

CIRA X2 User Manual





FW/

Preface

Copyright

Copyright ©2013 FW LLC. All rights reserved.

This document may not be copied in part or otherwise reproduced without prior written consent from Feeney Wireless except where specifically permitted under US and International copyright law.

Disclaimer

The information in this document is subject to change without notice. Feeney Wireless ("FW") assumes no responsibility for inaccuracies or omissions and specifically disclaims any liabilities, losses, or risks, personal or otherwise, incurred as a consequence, directly or indirectly, of the use or application of any of the contents of this document. For the latest documentation, contact your local supplier or visit us online at *www.feeneywireless.com*.

This publication may contain examples of screen captures and reports used in daily operations. Examples may include fictitious names or individuals and companies. Any similarity to names and addresses of actual businesses or persons is entirely coincidental.

Trademarks and Patents

Feeney Wireless and the FW logo are trademarks of Feeney Wireless LLC. Skyus, Skyus 3G, Skyus 4G, Skyus Global, CIRA, CIRA X, CIRA X2, and Axiom are trademarks of Feeney Wireless LLC. VaraSight and the VaraSight logo are trademarks of Feeney Wireless LLC.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Intended Use

Use this product only for the purpose it was designed for; refer to the datasheet and user documentation. For the latest product information, visit us online at *www.feeneywireless.com*.

Table of Contents

Overview	
Intended Audience	1
Scope	
Specifications	
Configuring the Cellular Modem	
Logging into the CIRA X2 Cellular Modem	
Configuring the Cellular Modem APN	3
Configuring the Access Point	
Logging into the CIRA X2 Access Point	4
Access Point Main Page	5
Monitoring Your CIRA X2 Access Point	6
System Log	6
Log Settings Page	7
Remote Log Page	7
Bandwidth Management Monitor Page	8
DHCP Client Table Monitor Page	8
Packet Statistics Page	9
WLAN Station Status Page	9
Mobile WAN Management Monitor Page	
Configuring Your CIRA X2 Access Point	
Wireless LAN General Configuration Page	
Wireless LAN Security Page	
WLAN MAC Address Filtering Page	
WLAN Advanced Page	
WLAN QoS Page	
WLAN Scheduling Page	
Mobile WAN Configuration Page	14
WAN Advanced Page	
WAN IGMP Snooping	16
LAN IP Page	
LAN IP Alias Page	17
DHCP Server Configuration (General) Page	
DHCP Server Advanced Page	
Network Address Translation (NAT) General Configuration Page	19
Network Address Translation (NAT) Application Configuration Page	19
Network Address Translation (NAT) Port Triggering Rules Configuration Page	20
Dynamic DNS General Settings Page	20
Open DNS General Settings Page	21

Static Route Configuration Page	21
Firewall General Settings Page	22
Firewall Services Configuration Page	22
Content Filter Configuration Page	23
Bandwidth Management Configuration Page	23
Bandwidth Management Advanced Configuration Page	24
Remote Management WWW Configuration Page	24
Remote Management SNMP Configuration Page	25
Universal Plug and Play (UPnP) Service Configuration Page	25
Maintenance Options for Your CIRA X2 Access Point	26
Maintenance General Settings Page	
Password Settings Page	26
Time Configuration Page	27
Firmware Upgrade Configuration Page	27
System Configuration Backup/Restore/Reset Page	
System Restart Configuration Page	
System Operation Mode Configuration Page	29
System Alerts Configuration Page	29
Using a Terminal Application with AT Commands	30
Establish Your Connection	
AT Commands	
USB Port Connection	
Contacting FW	32
Online Library	
Return and Warranty	
Further Specifications	
FCC Compliance	

Overview

This document is provided to elaborate on configuring the CIRA X2 specific to each end user environment. It should be used in addition to the CIRA X2 Quick Start Guide in order to fully utilize and implement your system setup.

NOTE: This document has been assembled for best viewing on a computer in order to keep the document page count limited. While it is possible to print and use the document, the computer allows for the zooming in on images.

Intended Audience

This document is intended for users responsible for configuring the CIRA X2 above and beyond the initial installation. The document assumes that the installer possesses a basic working knowledge of computer networking, wireless routing and network administration.

For further information on using your device, please utilize the following documentation:

- CIRA X2 Quick Start Guide: Available via http://www.feeneywireless.com/documents
- ALEOS Configuration User Guide: Available via http://www.sierrawireless.com/

Scope

The CIRA X2 User Manual focuses on preparing your device for use in the end-environment. The User Manual will focus on the configuration of the access point, with further information on the cellular modem available in the ALEOS Configuration User Guide as mentioned above.

Specifications

For Environmental specifications, Power specifications and Antenna specifications, as well as default settings, please reference the CIRA X2 Quick Start Guide as mentioned above.

Configuring the Cellular Modem

Although this document is not intended to provide a complete summary for configuring your cellular modem, this document will give a brief overview on how to log-in to your cellular modem and configure the APN.

Logging into the CIRA X2 Cellular Modem

After the initial power up, to see if the device is properly connected and operating correctly, you can log-in to the device via the methods listed below:

- Connect an Ethernet cable from a computer directly to one of the CIRA X2 LAN connections.
- Associate to the CIRA X2 Wi-Fi using the appropriate method as defined in the Quick Start Guide.
- If you know the CIRA X2's public IP address you can also log-in to the device remotely.
 - Remote Management URL: http//<modem ip>:9191 (:9191 is the port to route to your access point)

Once you have connected to the device perform the following steps:

- 1. Open a web browser on your connected device, specific browser does not matter.
- 2. In the browser's address bar, enter the IP Address: http://192.168.13.31:9191
 - a. Please note, that steps 1 & 2 are only necessary if you are not logging in remotely.

If you are successfully connected, the image below should appear:

Preemanager	~ V4.0	SIERRA WIRELESS
	LOGIN	Support
	Log in to Acemanager User Name : Password : Log In	
		Copyright © 2012 Sierra Wireless, Inc.

Figure 1: ACE Manager Log-in Page

Upon initial configuration, the default **User Name** is *user* and the default system **Password** is *12345*, if you have changed the **User Name/Password** since then, please enter the appropriate log-in information.

Upon a successful log-in, your screen should appear as the image in Figure 2. Please note, the image is for reference only and your values may or may not match.

										Help		Logo
								ļ	Firmware U	oload Down	load Rebo	ot <u>Ref</u>
Status	WAN/Cellular	LAN	VPN	Security	Services	GPS	Events Reporting	Serial	Applicatio	ns I/O	Admin	
ast update	ed time : 05-08-201	3 15:56:31								Apply	Refresh	Cance
Home			AT Phone	e Number			50	94800742				
WAN/Ce	llular		AT IP Ad	dress			0.0	0.0.0				
LAN			AT Netw	ork State			Ne	twork Link [Down			
LAN			AT Signa	I Strength (RS	SSI)		-1:	28				
VPN			LTE S	ignal Strength	(RSRP)		0					
Security	,		AT Cell In	ifo			Ce	Illn fo: RSSI:	-128			
Service	•		AT Netw	ork Service Ty	ype		No	ne				
Jervice.	3		AT Signs	Ought (ECK	version		4	0.1.002				
GPS				including (ECit Signal Quality (7		-1	U				
Serial			AT Chan	nel	(CORCE)		0					
Applicat	ione		WAN	/Cellular Bytes	s Sent		0					
Applicat	lons		WAN	/Cellular Bytes	s Rcvd		0					
About			AT Custo	mer Device N	ame		CA	134021704	1004			
			X-Car	rd Type			X-I	Card Not For	Ind			

Figure 2: ACE Manager Home Page

Once a successful log-in is accomplished, please reference the ALEOS Configuration User Guide, which is available at *http://www.sierrawireless.com/* for configuration. Please contact your FW Support Representative if further assistance is required.

Configuring the Cellular Modem APN

One of the more frequent requirements during initial configuration is to declare the APN. Through the tabs at the top of menu selections, select **WAN/Cellular**. If not already, expand the **Advanced** section to display the APN information. The page will show the **APN in Use** and provide the option for a **User Entered APN**. Once you have entered the APN, click the **Apply** option in the upper right corner and wait for the cellular modem to apply the changes.

NOTE: Configuring the APN is only potentially necessary for Verizon and ATT CIRA X2 Devices. For Sprint Devices, this step is not applicable.

ast updat	ted time : 05-08-201	3 14:37:59	VFN	security	JUTIOUS	UI S	Lvents Reporting	Joenar	Expand All		efresh	Cance		
	Index										un com	Carrie		
WAN/Ce	enular		[-] LTE	4								-		
			T AT L	TTE Data Service				LTE Preferred 💌						
			[-] Keep Alive											
			AT P	(eepalive IP Ac	ddress			4.2.2.2						
				AT Keepalive Ping Time (mins)					5					
				Troce Keepalive Ping					Disable 💌					
				[-] Advanced										
			APN in Use					XXXXXXXXXX						
			AT User Entered APN					MIP Preferred						
			Network Roaming Preference					Automatic 💌						
			F F	lesponse to In	coming Ping			ALEOS Responds						
			AT L	TE Authentica	tion Mode			NONE 💌						
			AT N	letwork User I	D									
			AT N	AT Network Password										
			AT N	letwork Watch	n Dog (mins)			120						
				TE Active Res	can			Disabled						

The image below shows an example of the proper procedure for performing this step:

Figure 3: Configuring the APN

Configuring the Access Point

The following sections will provide information, in detail, on how to log-in to the CIRA X2 access point and configure the device for your end environment. Please note, that all values shown are for reference only and may not match those set in your device.

Logging into the CIRA X2 Access Point

After the initial power up, to see if the device is properly connected and operating correctly, you can log-in to the device via the methods listed below:

- Connect an Ethernet cable from a computer directly to one of the CIRA X2 LAN connections.
- Associate to the CIRA X2 Wi-Fi using the appropriate method as defined in the Quick Start Guide.
- If you know the CIRA X2's public IP address you can also log-in to the device remotely.
 - Remote Management URL: http//<modem ip>:8080 (:8080 is the port to route to your access point)

Once you have connected to the device perform the following steps:

- 1. Open a web browser on your connected device, specific browser does not matter.
- 2. In the browser's address bar, enter the IP Address: http://192.168.1.1:8080
 - a. Please note, that steps 1 & 2 are only necessary if you are not logging in remotely.

If you are successfully connected, the image in Figure 4 should appear:



Figure 4: Access Point Log-in Page

Upon initial configuration, the default system password is *feeneyap*, if you have changed the password since then, please enter the appropriate password.

If it is the initial login, you will be prompted to change your password, as shown in Figure 5.

New Password: Retype to Confirm:	New Password:	
	Retype to Confirm:	

Figure 5: Change/Confirm Password Page

To leave the password as *feeneyap*, simply click the **Ignore** option.

If at this time you wish to change the system password you may enter the password of your choice in the **New Password** field. Enter it again in the **Retype to Confirm** section to confirm and your new password and click the **Apply** option.

NOTE: FW recommends that you set the password away from the default and document it in a private location to ensure the privacy of your network.

Access Point Main Page

Figure 6 shows the main status screen. After logging into the CIRA X2 web interface, this is the primary navigation and system status screen. From this screen, a user can view:

- Status Parameters
- Connection Status
- · Navigation lcons (left of the screen) for monitoring and configuring menus

Decker selectation Tayman Status Print Data Perint Nach Regime AddOil Status Status Nach Regime Visitability Status Status Case to Status Status AddOil Status Status - Off Units AddOil Status Status - Off Units AddOil Status Status - Off Units - Addoil Status Status - Off Units - Addoil Status Status - Off Units - Addoil Status - Off Units - P Month Status Status - Off Units - Default Status - Off Units - P Adonte Status Status - Off Units - Default Status - Off Units - P Adonte Status Status - Off Units - P Adonte Status Status - Off Units <th></th>	
Name Data Rem Net/Face AVCII Stylen Up Tem Net/Face AVCII Stylen Up Tem Face/Face/Face/Face/Face/Face/Face/Face/	
Heal Name A0001 Baylan Us Tim Immain sension: V1000001153.Marginet20022 Carant Dank's (All Markington): Rodur Maio Carant Dank's - With Markington:	Data
Promotive service Y1000Ar01 153300000000000 Camera Daw To Sign Of Biologic Right massau Right massau Sign Of Biologic Control Status Right massau Sign Of Biologic Right Massau Status Right Massau Sign Of Biologic Right Massau Status Right Massau Sign Of Biologic Right Massau Status Right Massau Sign Of Biologic Status Right Massau Status Right Massau Sign Of Biologic Status S	Timin, 17 seca
Bysic Planck Rodar Holds System Resolut Allow Medication 1 - 071/03/04/1 - 071/03/04/1 Allow Medication 2 - 071/03/04/1 - 071/03/04/1 - Mich Medication 2 - 071/03/04/1 - 071/03/04/1 - Off Child Contradition 3 - 071/03/04/1 - 071/03/04/1 - Mich Medication 2 - 02/05/05/05/05/0 - 071/03/04/1 - Mich Medication 3 - 02/05/05/05/0 - 071/03/04/1 - Mich Medication 3 - 02/05/05/05/0 - 071/03/04/1 - Mich Medication 3 - 071/03/04/1 - 071/03/04/1 - Mich Medi	2010-01-01/100:30:20
34V2 Marcelanden - Adie Marcharden - Adie Marcharden - Adie Marcharden - Marcelanden - Adie Marcharden - Marcelanden - Marcelanden - Marcelanden - P Adoessi - P Adoessi - P Adoessi - P Marcelanden - P Adoessi - P Ado	
- Adda Halman. Enclosed HAV. Conservation HAV. C	(m)
- 442 Adams Constant	27%
P Address 0-800 Present -P Model State 0-800 -Second State - Default Galeway 0-800 - Second State - Default Galeway - Second State - Second State - Default Galeway - Second State - Second State - Default Galeway - Second State - Second State - Default Galeway - Second State - Second State - Default Galeway - Second State - Second State - Default Galeway - Second State - Second State - Default Galeway - Second State - Second State - Second State - Second State - Second State - Second State - Second State - Second State - Second State - Second State - Second State - Second State - Second State - Second State	
• P Model Mark 0.000 • ServiceMark • Dethad Stark (*) 0.000 • Umail • Dethad Stark (*) 0.000 0.000 • Mich Address 0.000 • Mich Address • Mich Address Mich Address • Mich Address	Enance
- Collard 0.8.0.9 - Univer - CADOP Call On I Collard - Call P Collard Collard Link Instruments - Univer Collard - Information - Collard Collard - P Addressi CC 100 (\$10.9.06 - Collard - Information - Expension Collard - P Addressi Sci0.255.05 Collard - Coll Coll Sci0.255.05 Collard - Coll Coll Sci0.255.05 Collard - Coll Coll Sci0.255.05 Coll Collard - Coll Coll Sci0.255.05 Coll Collard - Coll Coll Coll Collard Coll Collard - Coll Coll Access Possibility Planotitististististististististististististi	Disative
OHOP Otel P Outel Manager -OHOP Outel Manager Outel Manager - WA ADMASE Otel Manager Second Manager - # AddMase Otel Manager Second Manager - # AddMase Display 2000 One Manager - # AddMase Display 2000 One Manager - @ KOP Display 2000 One Manager - @ KOP One Manager One Manager - WU, ADM Proper Octome Manager Manager - @ KOP Manager Octome Manager Manager - @ KOP Manager Octome Manager Manager - @ KADMASE Octome Manager Manager - @ KADMASE Octome Manager Manager - @ KADMASE Octome Manager Octome Manager	Drahed
Let internation Cet the 51 05 40 Second Sec	Disabled
INICA ADDALL CCD v161030 Summary INICADADAL 100 v06.11 Summary IP Address 100 v06.11 COD v06.01 IP Address 200 200.200.00 COD v06.01 IP Address 200 200.200.01 COD v06.01 IP Address COD v06.01 Pacent Education INICADADAD COD v06.01 V06.01 INICADADADADADADADADADADADADADADADADADADAD	
IP Address in 100 color.11 color.01 IP Address in UP Address in	
-IP Dutrick Mark 25525.55 Central Mark - (PCC)* Same CHCT Table 0. att, Al Markmolou; Pacont Database Pacont Database att, Al Markmolou; Access PaintMarke Pacont Database att, Al Markmolou; ChCT Table 0. Markmolou; att, Al Markmolou; ChCT Table 0. Markmolou; - Stabus CHC Table 0. Markmolou; - Stabus CHL 1. Access 0.00 - ShamedData; Access 0.00 -	
-CHCO* Same CHCO* Table (2) att, All Information Parcent Tableting Parcent Tableting att, All Information Access Paintable M_ent Tableting VALACE Private (2) Access Paintable M_ent Tableting VALACE Private (2) Access Paintable M_ent Tableting - Baba Chtter (2) Access Paintable Ment Tableting - State (2) Access Paintable Manufactor (2) Access Paintable - State (2) Access Paintable Manufactor (2) Access Paintable - State (2) Access Paintable Manufactor (2) Access Paintable - Observed Access Paintable Access Paintable Access Paintable	
Alt Alt Manufaber Plannit Distancio Plannit Distancio • WAARD OF None Access Paint Mode W, Alt Distancio • Manc Address CCXID 40: 91:30:30 - • Status ON - - • Status ON - - • Status ON - - • Observed Access report Mode - -	
Arty Act Of Mode Active Privilia/de VK, NY Block VK, NY Block March Address CC 100 4 of 10 80 - Status CV 100 4 of 10 80 - Status CV 100 4 of 10 80 - Status CV 100 4 of 10 80 - Status CV 100 4 of 10 80	
Later, Advess CCID #1910 800 - Rubu CH - Rubu Anno-1500 - Channel Anno-1500	
- Tabas OV - Namedicity acon-dool - Oxanet Association	
- Named SO() alto 7-600 - Channel Auto Channel	
- Channel Ado Channel	
Operating Channel One of the operating Channel	
- Security Mode. Katika PSK	
- 802 11 Mode: 882 115/pH	
-white Unconfigured	

Figure 6: Access Point Main Status Page

Monitoring Your CIRA X2 Access Point

The access point provides system diagnostic and monitoring informational pages which are available by clicking the **Monitoring** Icon located below the **Status** icon on the left side of the page.

Monitoring Icon

System Log

Figure 7 shows the system log display. This log will show information regarding system status, firewall status, access to the system web interface, and status of Mobile WAN connection cards, such as 4G connection cards. By default the CIRA X2 is configured to synchronize its system time online to GMT within a few seconds of obtaining an Internet connection.

F	Waxiem				Lassed
Ľ		Monitor > Log > Ve			
-	Den al close al	View Log Lo	g Settings Remote Log		
R	Log SW MONT Monitor DHCP Table Packet Statistics WLAN Station Status MWAN MONT Monitor	Logs Display:	al log 💌	Ratean) Cisa	ĵ
		Sun	mary		
			Time	Message	
		1	Aug 5 23:26:34	AXXXX local0.info udhcpc(1617): DHCP Client uses IP 68.25.47.240	
		2	Aug 5 23 26 34	A300M local0 info udhcpc[1617] Lease of 68.25.47.240 obtained, lease time 60	
		3	Aug 5 23:26:34	A300M local0 info udhcpc[1617] Sending renew	
		4	Aug 5 23:26:19	AXXXIII local0.info udhcpc[1617]: Sending renew	
		5	Aug 5 23:25:46	AXXXI local0 info udhcpc(1617): DHCP Client uses IP 68.25.47.240	
		6	Aug 5 23 25:48	AXXXI local0.info udhcpc(1617): Lease of 68.25.47.240 obtained, lease time 60	
		7	Aug \$ 23:25:46	AXXXIII local0.info.udhcpc(1617): Sending renew	
		8	Aug 5 23 25:31	AXXXIII local0.info.udhcpc(1617) Sending renew	
		9	Aug 5 23 24:57	A300M local0 info udhcpc[1617]. DHCP Client uses IP 88.25.47.240	
		10	Aug \$ 23:24:57	A300M local0 info udhcpc[1617]: Lease of 60.25.47.240 obtained, lease time 60	
		11	Aug 5 23 24 57	AXXXM locat0.info udhcpc[1617] Sending renew	

Figure 7: Access Point System Log

Log Settings Page

This page allows the user to configure the items, by type, that will be displayed in the system logs.

E	W/aviam	Los de la contra de
	MONITOR open all close all Monitor - ESS - BW MONIT Monitor - Decket Statutos - Packet Statutos - WULAN Station Status - MWAN MONIT Monitor	
		Appy Ratesh

Figure 8: Access Point Log Settings Page

Remote Log Page

This page allows the user to enter a syslog Server IP Address for transmitting of log files to a remote server. By checking the Enable Remote Log check box and entering an IP address in the **Server IP Address** field, the system logs can be sent over the Internet to a server compatible with syslog protocol.

NOTE: Enabling this feature will consume bandwidth on the cellular link

F	Waxiem			Linesd
1 0 E	MONITOR open all close all Monitor - Los DW MGMT Monitor - DHCP Table	Monitor > Log > Remote Log View Log Cog Settings Remote Log Encode Log Encode Remote Log		
	Packet Statistics WLAN Station Status MWAN MGMT Monitor	Server P Address :	Apply Read	

Figure 9: Access Point Remote Log Page

Bandwidth Management Monitor Page

When Bandwidth Management is disabled, as it is by default, the page will appear as blank. When the setting is enabled, the screen will show interface data usage for bandwidth management categories that are enabled.

F	Waxim		Logost
	AX Iom AMONETOR open all close all Monitor Log Evy Updati Konstor OHCP Table Packet Statistics WUAN Statistics MIWAN MOMIT Monitor	Monitor Monitor	

Figure 10: Bandwidth Management Monitor Page

DHCP Client Table Monitor Page

This option shows a list of currently connected Ethernet and Wi-Fi clients with DHCP IP assignments.

NOTE: If devices that are connected via Ethernet or Wi-Fi are configured with a Static IP address on the connected device itself they will not show up on this list.

F	Waxiem						Lagent			
	MONITOR	Monitor - DHCP	Table + DHCP Table							
0	open all close all Monitor - Log - BW MOMT Monitor	All CHCP Table DHCP Client Table								
<u>.</u>	Packet Statistics	T	able List							
	WLAN Station Status MIVAN MONT Monitor			MAC Address	IP Address	Expires in				
			1	5C:26:0A6C:31:70	192.168.1.33	23:37:28				
					Refresh					
		20								

Figure 11: DHCP Table Monitor Page

Packet Statistics Page

This screen shows system uptime as well as usage and status of Embedded WAN, LAN, Wi-Fi, and Mobile WAN (USB Mobile Broadband Card) interfaces.

You have the ability to select a **Polling Interval** and then click **Set Interval** in order to have this screen automatically refresh.

NOTE: The values listed in the 'Tx B/s' and 'Rx B/s' columns are usage in bytes since the initial system power up.

۰.,	CARTON	Hontor >								
	open al close al	Packet	Statistics							
	Log EW MGMT Monitor DHCP Table	Paci	oet Statistics							
	- Packet Statistics		Packet Statis	tics						
	WLAN Station Status WWAN WGNT Monitor		Port	Status	TxPitts	RoPids	Collisions	Tx B/s	Rx B/s	Up Time
			WAN	100M	171	135	0	57786	27600	00:26:00
			LAN	100М	4732	3779	0	3261796	2443824	00:26:52
			WLAN	Down	0	1	0	0	216	00:00:00
			Mobile WAN	Up	3183	14470	0	2364696	2784328	00:25:08

Figure 12: Packet Statistics Page

WLAN Station Status Page

This option shows any and all currently connected Wi-Fi clients.

F	Waxlorm		Logod
	MONITOR open all close all Monitor - Log - Brw MONT Monitor - DICP Table - Packet Statistics - WAAN STOOD Cation - MWAN MONT Monitor	Inonitir's WLAN Station Station S Association List Association List MAC Address MAC Address Association Time	1
		Reteat	

Figure 13: WLAN Station Status Page

Mobile WAN Management Monitor Page

This option shows signal strength and connection status for USB connection card when they are being utilized.

NOTE: The system is not designed to facilitate hot swapping of USB connection cards. Detection of a USB connection card is not guaranteed if inserted after system reboot.

To properly connect a USB connection card, power down the system, connect the card, and then power the system back up.

A Marker &	Montro R core al j case al core Notar Seciel Al Core Seciel Al Core Notar Seciel Al Core Secie Al Core Secie Al Core	MONETOR Open al close al MONAT MONITOr Open al close al MONAT MONITOr Monitor Log BW MONT Monitor Mobile VIAN MGMT Monitor Mobile VIAN MGMT Monitor Mobile VIAN MGMT Monitor Mobile VIAN Consection Information VIAN States States	
Novel of a general general general general general general de la constante de	Acceleration of a state of a stat	AdvantOrk open all close all MVVAN MGMT Monitor Log Monitor Expl Monitor Discrete Mobile WAN MGMT Monitor Discrete Mobile WAN Connection Information WAN States States	
Log Even Middler Monter Even Middler Monter Fachet Strainles WLAN Staten Status WLAN Staten Status WULAN Staten Status	 Log Work Wake Model Monitor Proceed Statistics Work Work of Monitor Work Work	Log Mobile WAN MGMT Monitor DisCP Table Packet States Mobile WAN Connection Information WAN States	
• WLAN Statistics • WLAN Statistics • WLAN Statistics • WUAN Statistics Statistics • Downer Model WAN Connection Information Item Data Connection Status: Up Network Type: WMAX Ts Power Mean: 9 dBm CRIR Mean: 27 dB Center Fireg 2683 5 MHz	Packet State Control Note WAAI State State Control Note Work State State Note Vision State	Packet Statistics WAN Connection Information WAN Station Status	
WLAN States Sales Mont Month Meeter Connection Status: Up Network Type: WMAX Tx Power Mean: 9 dBm Rx Power Mean: 45 dBm CRR Mean: 27 dB Center Freg: 2003 5 MHz	WAAA Station Status Item Item Connection Status: Up Network Type: WMAX Tx Power Mean: Polin Rx Power Mean: CoNR Mean: Z7 dB Center Freg Z603.5 MHz	WLAN Station Status	
Connection Status: Up Network Type: WMAX Tis Power Mean: 9 dBm Ris Power Mean: 455 dBm CBNR Mean: 27 dB Center Fireg: 2883.5 MM2:	Connection Status: Up Network Type: WMAX Tx Power Mean: 9 cBm CNR Mean: 455 dBm CNR Mean: 27 dB Center Freq: 2683.5 MAz	Item Data	
Network Type: WMAX Tx Power Mean: 9 dlm Rx Power Mean: 45 dBm CINR Mean: 27 dB Center Freq: 2683.5 MH2	Network Type: WMAX Tx Power Mean: 9 dBm Ri Power Mean: 45 dBm CHNR Mean: 27 dB Center Freg: 2683.5 MHz	Connection Status: Up	
Tx Power Mean: 9 dBm Rx Power Mean: 45 dBm CINR Mean: 27 dB Center Freg: 2603.5 MHz Betream	Tx Power Mean: 9 dBm Rx Power Mean: 45 dBm CINR Mean: 27 dB Center Freq: 2683.5 MHz	Network Type: WMAX	
Rx Power Mean: 45 dBm CBNR Mean: 27 dB Center Freg 2683.5 MHz Battean	Rx Power Mean: 45 dBm Center Freg 2003.5 MHz Between	Tx Power Mean: 9 dBm	
Cthird Mean: 27 dB Center Freg: 2083.5 MHz Batrash	CINR Mean: 27 dB Center Freg 2683.5 MHz Refresh	Rx Power Mean: -65 dBm	
Center Freq. 2083.5 MHz	Center Freg: 2083.5 MHz	CINR Mean: 27 dB	
Betras	Refrest	Center Freg: 2683.5 MHz	
			Retrest

Figure 14: Mobile WAN Management Monitor Page

Configuring Your CIRA X2 Access Point

The access point provides the ability for user configuration which is available by clicking the **Configuration** icon located below the **Monitoring** icon on the left side of the page.



NOTE: Upon completion of configuring your device, FW recommends utilizing the **Backup Configuration** option as described under the section called 'System Configuration Backup/Restore/Reset Page' on page 28.

Wireless LAN General Configuration Page

The Wireless LAN General Configuration Page is the default page displayed when selecting the **Configuration** icon and provides the ability to do the following:

- WLAN Control by toggling between OFF and ON, you can Enable or Disable the Wi-Fi radio.
- SSID Control the page allows you to define the operation of 4 simultaneous SSIDs.
 - Checking the Hide box for a given SSID will disable the broadcasting of the associated SSID which will make it more difficult for unauthorized users to detect and connect to your Wi-Fi network(s).
- Channel Selection this option allows you to set your Wi-Fi channel on the Channel Selection drop down menu.

• Auto Channel Selection – by checking this box, the CIRA X2 will automatically select a channel. Checking this box is recommended by FW.

Figure 15: Wireless LAN General Configuration Page

Default System Settings are as follows:

- Wi-Fi = ON
- Primary System SSID = Axiom-(last 4 digits of MAC address located on CIRA X2 label)

Wireless LAN Security Page

The Wireless LAN Security page allows the user to set the pass phrase for logging into the CIRA X2 Wi-Fi networks. The process for configuring the SSID is as follows:

F	Waxiam			Lagend
	CONFIGURATION ppen al close at phetwork - phetwork - who - w	Configuration - Network - Vitraesis LAN - Security General Security SSD Security Mode Pre-Shared Key Group Key Update Timer	sxiom-0078 • WPA-Persona(TKP) • Teeneysp 9800 seconds	1
			(Apply) Sencel	

Figure 16: Wireless LAN Security Page

- 1. To set the SSID pass phrase, use the **SSID Drop Down** list to select the desired SSID.
- 2. In the **Security Mode Drop Down** list to select the desired SSID security mode, *WPA-Personal* and *WPA2-Personal* are recommended for maximum security.
- 3. Insert the pass phrase in the **Pre-Shared Key** dialog box and set the time in seconds for the **Group Key Update Timer** in the related dialog box.
- 4. Once all settings are inserted, click the **Apply** button, and repeat as necessary for any other SSIDs being utilized.

Default System Settings are as follows:

- Security Mode = WPA-Personal(TKIP)
- Pre-Shared Key = feeneyap

WLAN MAC Address Filtering Page

In order to ensure not just any wireless client can join your Wi-Fi network, the CIRA X2 provides MAC Address Filtering, which will allow you to configure a list of clients that are allowed to join the network.

You can configure your MAC address filtering by doing the following:

F	Waxiem									Laday
	CONFIGURATION	Configuration > Network	> Wheless LAN > MAC	iter						_
R	CORENDATION Quental close all Metwork Metwork WAN LAN DRICP Server NAT DONS OpenDAS Static Route Static Route Static Route	General Security Access Policy SSD Policy Add e station 1 Set Range MAC Filter Delete	MAC Filter Advan	ced QoS Sch	eduling MAC Address	axion-0678 • Disable • No • (use 00 / Apply	(MAC Address Fo as wildcard in the las Delete Cance	ernat XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	MAC Address	

Figure 17: Wireless MAC Address Filtering Page

- 1. Select the proper SSID
- 2. Set the **Policy** to Enable MAC Address Filtering, or set disable to not filter.
- 3. Set a specific MAC Address or add a MAC Address range by leaving the last 1, 2, or 3 octets blank and toggle the Set Range field to 'Yes'.

WLAN Advanced Page

On the WLAN Advanced page, you can modify Wi-Fi advanced parameters such as the output power level.

Waxlem			
	Configuration > Network > Winsiess I AN > Advanced		
CONFIGURATION open all close all	General Security MAC Filter Advanced QoS Scheduling		
- Wreless LAN - WAN	Wireless Advanced Setup		
- LAN	RTS/CTS Threshold	2346 (256 ~ 2346)	
NAT	Progmentation Threshold	(256 - 2346)	
+ 00NS	Output Power	100% 💌	
- OpenDNS	HT Physical Mode		
Security	Operating Mode	@ Mixed O Green	
E Management	Channel BandWidth	C20 #2040	
	Guard Interval	Ciong @ Auto	
	Extension Channel	Channel-05 24325Hz	
		Apply Cancel	

Figure 18: WLAN Advanced Page WLAN QoS Page

On the WLAN QoS page you can enable or disable QoS. QoS enables you to use congestion management and avoidance tools, which prevent traffic from slowing down on you WLAN. The Default is enabled.

WLAN Scheduling Page

	11/											Lea	end
F	-W ^{axiom}												
(en													
	CONFIGURATION	Configuration	on > Network	> Wireless LAX	> 905								
	open al close al	General	Security	MAC Filter	Advanced	QoS	Scheduling						
0	Network												
	- WAN	WMM	Configuratio	on									
R .,	- LAN		Enable WM	M QeS									
	DHCP Server NAT												
	+ DONS								-				
	OpenDNS Static Route							APPN	Cancel			_	
	E Security												
	Management												
												_	

Figure 19: WLAN QoS Page

On the WLAN Scheduling page, you can define a schedule to control when the Wi-Fi radio is enabled or disabled. **Mobile WAN Configuration Page**

	CONFIGURATION open all close all Network	General	> Network > Wireless LAN > Scheduling Security MAC Filter Advanced	Gos Scheduling		
	- WAN	Wireles	ss LAN Scheduling			
		10	Enable Wireless LAN Scheduling			
	DHCP Server		Scheduling			
	- DONS		WLAN status	Day	For the following times (24-Hour Format)	1
	OpenDNS		O on ® Off	C Everyday	00 w (hour) 00 w (min) ~ 00 w (hour) 00 w (min)	1
	Static Route		O on @ Off	E Mon	00 . (hour) 00 . (min) ~ 00 . (hour) 00 . (min)	
E	B Management		O on @ off	E Tue	00 • (hour) 00 • (min) ~ 00 • (hour) 00 • (min)	
			O On @ Off	E Wed	00 w (hour) 00 w (min) ~ 00 w (hour) 00 w (min)	
			O on ® Off	E Thu	00 w (hour) 00 w (min) ~ 00 w (hour) 00 w (min)	
			O On ® Off	E Fri	00 w (hour) 00 w (min) ~ 00 w (hour) 00 w (min)	
			O on ® Off	E Sat	00 • (hour) 00 • (min) ~ 00 • (hour) 00 • (min)	
			On ® Off	E Sun	00 x (hour) 00 x (min) ~ 00 x (hour) 00 x (min)	

Figure 20: WLAN Scheduling Page

On the Mobile WAN Configuration page, the CIRA X2 allows the user to configure the settings to support USB connection cards. Officially supported devices for use are as follows:

- Skyus 3G Sprint
- Skyus 3G Verizon
- Skyus 3G GSM
- Skyus Global

For proper settings on your USB connection card, please contact your FW Support Representative.

FW/axiom			Lagod
CONFIGURATION open all close a	Configuration > Network > WAN > Mobile WAN Mobile WAN Advanced KGMP Snooping		_
Wretess LAN Wireless LAN Wi	Mobile WAR Configuration Connection Status : WIMAX connected Connect Mode : Maximum Connecton Retry : Action after Retry Falure :	Connect WBBAX Only • 10 Wait • 60 second(s) to retry again.	Ì
E Securby E Management	WMAX Configuration Realm : WMAX Signal Threshold : Warning: The WMAx consection may become utstable whe Note: For best performance when using a WMAX ad	10 (CNR in dB) Threshold is set lower than 15. spter, configure your WLAR to use a channel from 1-3.	1
	Embedded-Mobile WAN Fallover Configuration Show Advanced Options Primary WAN selection : Enable Fatback Check Period : Check Timeou : Check Tolerance : Check Embedded WAN Connectively	Mobile WAN (m. seconds) 50 (in seconds) 3 (in seconds) 3	

Figure 21: Mobile WAN Configuration Page

On WiMAX capable devices, set the **Connect Mode** to either *WiMAX Only* or *Auto*. When set to *Auto* then WiMAX will be preferred but the connection will fall back to 3G if WiMAX is not present or available. Please ensure that the **Primary WAN** selection is configured appropriately if **Connect Mode** is set to *Auto* to ensure use of the correct primary WAN interface.

The CIRA X2 will attempt to detect a WiMAX signal with acceptable quality as configured by the **WiMAX Signal Threshold** setting. The number of scan attempts is defined by the **Maximum Connection Retry** setting. If no WiMAX network with acceptable signal strength is detected within the number of attempts defined in the **Maximum Connection Retry** field, then the **Action after Retry Failure** setting controls the behavior of the system.

For WiMAX devices it is recommended to set the **Action after Retry Failure** *WAIT* and set a wait time of at least *60 seconds*. In this mode, a new series of scans will be started every 60 seconds, other options include *NONE* and *REBOOT*. If *NONE* is selected, the system will make no further attempts to scan for a Wi-Max connection until the system is power cycled. If the action is set to *REBOOT*, the system will perform a reboot if the scans do not detect a WiMAX connection. This option can be useful if the system is designed in a WiMAX only connection scenario where persistent connectivity is essential.

For LTE capable devices set LTE for Connect Mode.

You can select your preferred WAN interface by checking the **Show Advanced Options** checkbox. You may then select either the *Embedded WAN* or *Mobile WAN* by toggling the **Primary WAN Selection** setting.

If you are using both Embedded and Mobile WAN connections, setup the failover ping check function by checking the **Enable Fallback** box. Set a **Check Period** in seconds to run the failover ping test.

NOTE: It is recommended not to set this value less than 45 seconds to avoid potential issues with cellular radios being unable to enter a dormancy state. Should this value be set too short, you may find that connections in rural areas will be unable to transition to 3G from 2G or roaming states.

Setup the IP addresses to ping check by checking the **Check Embedded WAN Connectivity** and **Check Mobile WAN Connectivity** check boxes. It is recommended to select the **Ping User Specified Address** for both WAN connections and input an IP address which is known to be pingable.

Embedded-Mobile WAN Failover Configuration	
Show Advanced Options	
Primary WAN selection :	Embedded WAN 👻
Tenable Fallback	
Check Period :	20 (in seconds)
Check Timeout :	3 (in seconds)
Check Tolerance :	3
Check Embedded WAN Connectivity	
Ping Default Gateway	
Ping User Specified Address	4.2.2.1
Check Mobile WAN Connectivity	
Ping Default Gateway	
Ping User Specified Address	4.2.2.1

Figure 22: Embedded-Mobile WAN Failover Configuration

WAN Advanced Page

The WAN advanced page provides settings for multi-cast traffic. By default this option is disabled.

F	Waxlem		Legou
	CONFIGURATION open all close all	Configuration > Network > WAN > Advanced Mobile WAN Advanced KONP Snooping	
<u>0</u>	Intervors. Wretess LAN Workess LAN LAN LAN ChCP Server NAT DONS OperCNS Static Route Static Route Security	Muticeat Setup None Auto-bridge Enable Auto-bridge mode	
	() Kanagement		

Figure 23: WAN Advanced Page

WAN IGMP Snooping

The WAN IGMP snooping page provides settings for IGMP snooping. By default, this option is disabled.

F	N/axiem		Logod
0	CONFIGURATION open al close al Network - Wireless LAN - Wireless LAN	Configuration > Network > WAN > KMP Snooping KGMP Snooping KGMP Snooping Setup	1
R.	LAN LAN CHCP Server NAT CONS OperONS Static Route Securty Management	Enable KBMP Snooping LAN1 LAN2 LAN3 LAN4	

Figure 24: WAN IGMP Snooping

LAN IP Page

The LAN IP page allows you to set the access point LAN IP address and subnet mask. This is the local IP address and subnet mask of the CIRA X2 on the LAN interface. By default, the **IP Address** is 192.168.1.1 and the default **IP Subnet Mask** is 255.255.255.0.

F	Waxiem			Lagend
	CONFIGURATION	Configuration > Network > LAN > IP		
	open al close al ■ Network = Wireless LAN = WAN = UAN = DHCP Server = Net	P P Alias LAN TCPIP P Address : P Subnet Mask :	192, 168, 1, 1 265, 255, 255, 0	
	DONS OpenDNS Static Route Security Management		Repty Read	

Figure 25: LAN IP Configuration Page

LAN IP Alias Page

The LAN IP Alias page allows for configuration of a secondary IP address on the LAN interface. By default this option is disabled.

E			1904
	CONFIGURATION open all close all Network • Wireless LAN	Configuration > Nathwork > LAN > IP Alas P IP Alas	
R	WAN LAN DHCP Server NAT ODNS OpenONS Statc Revie	P Ales P Ades P Aderes: 0000 P Subnet Mask: 0000	
	Sant House Security Management		

Figure 26: LAN IP Alias Configuration Page

DHCP Server Configuration (General) Page

This option allows the user to define the starting DHCP pool address and the pool size. By default, **DHCP Server** is enabled with the **IP Pool Starting Address** at 192.168.1.33 and the **Pool Size** set to 32 IP addresses.

NOTE: To support additional wired and Wi-Fi clients, increase the Pool Size.

F	Waxiem		Laand
	CONFIGURATION open at close at	Configuration - Network - DHCP Server - General General Advanced	
	Network Wreless LAN Worless LAN WAN LAN DICP Server NAT CONS Constitution	LAN DHCP Setup @Enable DhCP Server IP Pool Starting Address 192:168.1.33 Pool Start	32
	Shake Route Security Management	East Read	

Figure 27: DHCP Server Configuration Page

DHCP Server Advanced Page

This option allows the user to assign static DHCP leases based on MAC addresses. This allows for the assignment of the same IP address to a wired or wireless client. Enter the client's MAC address and a desired IP address. IP addresses must be on the same subnet as configured for the LAN interface of the CIRA X2 itself.

It is also necessary to define DNS behavior for the DHCP server. By default, the **First DNS Server** is set to relay. This setting will pass DNS requests to the DNS server assigned by the systems cellular carrier. Using the dialog boxes located to the right of drop down lists, the user also has the option of statically defining both a first and second DNS server manually.

Advanced				
LAN Static DHCP Table				
	MAC Address		IP Address	
1	00 00:00 00:00 00		0.0.0.0	1
2	00.00.00.00.00.00		0.0.0.0	
3	00 00 00 00 00 00		0.0.0.0	
4	00 00 00 00 00 00		0.0.0.0	
5	00 00 00 00 00 00		0.0.0.0	
6	00 00 00 00 00 00		0.0.0.0	
7	00 00 00 00 00 00		0.0.0.0	
8	00.00.00.00.00.00		0.0.0.0	
	1 2 3 4 5 6 7 8 005 Server DHS Servers Assigned by D	1 00 00 00 00 00 00 00 2 00 00 00 00 00 00 3 00 00 00 00 00 00 4 00 00 00 00 00 00 5 00 00 00 00 00 00 6 00 00 00 00 00 00 7 00 00 00 00 00 00 8 00 00 00 00 00 00	1 00 00 00 00 00 00 2 00 00 00 00 00 00 3 00 00 00 00 00 00 4 00 00 00 00 00 5 00 00 00 00 00 6 00 00 00 00 00 7 00 00 00 00 00 8 00 00 00 00 00	1 00 00 00 00 00 00 0.0.0 2 00 00 00 00 00 0.0.0 3 00 00 00 00 00 0.0.0 4 00 00 00 00 00 0.0.0 5 00 00 00 00 00 0.0.0 6 00 00 00 00 00 0.0.0 7 00 00 00 00 00 0.0.0

Figure 28: DHCP Server Advanced Page

Network Address Translation (NAT) General Configuration Page

This option allows the assignment of a DMZ IP address if desired, by inputting a value into the **Server IP Address** field. **Network Address Translation** must be enabled to support multiple clients on LAN or Wi-Fi interfaces.

-	Waxiem			Lagod
	CONDENDATION	Configuration + Network + NAT + General		
	open all close all	General Application Advanced		
	Herkvork Winkes LAN WAN LAN LAN DICP Server DICP Server Code Static Roule Static Roule Security Management	NAT Setup Enable Network Address Translation Default Server Setup Server IP Address :	0 0 0 0 Apply Reset	

Figure 29: NAT General Configuration Page

Network Address Translation (NAT) Application Configuration Page

This option allows users to configure port forwarding rules. Port translation is supported, allowing a different incoming port and translating to an internal (server) port. This is useful for forwarding to devices such as cameras where port 80 may be blocked.

F	W/axiom									Logout
۲	CONDOURATION	Configuration								
	open al close al	General	Application Ad	vanced						
0	Network	_								
-	- WAN	Add A	Application Rule							
R,	LAN DECEMBER 1		Active							
	- NAT	5	Service Name					ser Defined 💌		
	DONS		Aprt				(D	c 10-20,30,40)		
	Static Route		Server P Address			0000	- C.			
	E Security		Herver Port							
	U wanagement	Apple	cation Rules Summ	ary						
			Application Rule	s Summary						
			# Active	Name	Port	54	rver IP Address	Server Port	Modify	
		_					_			
						Apply	Asset			

Figure 30: NAT Application Configuration Page

To create a port forwarding rule, perform the following steps:

- 1. Check the **Active** Box.
- 2. Enter a name for the service in the **Service Name** field.
- 3. In the **Port** field, enter the TCP and/or UDP port number traffic will be received on the WAN interface(s) of the CIRA X2.
- 4. In the **Server IP Address** field, enter the LAN IP address of the client connected via either the Ethernet or Wi-Fi to the CIRA X2 you wish to forward the selected port to.
- 5. In the **Server Port** field, enter the port you wish the traffic to be forwarded to.
 - a. In many cases, this may be the same as the Port field above. If you wish to translate from an outside port to an inside port, you may do so by entering a different port number in the **Server Port** field.
- 6. Click the **Apply** button so save the rule, or **Reset** to begin the process again.

Network Address Translation (NAT) Port Triggering Rules Configuration Page

This option allows incoming traffic on ports when traffic is detected on a trigger port.

F	-Waxiem							Latend
(er								
	CONFIGURATION	Configuration > Network	+ NAT + Advanced					
_	open all close all	General Applicatio	Advanced					
0.	Network							
-	WAN	Application Rules	Summary					A
Π.		1.000						
	DHCP Server	Port Trigg	pering Rules					
	- 6501 - 70045		hisma		ncoming		Trigger	
	OpenDNS		rearrie	Port	End Port	Port	End Port	
	Static Route	1		0	0	0	0	
	E Security	2		0	0	0	0	
	(i) Wanagement	3		0	0	0	0	
		4		0	0	0	0	
		5		0	0	0	0	
		6		0	0	0	0	1
		7		0	0	0	0	
		8		0	0	0	0	

Figure 31: NAT Port Triggering Rules Configuration Page

Dynamic DNS General Settings Page

This option allows the user to transmit WAN IP addresses to many available DDNS service providers. This option can be useful when WAN IP addresses are dynamic.

F	Waxiem		Logod
	CONFIGURATION open al close al Wretess LAN WAN LAN DRCP Server NAT SECO OpenONS State Route B Security B Management	Configuration > Network > DDNS > General General Dynamic DNS Setup Cnable Dynamic DNS Service Provider : WWW DynDNS ORG Heat Name : User Name : User Name : Dass word :	
		App) Read	

Figure 32: Dynamic DNS General Settings Page

Open DNS General Settings Page

This option allows for Open DNS configuration.

F	Waxiom		Lass
	CONFIGURATION	Configuration > Network > OpenDNS > General	
	open all close all	General	
	WiXeless LAN WIXA UAN LAN Cin(2) Server NAT DONS DONS State Route Security Management	Create New Account / Configure Personalized Setting After OpenONS After OpenONS Finable OpenONS Hoat Name : User Name :	
		Password :	

Figure 33: Open DNS General Settings Page

Static Route Configuration Page

This option shows a routing table and allows for manually configuring and managing static routes.

F	Waxiam									Lasse
-	CONTROLIDATION	Configuration - Network								
	open all close all	IP Static Route								_
•	Wireless LAN WAN	Static Routing Settings								
re.	DHCP Server NAT	Route Name	Address							
	DONS OpenDNS	P Subnet Mar	sk							
	Since Route	Galeway P A	Address							
	(i) Management	Metric								
		Interface			LAN	•				
		Add Rule								
		Applicati	ion Rules Summa	n						
		No.	Active	Name	Destination	Gateway	Metric	Interface	Delete	
		1	9	default	255 255 255 255	0.0.0.0	0	LAN		
		2	.	default	192.168.1.0	0.0.0.0	0	LAN		
		3	9	default	107.62.55.0	0.0.0.0	0	WAN		
		4	9	default	68.25.47.0	0.0.0.0	0	WAN		
		5	9	default	0.0.0.0	107.62.55.1	0	WAN		
		6	9	default	0.0.0.0	68.25.47.1	10	WAN		
		_				Beard				

Figure 34: Static Route Configuration Page

Firewall General Settings Page

This option allows for Enabling or Disabling Denial of Service (DoS) protection. By default, this option is set to enabled.

F	Waxiem						Lazod
•							
	CONFIGURATION	Configuration	on > Security > Firewall > Gen	ensi			
_	open al close al	General	Services				
0	Network						
00	- Wreless LAN	Firew	all Setup				
R	+ LAN		Enable DoS				
	DHCP Server					-	
	+ NAT				Apply	Reset	
	- 00NS						
	Static Route						
	E Security						
	• Frewal						
	Content Filter						
	Management						

Figure 35: Firewall General Settings Page

Firewall Services Configuration Page

This option provides the user the ability to create rules to block client services. By default, all incoming traffic is blocked with the exception of the HTTP web interface for the access point. The option also allows the user to choose to reply to pings on the CIRA X2 WAN interfaces by toggling the **Respond to Ping On** settings box.

NOTE: Creating port forwarding rules under NAT application automatically creates a firewall rule to allow traffic on that port.

NOTE: Many cellular carriers block pings by default so on some carriers enabling this setting will not circumvent this restriction.

CONFIGURATION	Configuration > Security > Firewall > Services		
open all close al	General Services		
Network • Wreless LAN • WAN • LAN • DHCP Server • NAT	KCMP Respond to Ping on: (Apply:)	Deatie	
- DONS - OpenCNS - Static Route 3 Security - Freeval	Enable Firewall Rule		
- Content / Paer	Add Firewall Pale Service Name : MAC address Dest P Address Source P Address Protocol Dest Port Range Source Port Range (Add Rile)		

Figure 36: Firewall Services Configuration Page

Content Filter Configuration Page

This option allows specifically defined websites to be blocked.

FW axtern					
CONFIGURATION open all close all	Configuration > Security > Content Filter				_
Network Wineless LAN WAN LAN DHCP Server NAT	Trusted IP Setup A trusted computer has full access to all Trusted Computer IP Address.	blocked resources. 0 0 0 0 means there is 0 0 0 0	s no trusted computer.		
DONS OpenONS State Route Security Frewal Content Files Management	Restrict Web Features ActiveX Keyword Blocking Enable URL Keyword Blocking Keyword Keyword List	ina i	Cookes	Web Proxy	
	* Delete Clear Al		(Anne) (Baran)		

Figure 37: Content Filter Configuration Page

Bandwidth Management Configuration Page

This option allows the user to either Enable or Disable Bandwidth Management.

F	Waxiem		Lagod
F	CONFIGURATION CONFIGURATION gepen all close all Network - Witheless LAN - WAN - LAN - DRCP Server - NAT - DORS - OpenCINS - Spatic Route - Security - Freewal - Context Filter - Management	Configuration - Management - Bandwitth Management - General Ceneral Advanced Monitor Service Management Cruble Bandwitth Management Read Read	
	Eliteritation la sugemente Eliteritation Remate Management Unive		

Figure 38: Bandwidth Management Configuration Page

Bandwidth Management Advanced Configuration Page

This option allows the user to create bandwidth management rules. In order to create bandwidth management rules, perform the following steps:

- 1. Select both an Upstream Bandwidth and Downstream Bandwidth from the drop down menus.
- 2. Set the **Priority** and check the boxes for the **Service** to which you wish to apply bandwidth management rules.
- 3. You may select the **Advanced Settings** or manually configure rules for each category as desired as well.

CONDUIDATION	Configuration > Utility > I				
open all close al	General Advanced	d Monitor			
Network Wintess LAN WAN LAN LAN ORCP Server NAT CONS OperDNS OperDNS	Management Bar Upstream Bar Downstream Application List	ndwidth ndwidth 3210 w (bps) Bandwidth 32210 w (bps)			
 Static Houte Security 	Applicati	on List			
Frewall Content Eller		Priority	Category	Service	Advaced Salling
- Company Lange					Humanices oreany
3 Management	1	High 💌	Game Console	XBox Live	Advanced dening
Management	1	High w	Game Console	PlayStation	
Management Management Remote Management UPnP	1	High 💌	Game Console	XBox Live PlayStation MSN Game Zone	2 2 2
Kanagement Kanagement Elizabeteten Management Elizabeteten Management UPnP	1	High I	Game Console	XBox Live PlayStation MSN Game Zone Battlenet	2 2 2 2
Kanagement Anagement Endowlen Management Enerote Management UPnP	1	Нара на	Game Console VolP	XBox Live PlayStation MSN Game Zone Battlenet VolP	2 2 2 2 2 2 2 2 2 2 2
Wanagement Ecologic content free Renote Management UPoP	23	High w High w	Game Console VolP Instant Messenger	XBox Live PlayStation MSN Game Zone Battlenet VolP Instant Wessenger	2 2 2 2 2 2 2 2 2 2 2
United Free United States (United States) Rends Management United	2 3 4	High a High a High a	Game Console VolP Instant Messenger Web Surfing	Xitos Live PlayStation MSN Game Zone Battienet VolP Instant Messenger Web Surfing	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
 Content rate Banagement Bandonictin Management Brencte Management UPoP 	1 2 3 4 5	Migh a Migh a Migh a Migh a	Game Console VolP Instant Messenger Web Surfing P2P#TP	Xitos Live PlayStation MSN Game Zone Battlenet VolP Instant Messenger FTP	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Long Tener Long Statistical United Statistics Remote Management UPuP	1 2 3 4 5	High a High a High a High a	Game Console VolP Instant Messenger Web Surfing P2P#TP	Xitos Live PlayStation MSN Game Zone Battlenet VolP Instant Messenger FTP Huse Surting FTP Huse	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Hanagement Ensource Here Ensource Here Ensource Hanagement UPuP	1 2 3 4 5	High x High x High x High x	Game Console VolP Instant Messenger Web Surfing P2P#TP	XBox Live PlayStation MSN Game Zone Battlenet VodP Instant Messenger Web Sufing FTP eklule BitToment	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

Figure 39: Bandwidth Management Advanced Configuration Page

Remote Management WWW Configuration Page

This page allows for the configuration of WWW remote management.

F	Waxiem	
	CONFIGURATION open al close all Network UNAN LAN DHCP Server NAT CONS OpenDNS OpenDNS Security Frewal Frewal Banagement Banagement Banagement Banagement Banagement Banagement Banagement Banagement UNAP	Configuration > Management > Nummer Configuration > Management > Managemen

Figure 40: Remote Management WWW Configuration Page

Remote Management SNMP Configuration Page

This page allows for SNMP to be enabled. By default it is disabled. To utilize, define the community string for reading of monitoring parameters via SNMP, then click **Apply**.

F	Waxiem			Lassu
	CONFIGURATION open al close al Petwork Wiveless LAN UNICP Server NAT CONS OpenDNS Static Bode	Configuration = Management = Remote Management = SHAP SHAP SMAP Setup Chable SMAP SMAP Version Get / Set Community	vi m public	
	Securty Frewall Context Filter Management Management Randowdh Management WWW Emoto WWW UNU UNU		Heads	

Figure 41: Remote Management SNMP Configuration Page

Universal Plug and Play (UPnP) Service Configuration Page

This page allows for UPnP to be enabled. By default it is disabled. UPnP automates the creation of firewall rules, but the feature is not recommended for most customer application scenarios. Please contact your FW Support Representative to determine if this feature is appropriate for your application.

E	W/axiam	Loood
-	•••	
	CONFIGURATION	Configuration > Management > Univer > General
-	open all close all	General
0	Wreless LAN	Upol Salas
-	- WAN	Provide Name Faces AVVII
-	DHCP Server	Faste the Universal Rus and Ray (URIN) Feature
	- NAT	
	OpenDNS	
	Static Route	Apple Reset
	Frewal	
	- Content Filter	
	Bandwidth Management	
	Remote Management	
	- SNMP	
	- UPaP	

Figure 42: UPnP Service Configuration Page

Maintenance Options for Your CIRA X2 Access Point

The access point provides the ability for routine maintenance which is available by clicking the Maintenance icon located at the bottom of the listings on the far left of the page.



Maintenance General Settings Page

This page allows the user to set the **System Name** and the **Domain Name**. The page also provides the opportunity to configure the web interface timeout via the **Administrator Inactivity Timer**, which by default, is set to 5 minutes.

F	Waxism			Lasad
	MAINTENANCE open al close al Martenance - Deserve - Tene - Tene - Tenewer Upgrade - Backup / Restore / Reset - Backar/ - Sys OP Mode - Alert	Mantenance - General General System Setup System Name : Domain Name : Administrator Inactivity Timer :	AXOM feeneywireless.com 5 (minutes, 0 means no timeout)	
			(Apply) [Read]	

Figure 43: Maintenance General Settings Page

Password Settings Page

This page allows the user to set the system password. To do so, you need to enter the existing, or **Old Password**, then enter the **New Password**, and **Retype to Confirm**. Once all passwords have been entered, click **Apply** to save the settings.

I	Wax ie m			Lasa
	MAINTENAANCE open al close al Markinaanse General - Bratsausti - Tree - Firmware Upgrade Beackup / Resider Reset Resider Beackup / Resider Alexet Sign Of Mode Alext	Maniferance - Password - Password Setup Password Setup Old Password : New Password : Retype to Confirm :		1
			Epoty Reset	

Figure 44: Maintenance Password Settings Page

Time Configuration Page

This page provides the option to configure **Network Time Protocol (NTP)** to automatically set system time when a WAN connection is available. By default, this option is enabled with the time set to GMT.

Maintenance > Time > Time Setting	
open all close all Time Setting	
al Current Time and Date	
Current Time -	2148-48
are Upgrade Current Date :	2011-08-05
p / Restore / Reset 1	
P Mode Current Time and Date	
OManual	
New Time (hh:mm:ss) :	23 : 56 : 16
New Date (yyyy/mm/dd) :	2011 / 8 / 5
R Get from Time Server	
₽ Auto	
Ouser Defined Time Server Address :	192.5.41.41
Time Zone Setup	
Time Zone :	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London 💌
Dayight Savings	
start Date (mm/dd)	/ at erdeck
End Date	/ at stock

Figure 45: Time Configuration Page

Firmware Upgrade Configuration Page

This page provides the ability to upgrade the firmware of the access point via the web interface. Please contact your FW Support Representative if you are unsure of whether or not you are operating with the latest firmware.

NOTE: FW recommends that you update your firmware with a computer connected via Ethernet or Wi-Fi whenever possible.

F	Waxiem		Lessed
	MANTENANCE open al close al Mantenance - Ceneral - Password - Time - Extent loggrade - Backup / Restore / Reset - Says Of Mode - Alert	Maintenance > Finiware Upgrade Firmware Upgrade Upgrade Firmware Upgrade Firmware To upgrade Firmware To upgrade Firmware To upgrade file internal device firmware, browse to the location of the binary (BR) upgrade file and cick Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (2P file), you must first extract the binary (BR) file. In some cases, you may need to reconfigure. File Path: Choose File No file chosen	1
		Lyned	

Figure 46: Firmware Upgrade Configuration Page

System Configuration Backup/Restore/Reset Page

This page provides the ability to backup and restore system settings. Functionality for each is as follows:

- **Backup Configuration** allows the user to backup all of the user settings to provide a restore point should something occur to erase these settings.
- Restore Configuration allows the user to locate and upload the stored user settings should a factory reset occur.
- Back to Factory Defaults clears all user-entered configuration settings and restores the system to FW defaults.

System Restart Configuration Page

F	Waxlom	
	MAINTENANCE open all close all Maintenance - General - Pasaword - Time - Firmare Upgrade	Mandomance × Backup / Restore / Reset Backup / Restore / Reset Backup Configuration Cick Backup to save the current configuration of your system to your computer. Backup
	Deckup / Restore / Reset Restart Sys OP Mode Alert	Restore Configuration To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload File Path : Choose File, No file chosen Upload
		Back to Factory Defaults Cick Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the - Password will be freeneysp - LAN IP address will be 112:163.1.1 - DHCP will be reset to server Easet

Figure 47: System Backup/Restore/Reset Page

This option allows the user to set an access point reboot automatically after a certain number of hours have elapsed. By default, this option is set to 0, which disables the option.

With the option set to '0', clicking **Apply** will initiate a single reboot of the system.

F	Waxingm		Logout
	MARTI NANCE open all close all • General • Password • Time • Firmware Upgrade • Backup / Restore / Reset • Stys OP Mode • Alort	Maintenance > Restart	1

Figure 48: System Restart Configuration Page

System Operation Mode Configuration Page

This option allows the user to configure the operation of the system. Please see the page for a description of the settings.

ł			Legent
	MAINTENANCE open all (dose all e Maintenance - Georal - Pessword - Time - Premware Upgrade - Backup / Restore / Rest - Restart - Restart - Alert	Mantenance > Sys OP Mode Sys OP Mode Configuration Mode Router Node Router Node Note: Router in this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same P to ISP through WAN Port.	1
		Access Point. In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network. WIGP Node: In this mode, the device acts as a wireless client, it can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAK.	

Figure 49: System Operation Mode Configuration Page

System Alerts Configuration Page

This option allows for the configuration of system alerts.

F	-Waxlom		2055
	IMANTENANCE open all close all → Haantenance → Pessword → Time → Fremware Upprade → Backup / Restore / Reset → Backup / Restore / Reset → Sys OP Mode → Sys OP Mode		
		Apply Reset	

Figure 50: System Alerts Configuration Page

Using a Terminal Application with AT Commands

It is possible to access and configure your cellular modem using Microsoft HyperTerminal, PuTTY, or a similar terminal emulator application. The following are directions for use with Microsofts Hyperterminal. Please contact your FW Support Representative for instructions on using other terminal emulator applications.

Establish Your Connection

- 1. Choose a name and icon for your connection:
 - a. Choose a name for your connection, such as CIRA X2. The name and icon are only for your own reference so that the connection can be found easily at a later date.
 - b. Select OK.
- 2. At the Connect to window, using serial:
 - a. Select the COM port to which the device is connected, for the "Connect using" option.

Connect To		? 🔀	
🧖 Sierra W	rieless AirLink Solutions		
Enter details for	ihe phone number that you wa	nt to dial:	
Country/region:	United States (1)	2	
Area code:	510		
Phone number:	3		
Connect using	COM1	~	
	BCM V.92 55K Modem Standard 33600 bps Modem COM3		
	COM1 TCP/IP (Winspek)	hit	

Figure 51: Connect To Window

- b. Change or verify the settings when the **COM Properties** window appears:
 - Bits per Second: 115200 (default)
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: Hardware (or None)
 - **NOTE:** If you have configured your CIRA X2 via the ALEOS Configuration Guide for settings different than the defaults for Bits per Second, Data Bits, Parity, and/or Stop Bits, you must use your changed settings.
 - Select **OK**

10 -		
Bits per second	115200	×
Data bits	8	*
Parity	None	~
Stop bits	1	~
Flow control	Hardware	~
	_	

Figure 52: Port Settings

AT Commands

For a full listing of supported AT Commands, please reference the ALEOS User Guide available at: http://www.sierrawireless.com. When using a terminal application, you will need to manually type in each command.

- For most commands, when you are entering them using a terminal connection, you will need to preface the command with *AT* (exceptions are noted), i.e., *ATA* which is listed as *A*.
- Some commands have specific parameters while other commands will take whatever you type.
- Required variable parameters are denoted with italicized text, example, Dn. The n is variable.
- Acceptable parameters and/or specific formats are listed with each command
- Most commands with parameters can be entered with ? to read the current value. For example AT&D? will respond with "2" if the default has not been changed.
- Optional parameters are denoted with square brackets [].
- AT Commands are not case sensitive.
- When you are using a terminal connection, if you enter a command which is recognized by the CIRA X2, it will respond with "OK". If the command is not recognized, the response will be "ERROR".
- Any commands applicable only to certain model numbers of the CIRA X2 will be noted.

NOTE: Symbols listed with commands, such as *, /, &, or ?, are part of the command and must be included. Commands with symbols other than * may require PassThru mode.

USB Port Connection

As mentioned in the CIRA X2 Quick Start Guide, the device can be configured to support redundant 3G. For confirmation of supported devices, please contact your FW Support Representative. For information on configuring your device to operate with a USB Mobile Cellular connection, please see the section entitled 'Mobile WAN Configuration Page' on page 14.

Contacting FW

For help with installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided.

If you still have questions, contact us during business hours:

Monday through Friday, excluding holidays, between 8 a.m. and 5 p.m. Pacific Time.

Support E-mail	support@feeneywireless.com
Telephone	(800) 683-4818
Website	www.feeneywireless.com
Mailing Address	P.O. Box 2549, Eugene, OR 97402

When contacting technical support, please have the following information on-hand:

- 1. Serial Number
- 2. Date that you received your device
- 3. Brief description of the problem

Online Library

For other documentation, see our online document library at: http://feeneywireless.com/documents

Return and Warranty

FW offers a standard one-year warranty on all hardware. For returns or warranty information, call our 800 number.

Further Specifications

For more specifications please see the CIRA X2 Quick Start Guide.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication. FW does not guarantee that interference will not occur in a particular installation.

Operation is subject to the following conditions:

- a. This device may not cause harmful interference.
- b. This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

If this equipment does cause harmful interference to radio or television reception, which can be determined by tuning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- a. Reorient or relocate the receiving antenna.
- b. Increase the distance between the equipment and the receiver.
- c. Connect the equipment to outlet on a circuit different from that to which the receiver is connected.
- d. Consult the dealer or an experienced radio/TV technician for help.

Exposure to RF radiation - To comply with FCC RF exposure compliance requirements, for mobile configurations, a separation distance of at least 20cm must be maintained between the antenna of this device and all persons. Do not collocate or operate this device in conjunction with any other antenna or transmitter.

Contains TX module FCC ID: N7N-MC7750 Contains TX Module IC: 2417C-MC7750