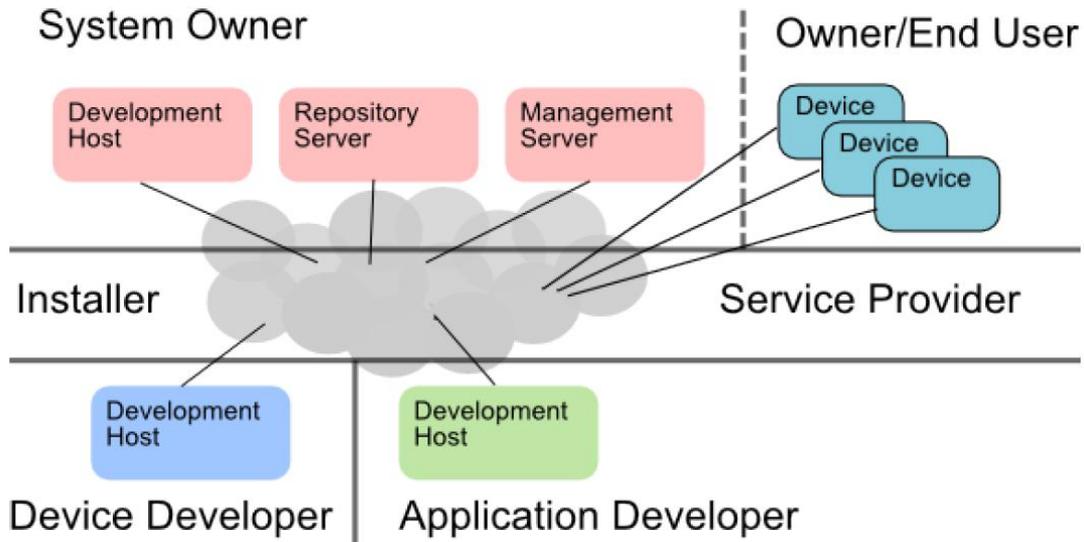
Included in IDP XT
- Wind River Linux
- Wind River Workbench
- Wind River Intelligent Device Platform XT
- McAfee Embedded Control

1.2   System Specifications

1.2.1   CPU

- Onboard Intel® ATOM™ E3815 (1.46 GHz) processor

1.2.2   BIOS

- AMI (American Megatrends Inc.) UEFI (Unified Extensible Firmware Interface) BIOS.

1.2.3   System Memory

- One DDR3L 204-pin SO-DIMM (1.35V) slot.
- Supports 1066MHz up to 4GB (E3815)

1.2.4   Display

- A slim type 15-pin D-Sub connector as VGA connector.

1.2.5   Ethernet Ports

- LAN 1 and LAN 2

  The board has dual RJ-45 connectors, support 10/100/1000 Base-T with 1.5KV magnetic isolated protection.

1.2.6   Storages

- 1 x 2.5" SATA SSD (or HDD) drive bay.
- 1 x CompactFlash TypeII socket (or mSATA).

1.2.7   Wireless

- 1 x Full size Mini Card slot supports 3G/GPRS
- 1 x SIM Card Socket.
- 2 x Antenna holes.

Note: CF and mSATA function can be either one, it can be select by BIOS menu.
mSATA and wireless use the same slot, and only one of them can be selected.

1.2.8   USB

● 2 x USB2.0

● USB Pin Define :

Pin	Signal USB Port 0	Pin	Signal USB Port 1
1	VCC	5	VCC
2	D-	6	D-
3	D+	7	D+
4	GND	8	GND
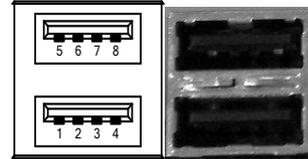
1.2.9   COM

● 4 ports DB9 support RS-232/422/485 which can be selected by BIOS.

● Supports Auto Flow Control in RS485 mode.

● Serial Port Pin Define: (DB9 Male) as below

COM1~4

Pin	RS-232	RS-422	RS-485
1	DCD	TX-	Data-
2	RXD	TX+	Data+
3	TXD	RX+	--
4	DTR	RX-	--
5	GND	GND	GND
6	DSR	--	--
7	RTS	--	--
8	CTS	--	--
9	RI	--	--
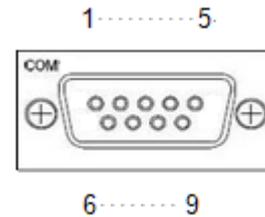
1.2.10   Power

● Wide-range 12 - 24V DC power input with terminal block.

● OVP and Reverse protection.

Pin	Signal
1	+
2	NC
3	-
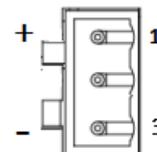
1.2.11 WatchDog Timer (WDT)

- 1~255 seconds or minutes; up to 255 levels.

1.2.12 Restore BIOS Optimal Defaults (JP2)

- Put jumper clip to pin 2-3 for a few seconds then move it back to pin 1-2. Doing this procedure can restore BIOS optimal defaults.

Function	Setting
Normal (Default)	1-2 close
Restore BIOS optimal defaults	2-3 close
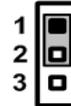
1.2.13 System LED

- There are showed the LED's indicators and functional descriptions.

LED Name	Description	Color
ACT	Indicate the storge status and it's flashing when storge access.	Green
PWR	Indicate the Power status. When the DC input is acceptable, the LED will ON.	Yellow

1.2.14 Operation Temperature

- -20℃ ~ +70℃
- -40℃ ~ +70℃ (optional)

1.2.15 Storage Temperature

- -40℃ ~ +85℃

1.2.16 Humidity

- 10% ~ 95% (non-condensation)

1.2.17 Weight

- 1 kg

1.2.18 Dimensions

- 48mm(1.88") (W) x110mm(4.33") (D) x155mm(6.1") (H)

1.2.19 System I/O Outlets

- Four 9-pin D-Sub male connectors, COM1~COM4.

- One 15-pin D-Sub female connector for VGA.

- Two 10/100/1000 Base-T RJ-45 with 1.5KV magnetic isolated protection.

- Two USB 2.0 connectors.

- One DC Power Input with terminal block.

- Two Antenna holes.

1.3 Dimensions

The following diagrams show you dimensions and outlines of the ICO300-MI
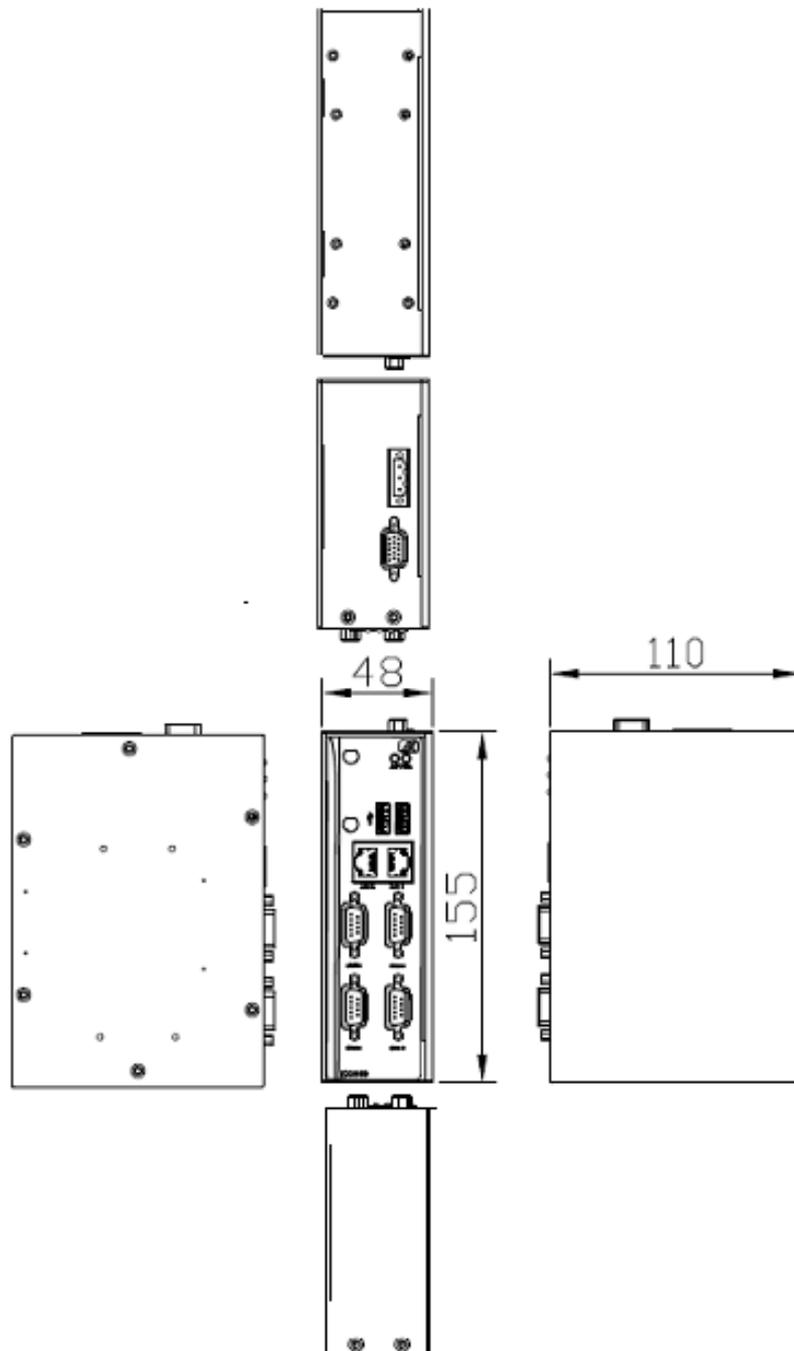
1.4   I/O Outlets

The following figures show you I/O outlets on front view and top view of the ICO300-MI
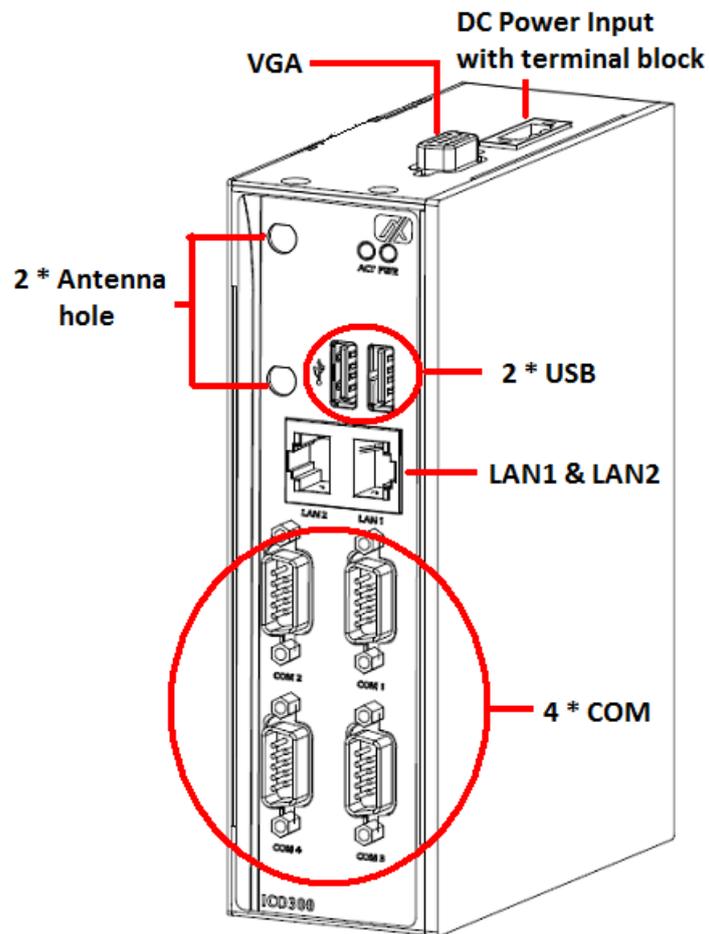
CHAPTER 2
HARDWARE INSTALLATION

2.1   Installing Din-rail Mounting

The ICO300-MI provides Din-rail Mount for 2 methods that customers can install as below:

Step 1   Prepare Din-rail Mount assembling components (screws and bracket) ready.

Step 2   Assembly the bracket to the system and fasten screws tight.

Method -1:
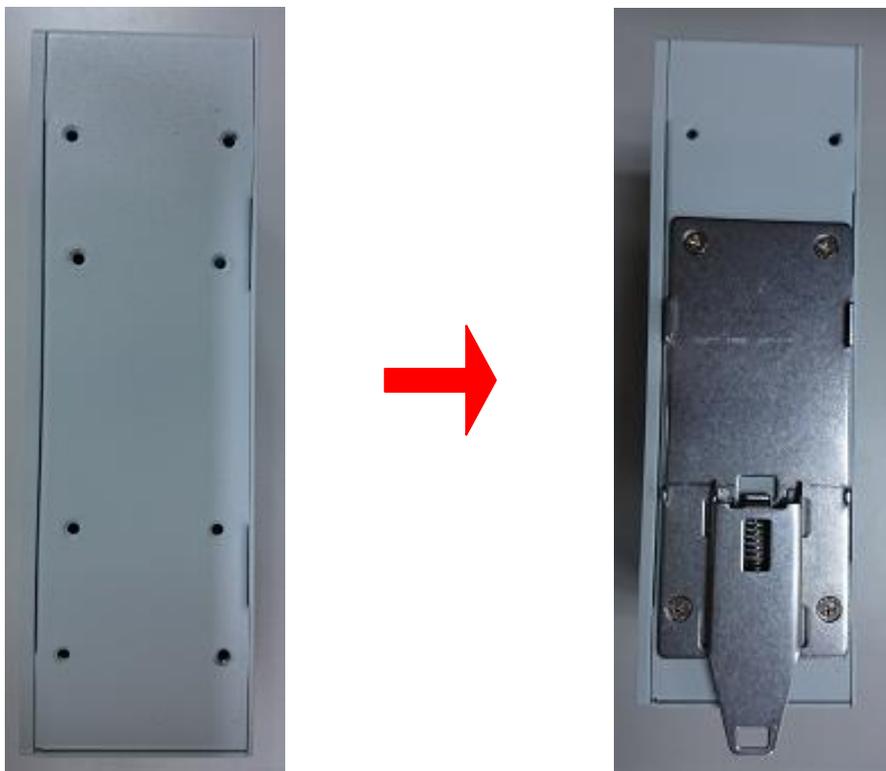
Method-2 :
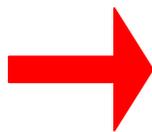
2.2   Installing Wall Mounting (optional)

The ICO300-MI provides Wall Mounting that customers can install as below:

Step 1   Prepare Wall Mount assembling components (screws and bracket) ready.

Step 2   Assembly the bracket to the system, and fasten screws tight.

This page is intentionally left blank.

CHAPTER 3
Webif

About Webif

You can use the Webif interface to configure your gateway or router (your IDP XT device) in the

same way you would configure your home Wi-Fi router.

When you create a default SRM platform project, the **wr-idp-devkit** layer and glibc-idp are

automatically configured. This causes Webif to be included in the project and sets up your IDP

XT target to act as a gateway by default.

you can access https://192.168.1.1 for configurations via LAN1

Login in (user: **admin**, password: **admin)**

If you successfully login and can see below picture.

Webif Interface Main Tabs

The Main tabs provide the bases for making configuration changes to your wireless gateway.

The default Webif interface provides the following tabs and their relevant settings to make

configuration changes to your residential home gateway router:

Info Tab

Use to get system information.

Graphs Tab

Use to get information on CPU usage and traffic on various interfaces.

Status Tab

Use to view the status of routers, modules, the system, and so on.

Log Tab

Use to view the **syslog** and **dmesg** logs.

System Tab

Use to set system-specific setting, such as time, theme and language, access control, password,

and backup and restore, and to upgrade and reset the router.

Includes Startup, Crontabs, File Editor, Mountpoints, and TPM subtabs.

Network Tab

Use to view and set detailed networking parameters. These include WAN, LAN, WWAN,

Wireless, Bluetooth, Firewall, DHCP, Hosts, Routes, UPnP, Zigbee, MultiWAN, and Tweaks.

For more information, see *Network Tab* on page 89.

VPN Tab

Use to add a new IPsec configuration rule for your own IPsec-based VPN network.

Device Agent Tab

Use to manage repositories and agents. Includes RPM Repository, WKS OMA DMC, and OneAgent TR069 subtabs.

Info	Graphs	Status	Log		System	Network	VPN	Device Agent		Logout
System	Notes	About								
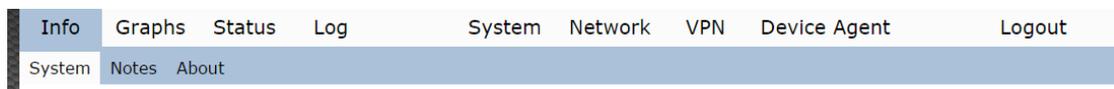
Webif Interface Default Settings

Refer to these default settings when you need to setup or modify your Wi-Fi router.

When working with the Webif interface, you will need the following information:

• **Web login username/password**: admin/admin

• **WAN port**: eth0 (DHCP to get IP address)

• **Bridge**: br-bridge (including wlan0 and other Ethernet interfaces, STATIC IP: 192.168.1.1, with DHCP server running on it)

Network Tab

Use the Network tab to view and change basic networking parameters, including LAN, WAN, and WWAN for your gateway router.

Setting	Description

Network Configuration	Use this section to modify your Network settings. Some key options include:
	
	• WAN Configuration
	
	  - Connection Type: Default is **DHCP**.
	  - Interface: Default is **eth0**.
	
	• LAN Configuration:
	
	  - Connection Type: Default is Static IP
	  - Interface: Default is **wlan0**
	  - IP Address: Default is **192.168.1.1**
	
	• WWAN Configuration:
	
	  - Connection Type: Default is **WWAN**
	  - Interface: Default is **3g-wwan**
	  - Device: Default is **/dev/ttyACM0**.
	  - Service Type: Select a network that matches your SIM card. Default is **UMTS**.
	  - APN Name: Matches the access point name of the network the 3G modem is connected to.

Working with the Status Page

1. Click the **Status** tab. The **System** sub-tab displays the total space and available space on each mount point, as well as the memory usage and tracked connections. Under the Tracked Connections section, click **View Conntrack Table** to display additional information about your tracked connections (on the **Status** > **Conntrack** tab).

2. Click the **Processes** tab to display a current list of processes running on the target (board). The page refreshes every 20 seconds unless you click **Stop Refreshing**. Click to **see the legend** to display a legend that describes processes states.

3. Click the **Conntrack** sub-tab to display the currently tracked connections. You can filter out data to focus on the issue you want to resolve.

In the **Text to Filte**r field, enter **ESTABLISHED | TIME_WAIT** and in the **Filter Mode** field select **Exclude**, then click **Filter Records** to filter these connections out of the display. A subset of the records displays. Verify if the pattern match is case-sensitive.

4. Click the **Diagnostics** sub-tab to run the **ping** and **traceroute** commands for network diagnosis. In the field to the left of the **Ping** or **TraceRoute** button, enter *$HOST_IP* (The IP address of your host computer), then click the button.

Working with the Log Page

1. Click the **Log** tab. The initial view is the **Syslog** sub-tab, which displays the syslog file. You can use the Text Filter section to filter in or out content that you do or do not want to see in the log.

2. In the **Text to Filter** field, enter **usb | USB**, in the **Filter Mode** field select **Include**, then click **Filter Messages** to find all messages in syslog related to USB.

3. Click the **Kernel** sub-tab and notice that the messages are similar to those in the **Syslog** sub-tab, with the same filtering ability. Filter for **igb** and observe that LAN driver status.

Working with the System Page

1. Click the **System** tab. The default **Access Control** sub-tab lets you add, modify, and remove Webif users to control who can use different pages and tabs within the Webif program. Note that Webif users are not system user log in names.

NOTE: Do not change the **Webif Enable** field from **Enable**. If you disable this field, you will lose the Webif connection to the target system, and you must restart Webif from the target (board).

2. In the **Username** field, enter **Testuser**, in the **Password** field enter **Testpass** and re-enter that password in the **Confirm Password** field, then click **Add User** to add that user to the Webif user database.

3. Give the user **Testuser** access to some of the Webif pages. Scroll down the Access Control sub-tab to configure the following settings, then scroll to the bottom of the page and click **Save Changes**. After the screen refreshes, scroll to the bottom again and click **Apply Changes**.
   - In the Info section, in the **System** field, select **Enabled**.
   - In the Logout section, in the **Logout** field, select **Enabled**.

Device Agent

RPM Repository	Disabled ▼
WKS OMA DMC	Disabled ▼
OneAgent TR069	Disabled ▼

Graphs

Graphs	Disabled ▼

Info

System	Disabled ▼
Notes	Disabled ▼
About	Disabled ▼

Log

Syslog	Disabled ▼
Kernel	Disabled ▼

Logout

Logout	Disabled ▼

NOTE: You must click on both **Save Changes** and **Apply Changes** for your changes to take effect.

4. Close the browser.

5. Start another browser session then connect to the target system, but log in as the user **test**. Could you log in? How does the display differ from before?

Logout Page

1. Start a browser session and log in as the user **admin**.

2. Click the **Logout** tab, then close the browser. This is the recommended procedure to disconnect from the target system.
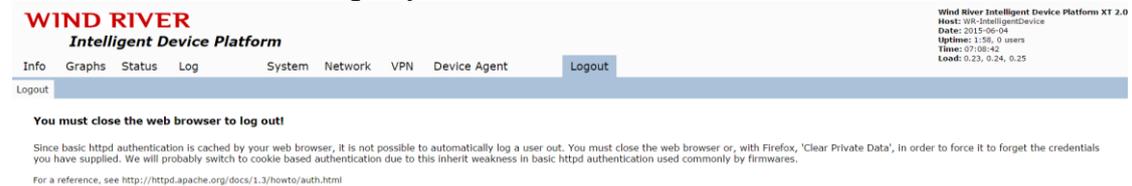
Note : If user wants to further understand IDP (Intelligent Device Platform), pls connect following URL.

https://www-ssl.intel.com/content/www/us/en/embedded/design-tools/evaluation-platforms/gateway-solutions/wind-river-idp-xt2-programmers-guide.html