Alliant Networks

Cellular Gateway

User Guide

Version 1.4

Document version: 23

Product and technical information in this document is subject to change without notice and does not represent a commitment on the part of Alliant Networks, Inc.

Export restrictions: OpenSSL software uses strong cryptography, and it falls under certain export/import and/or use restrictions in some parts of the world. IT IS YOUR RESPONSIBLITY TO OBEY THESE LAWS.

REGULATORY COMPLIANCE INFORMATION

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications not expressly approved by, Alliant Networks, Inc. could void the user's authority to operate the equipment.

NOTE: 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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Exposure to Radio Frequency Radiation

To comply with RF safety requirements, please maintain a separation distance of 20cm from the antennas located on the sides of the device.

The internal wireless radio operates within guidelines found in radio frequency safety standards and recommendations, which reflect the consensus of the scientific community. Alliant Networks, Inc. therefore believes the internal wireless radio is safe for use by consumers. The level of energy emitted is far less than the electromagnetic energy emitted by wireless devices such as mobile phones. However, the use of wireless radios may be restricted in some situations or environments, such as aboard airplanes. If you are unsure of restrictions, you are encouraged to ask for authorization before turning on the wireless radio.

ONE-YEAR LIMITED WARRANTY

Alliant Networks Inc., networking products are warranted to be free of defects in material and workmanship for one year from date of purchase.

Alliant Networks Inc. will, at its election, repair, or replace or make appropriate adjustment where Alliant Networks, Inc. inspection discloses any such defects occurring in normal usage within the warranty period. Alliant Networks Inc. is not responsible for removal shipping, or installation costs.

IMPLIED WARRANTIES INCLUDING THAT OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY LIMITED IN DURATION TO THE DURATION OF THIS WARRANTY. ALLIANT NETWORKS, Inc., DISCLAIMS ANY LIABILITY FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES. Some states/provinces do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of special, incidental or consequential damages so these limitations and exclusions may not apply to you. This warranty gives you specific legal rights. You may also have other rights which vary from state/province to state/province.

This is our exclusive written warranty.

WARRANTY RETURN POLICY

If you have a problem with your product, please call Alliant Networks Technical Support at 408-744-1500. Alliant Networks Technical Support will assist with resolving any technical difficulties you may have with your product.

After calling Alliant Networks Technical Support, if your product is found to be defective, you may return the product to Alliant Networks after obtaining an RMA (Return Merchandise Authorization) number from Alliant Networks Customer Service. The product must be returned in its original or secure packaging. The RMA number should be clearly marked on the outside of the box. Alliant Networks cannot be held responsible for any product returned without an RMA number, and no product will be accepted without an RMA number.

RIGHT TO CHANGE

Alliant Networks, Inc. reserves the right to make changes without notice to any products herein for any reason at any time, including but not limited to improving the reliability, form, fit, function or design. Alliant Networks does not assume any liability arising out of use, misuse or application of any product or circuit described herein, nor does it convey any license under its patent rights nor the rights of others.

Information and specifications in this manual are checked, however no responsibilities for inaccuracies can be assumed by Alliant Networks. Please consult an Alliant Networks salesperson to obtain the latest specifications before placing your order for Alliant products.

LIFE SUPPORT POLICY

Alliant Networks' products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Alliant Networks product could create a situation where personal injury or death may occur. Authorization for such use may only be given in the form of express written approval of the president of Alliant Networks.

Should the buyer or user purchase or use Alliant Networks products for any such unintended or unauthorized application, both buyer and user shall indemnify and hold harmless Alliant Networks and its officers, employees, subsidiaries, affiliates, suppliers, and distributors against all claims, costs, damages, and expenses, and attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Alliant Networks was negligent regarding the design or manufacture of the device, or was aware of a defect that could cause malfunction.

FCC WARNING

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 in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio Technologies. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

This device contains an 802.11b/g transmitter which has been approved under FCC certification, with FCC ID: SHE-WL007.

When used with a Cellular PC Card, the Cellular Gateway can be considered a co-transmitting device. The following are power density estimates under this configuration:

1. Maximum EIRP for possible Cellular 1900 Co-transmitter is 4.79 W
2. Maximum EIRP for possible Cellular 850 Co-transmitter is 2.7 W (1.64 W ERP)

EUROPEAN TELETECHNOLOGIES STANDARDS INSTITUTE

Statement of Compliance

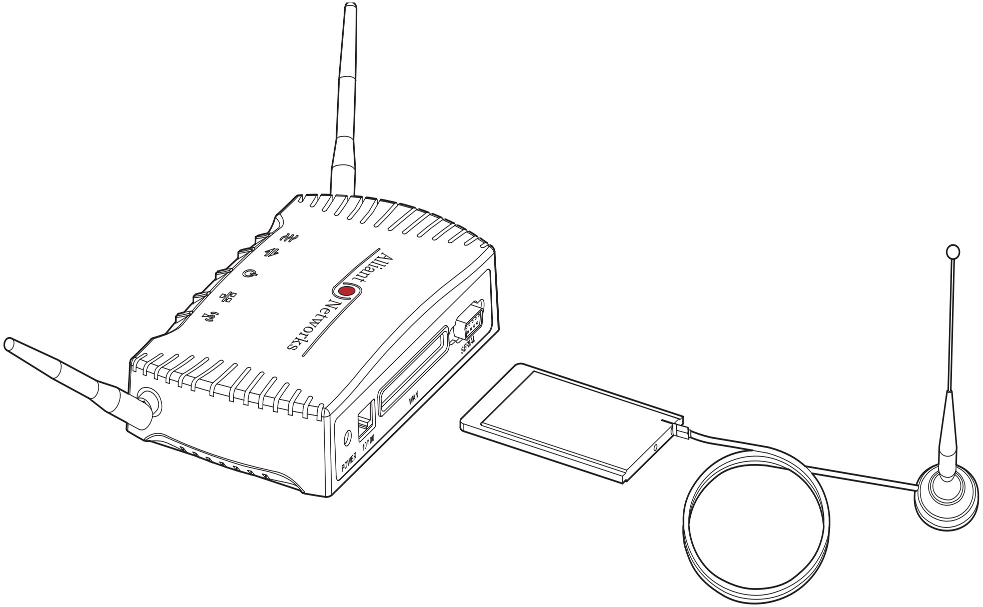
Information to User

This equipment has been tested and found to comply with the European Telecommunication Standard ETS 300.328. This standard covers Wideband Data Transmission Systems referred to in the CEPT recommendation T/R 10.01. This type of accepted equipment is designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial 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 Technologies.

Contents

Introduction

The Alliant Networks Cellular Gateway combines the convenience of standard networking with the flexibility and coverage of cellular networks. Using the gateway, anyone can set up an instant personal network and connect to the Internet from any location that supports cellular phone service.



FCC regulations require the use of an external antenna with the Cellular PC Card. The cellular antenna must be located at least 20cm from the wireless LAN antennas.

Although it is simple to install and easy to use in its default configuration, the gateway can be configured for sophisticated machine-to-machine communication applications. It extends the serial interface across the cellular network to IP-based protocols, so that sensing, mechanical, and control devices can report to Internet computers.

For those who only need quick and reliable Internet access, the gateway is ready to use right out of the box. For users with more complex requirements, the gateway offers both Web-based, SNMP and Command Line Interface configuration tools.

By uniting three networking media—Ethernet, serial, and cellular—the gateway can provide Internet access to embedded products that are difficult to network with conventional wired solutions. Equipment that generates Ethernet or serial data can communicate with computers on the Internet by making a data connection to the cellular service provider. The gateway does not interpret serial data, thereby eliminating the need to modify legacy products to allow them to leverage its features.

Cellular access standards

The Cellular Gateway comes in three different models; identified in the table below. Different cellular service providers employ different access standards for carrying data over the cellular network. Your choice of gateway depends on the service provider you have chosen. The CGW101 and CGW102 contain an internal radio.

The CGW103 requires an additional PCMCIA/PC Card that can be either GPRS or CDMA 1.x. The list of supported PC Cards are shown in the CGW103 row.

Installation depends on the model and is covered in Installation Instructions on page 29.

Model	Standard	Cellular service providers
CGW101	GPRS	T-Mobile AT&T Wireless

Model	Standard	Cellular service providers
CGW102	CDMA 1x	Sprint Verizon
CGW103	Depends on the PC Card.	Verizon Wireless AirDirect 555D

Supported PC Cards

The CGW103 product requires a PC Card with an associated cellular-with-data plan, which can be purchased from an appropriate cellular store or qualified reseller. Some PC Cards come with a SIM. Refer to the PC Cards installation for more detail. The table below lists Along with the PC Card a cellular-with-data plan is also required. A PC Card may also required a SIM ch

PC Card	Standard	Cellular service providers
CGW101	GPRS	T-Mobile AT&T Wireless
CGW102	CDMA 1x	Sprint Verizon
CGW103	Depends on the PC Card.	Verizon Wireless AirDirect 555D

Operating components

- **LAN gateway**

  Like home gateway, cable, or DSL modems, the Cellular Gateway provides Internet connectivity for one or more computers over a standard wired Ethernet connection or through 802.11 wireless association. Because it forwards standard IP traffic onto the

Internet, no special software is needed on the computers or devices inside or outside the gateway. (Devices connected to the gateway through the Ethernet or serial ports or through wireless association are considered to be *inside* the gateway. Computers connected to the Internet (but not to the gateway itself) are considered to be *outside* the gateway.)

The gateway is well-suited for local area network (LAN) applications where Internet connectivity is required and alternative connections are not available due to technical or economic constraints, or to the need for mobility.

You can set up a LAN quickly and easily using the gateway in its default configuration. The gateway performs Network Address Translation (NAT) to support a full IP subnetwork with one cellular connection. Connections to the outside must be initiated by an inside device, providing protection against unsolicited connection. Once a connection is established, data can flow in both directions.

- **Serial passthrough**

  The Cellular Gateway extends the serial interface across the cellular network to IP-based protocols, so that sensing, mechanical, and control devices can report to Internet computers. The connection protocol is configurable (TCP or UDP). The gateway does not interpret or change serial data.

Example applications

- **Mobile LANs**

  The Cellular Gateway is not tethered to any wired infrastructure, so you can create an instant personal network with Internet connectivity wherever needed. Because it works anywhere that has cellular-with-data service, it can be installed in mobile environments such as trucks, recreational vehicles, and even boats.

- **Convenience LANs**

The Cellular Gateway requires no installation of telephone, DSL, or cable lines. The gateway is ideal for situations that require fast, easy connection to the Internet, such as emergency and disaster relief teams, remote field offices, construction trailers, and booths at trade shows and conventions.

- **Machine status**

  Because it is completely self-contained and does not require a wire to make a data connection, the gateway is ideal for embedding inside devices such as vending machines, as part of a sensing and control network. The I/O lines on the gateway can be used to report inventory and digital status information. The thermocouple can be used to report the temperature of the refrigerated or ambient sections of the machine.

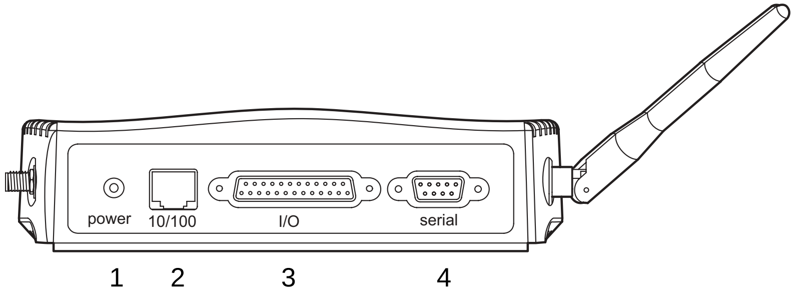
- **Telemetry**

  The gateway allows remote or inaccessible test and measurement equipment to report data back to a central location. It can support power line sensors, electric and gas meters, and a host of other specialized devices.

Hardware description

Back panel

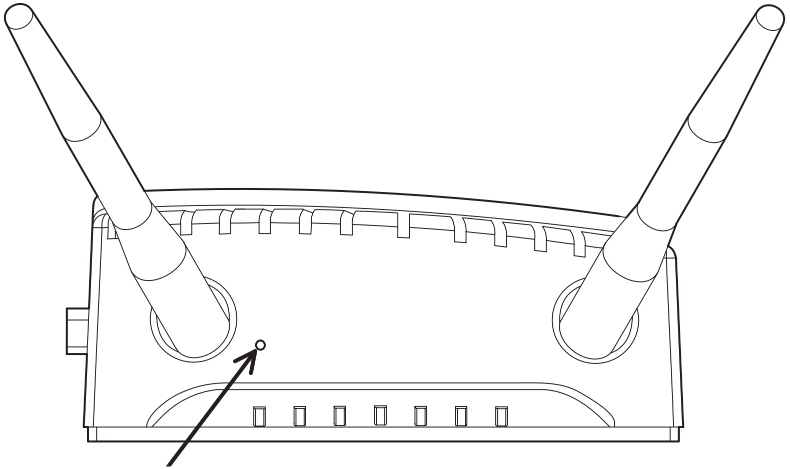
The various ports and the power connector are located on the back panel, as shown and described below.



Item	Description
1. Power connector	For use with the supplied 12 volt DC power supply at 25 Watts.
2. Ethernet port	10/100 Ethernet with auto-negotiation and auto MDI/MDIX crossover.
3. I/O passthrough port	Used for serial bridging to the DB25 digital I/O interface. For more information, see the *Advanced Operations Guide*.
4. Serial port	High speed DB9 UART supports serial data transfer at the following baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200.

Configuration button

The Configuration button is located on the side of the unit, as shown.



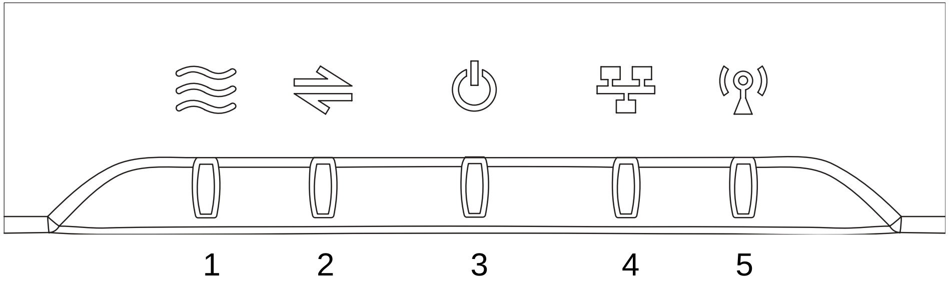
You can use the Configuration button to restore the software to factory defaults or, if serial passthrough is running, to disable it so that you can use the serial command line interface.

Insert a pointed object (such as the end of a straightened paper clip) into the reset hole to press the button.

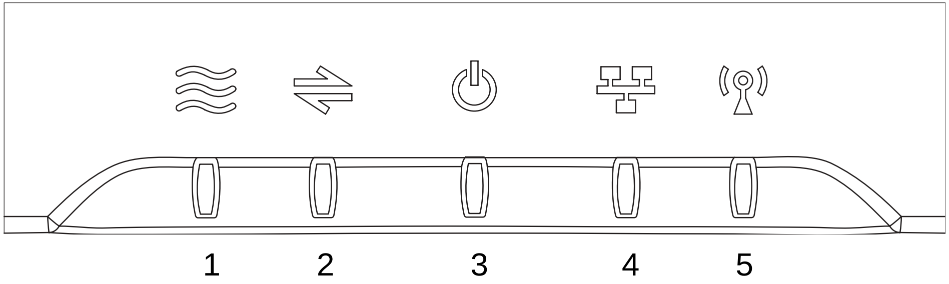
- To restore to factory defaults: Press and hold the button for 5 seconds.
- To disable serial passthrough and put the serial CLI command mode: Press and release the button.

LEDs

When power is connected, the LEDs on the front panel light to indicate the operating conditions, as shown and described below.



LED	Description
1. 802.11 Wireless Signal Strength/Activity	GREEN. Faster blinking indicates greater activity.
2. Serial (UART) Activity	GREEN indicates transmission. YELLOW indicates reception.
3. Power/Error	GREEN indicates that the gateway is receiving power. YELLOW indicates CPU error.
4. 802.3 Wired Ethernet Link Speed/Activity	GREEN indicates 100 Mbps YELLOW indicates 10 Mbps Faster blinking indicates greater activity.



LED	Description
5. Cellular Signal Strength/Activity (GPRS or CDMA)	GREEN indicates excellent signal. YELLOW indicates good signal. RED indicates poor signal. Faster blinking indicates greater activity.

Features and specifications

The major features of the Cellular Gateway are described in the following sections.

Wired or wireless LAN support

The gateway supports 802.3 wired Ethernet and 802.11 wireless LANs. The wireless feature complies with IEEE 802.11b and 802.11g standards, ensuring interoperability with third-party wireless equipment that also complies with these standards.

Web management interface

You can configure and manage the gateway through your Web browser. A Java-based discovery utility assists in connecting to the gateway configuration user interface during initial setup.

Secure network authentication

The gateway provides a variety of options for authentication. It can act as either a supplicant to another authenticator, or it can act as an authenticator for 802.11 clients.

When acting as a supplicant, the gateway requests authorization from an authenticator to be on the network. Acting as an authenticator, the gateway processes requests for network authentication from clients, and allows or disallows the client access to the network as a result. Authentication is achieved using either the IEEE 802.1X standard or the IEEE 802.11i standard, depending on the configuration.

Network encryption

The gateway can also provide encryption for 802.11 wireless links. To support legacy equipment, Shared Key WEP is supported, though not recommended. Other encryption support includes Pairwise Key WEP, Robust Secure Network (RSN) TKIP, Robust Secure Network (RSN) AES, Wireless Public Access (WPA) TKIP, and Wireless Public Access (WPA) AES. These options are described in more detail in 802.11 Encryption on page 56.

Network address translation (NAT)

NAT is an Internet standard that enables the network inside the gateway to use one set of IP addresses for inside traffic and a single second address for outside traffic, resulting in two main benefits:

- Provides a level of security by hiding internal IP addresses and blocking connections from outside devices.
- Enables the use of any set of IP addresses for the inside network. Because the addresses are only used internally, there is no possibility of a conflict with outside IP addresses.

The gateway allows up to 1024 simultaneous connections with outside computers.

DHCP server

The Dynamic Host Configuration Protocol (DHCP) provides a means for IEEE 802.3 client devices to receive IP addresses for the network. A DHCP client computer (or other type of network device) begins by asking a DHCP server for an IP address. The server provides an address, creates a lease period for that client, and keeps track of the address assigned to that client. The client then uses that IP address and periodically renews the lease if it exceeds the lease period.

You can specify the following major DHCP server features:

- A range of IP addresses to be assigned to clients (known as the address pool).
- The domain name.
- The primary and secondary DNS servers (or you can defer to values retrieved over the cellular connection).
- The lease period.

The gateway DHCP server allows up to 1024 DHCP clients.

DHCP Client

The device can also act as a DHCP client to be configured by an existing DHCP server.

DNS proxy

DNS proxy allows the device to handle and forward DNS requests to remote DNS servers. This allows inside clients to use convenient naming such as www.alliantnetworks.com when addressing remote computers.

Backup and restore

The gateway provides a means of backing up and restoring its configuration via TFTP. It is prudent to back up the gateway configuration before altering functionality.

Firmware upgrade

From time to time new firmware with improvements to gateway functionality becomes available. The gateway provides a means of upgrading firmware via TFTP.

Advanced operations features

SNMP

You can configure and manage the gateway through the Simple Network Management Protocol (SNMP) using any MIB browser. Parameters are stored in MIBs (Management Information Base), which provide a standard format for accessing data of various types. The gateway supports versions 1, 2c, and 3 of the SNMP protocol. SNMP V2c adds additional error status reporting over SNMP V1, while SNMP V3 adds secure authentication and encryption for reading and writing MIBs. For more information, see the *Advanced Operations Guide*.

Serial and Telnet command line interface

You can configure and manage the gateway through a Command Line Interface (CLI), which provides access to every configurable aspect of the product. There are two ways to connect to the gateway and access the CLI:

- Through the DB9 interface (serial CLI)

  The serial CLI shares the DB9 interface with the serial passthrough feature. If serial passthrough is running, pressing and releasing the configuration button disables serial passthrough and brings up the serial CLI. The default serial settings are 38400 N-8-1.

- Over Ethernet (Telnet CLI)

  The Telnet CLI allows access from any computer connected directly or indirectly to the 802.3 port on the gateway. The Telnet CLI allows only one connection at a time.

The two access mechanisms provide access to the same set of CLI commands. For more information on the CLI, see the *Advanced Operations Guide*.

SYSLOG

SYSLOG is the standard protocol described in RFC 3164 for logging system events. It was initially used by Unix systems and is now commonly used by switches, routers and other embedded devices. Using SYSLOG, you can send a log of system events to a SYSLOG server, centralizing important management information.

Two important aspects of system events are severity and message. The gateway provides functionality for filtering out events based on severity and for specifying multiple SYSLOG servers to receive event logs.

A limited amount of SYSLOG information is stored in the gateway using on-board logging, which provides the same filtering functionality and allows you to view events through the CLI.

Serial passthrough

The serial passthrough converts serial data from the DB9 interface to IP network traffic. With this passthrough, a TCP or UDP socket-based application can communicate with a serial device. The gateway does not interpret or change any of the serial data. For more information, see the *Advanced Operations Guide*.

I/O passthrough

The I/O passthrough converts data from the DB25 interface to IP network traffic. Like serial passthrough, this type of passthrough supports the connection modes TCP Connect, TCP Listen, and UDP. For more information, see the *Advanced Operations Guide*.

Data transfer protocol

The I/O passthrough data format uses XML to transfer information between the remote host and the bridge. For more information, see the *Advanced Operations Guide*.

About this guide

This guide is intended primarily to be viewed on your computer, and it provides *hot links* to referenced topics. If you print this guide, references and indexes list page numbers, so you can easily find referenced topics by turning to the listed page number.

Turn or jump to the following topics for more information:

- For detailed installation instructions, see Installation on page 28.
- For a description of the Alliant Web Configuration Interface, which allows you to configure device features, see Using the Web Configuration Interface on page 39.

- For a description of the CLI structure and an exhaustive list of CLI commands, see the *Advanced Operations Guide*.

Contact information

Alliant Networks technical support:

Email: support@alliantnetworks.com

Telephone: 408-744-1500 (extension 112)

Installation

The Cellular Gateway must be installed in a location that has access to a standard 110 V power outlet and is within the coverage area of your cellular service provider.

Make sure the gateway model you have chosen matches the access standard used by your cellular service provider. For details, see Cellular access standards on page 14.

Once installed, the gateway is ready for use as an Internet gateway. If further configuration is necessary, the gateway can be configured through its Web-based configuration interface. For details, see Using the Web Configuration Interface on page 39.

For more sophisticated applications, see the *Advanced Operations Guide*.

Package contents

In addition to the gateway itself, the following items are shipped with all models:

- Basic Setup Guide
- CD containing documentation, firmware and the Alliant Discovery Tool.
- DB9 serial modem cable
- Ethernet cable
- DC power supply
- Cellular antenna

Installation Instructions

The installation instructions depends on the product. The directions below provides details on how to setup and install software for the Cellular Gateway GPRS, Cellular Gateway CDMA and Cellular Gateway PC Card.

Once setup, install software, connecting to an existing LAN and customization are all the same. Discussions of these topics start on page page 35.

Cellular Gateway GPRS CGW101

Other requirements

- A cellular-with-data service contract with a cellular service provider whose data protocol is compatible with the gateway. All cellular-with-data service contracts require an IMEI number. The Cellular Gateway IMEI number is located on the bottom of the device as a bar code labeled IMEI.The number is unique to each product and is used by the cellular carrier to track your product.

  If you are purchasing a T-Mobile plan, make sure to ask for an appropriate APN (for example, internet2.voicestream.com). The APN is specific to the type of data plan. T-Mobile users must configure the gateway with this APN. This extra step is not required for AT&T data plan users.

  See the list of providers in Cellular access standards on page 14.
- The Cellular Gateway 1000 requires a GPRS cellular SIM card, received when you purchase a cellular-with-data service contract. The SIM card enables the gateway to communicate with the cellular network. (The Cellular Gateway 1100 does not require a SIM card.
- For LAN connection, your computer must be equipped with a 10/100 Mbps Ethernet network interface card or a compatible 802.11 PCI or PCMCIA wireless card.

Installation steps

The basic installation of the Cellular Gateway involves attaching the cellular antenna, connecting power, and making a LAN connection (wired or wireless).

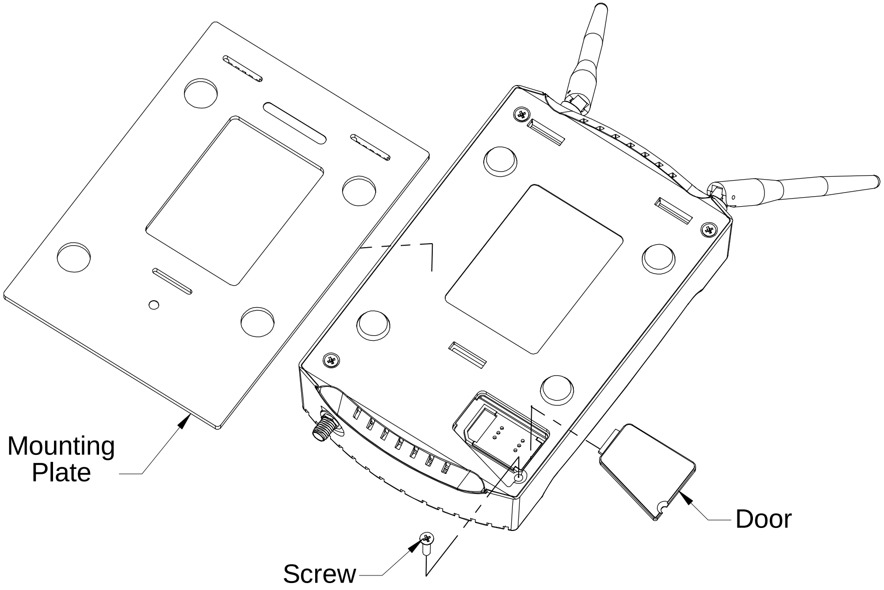
The Cellular Gateway 1000 requires that you first install a GPRS cellular SIM card (not provided) into the gateway. Instructions for installing the SIM card are given in Installing the SIM card (model 1000 only), below. The Cellular Gateway 1100 comes with a CDMA 1x cellular SIM card already installed.

Installing the SIM card (model 1000 only)

Refer to the illustration below and follow these steps to insert the SIM card:

1. Disconnect the gateway from power and place it on a flat work surface.

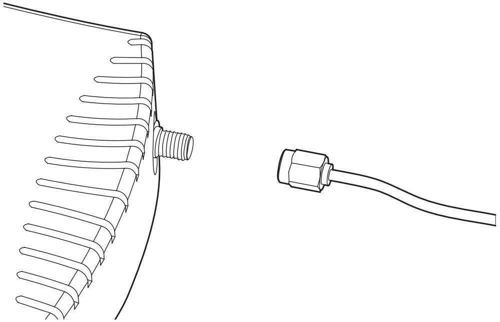
2. If the gateway is attached to the mounting plate, remove the mounting plate. Grasp the mounting plate and pull to release it from the unit.
3. Locate the removable Door (see illustration).
4. Remove one screw (see illustration) and remove the Door to reveal the SIM card hatch. Set the Door and screw aside.
5. Slide the SIM card hatch lid to the Open position.



6. Lift the hatch lid.
7. Align the SIM card to the guides in the hatch. Make sure the gold connectors on the card are facing down. The card's gold connectors must make contact with the hatch's gold pins.
8. Lower the hatch lid and slide the hatch lid to the Closed position.
9. Replace the Door and the screw.

Attaching the cellular antenna

To attach the antenna, insert the SMA connector on the end of the antenna cord into the connection point on the side of the gateway and hand-tighten the thumbscrew. To minimize interference, place the cellular antenna as far away as possible from the 802.11 antennas. (See the illustration on page 13.)



Connecting power

Connect the provided power supply to the gateway power port and to a standard 110 V power outlet. (For the location of the power connection on the gateway, see Back panel on page 17.) When it is connected to power, the LEDs light. For a description of the LEDs, see LEDs on page 20.

Cellular Gateway CDMA Model CGW102

Other requirements

- A cellular-with-data service contract with a cellular service provider whose data protocol is compatible with the gateway. All cellular-with-data service contracts require an IMEI number. The Cellular Gateway IMEI number is located on the bottom of the device as a bar code labeled IMEI.The number is unique to each product and is used by the cellular carrier to track your product. See the list of providers in Cellular access standards on page 14.

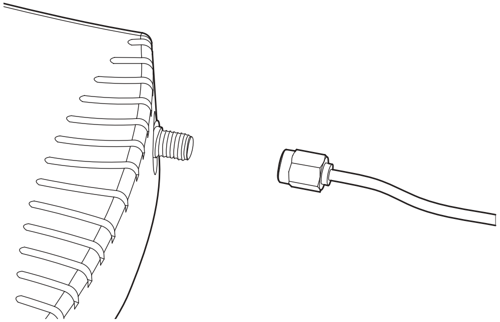
- For LAN connection, your computer must be equipped with a 10/100 Mbps Ethernet network interface card or a compatible 802.11 PCI or PCMCIA wireless card.

Installation steps

The basic installation of the Cellular Gateway involves attaching the cellular antenna, connecting power, and making a LAN connection (wired or wireless).

Attaching the cellular antenna

To attach the antenna, insert the SMA connector on the end of the antenna cord into the connection point on the side of the gateway and hand-tighten the thumbscrew. To minimize interference, place the cellular antenna as far away as possible from the 802.11 antennas. (See the illustration on page 13.)



Connecting power

Connect the provided power supply to the gateway power port and to a standard 110 V power outlet. (For the location of the power connection on the gateway, see Back panel on page 17.) When it is connected to power, the LEDs light. For a description of the LEDs, see LEDs on page 20.

Cellular Gateway PC Card Model CGW103

Other requirements

- The Cellular Gateway PC Card requires a PC Card. The Verizon Wireless AirDirect 555D is the supported card for this product. This card can be purchased from any Verizon store or qualified reseller.
- A cellular-with-data service contract with a cellular service provider whose data protocol is compatible with the gateway. A service plan can be purchased from any Verizon store or qualified reseller.
- For LAN connection, your computer must be equipped with a 10/100 Mbps Ethernet network interface card or a compatible 802.11 PCI or PCMCIA wireless card.

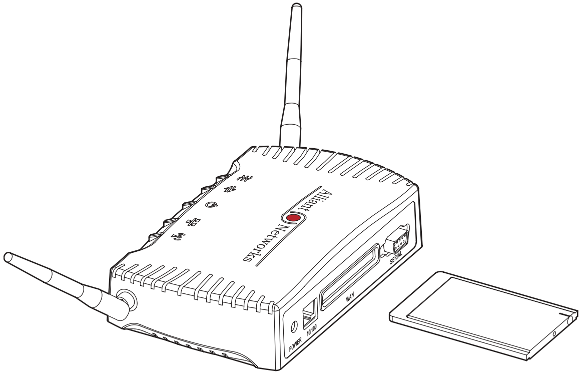
Installation steps

The basic installation of the Cellular Gateway involves inserting the PC Card, attaching the cellular antenna, connecting power, and making a LAN connection (wired or wireless).

Insert the PC Card.

Refer to the illustration to the right and follow these steps to insert the PC card:

1. Disconnect the gateway from power and place it on a flat work surface.
2. Insert PC Card in the slot located in the back of the gateway.



Connecting power

Connect the provided power supply to the gateway power port and to a standard 110 V power outlet. (For the location of the power connection on the gateway, see Back panel on page 17.) When it is connected to power, the LEDs light. For a description of the LEDs, see LEDs on page 20.

Installing Software

The CD provided contains manuals and a few other advanced items. Insert the CD into the CD drive and follow the directions. For home use the minimal installation is adequate. The maximum install and custom provide an additional discovery tool usually only needed in a corporate environment.

LAN connection

You can use the gateway in its default configuration as the Internet gateway for one or more computers equipped for wired Ethernet connection or wireless LAN association. It is assumed that your computer is configured to acquire its IP address from a DHCP server.

Refer the applicable instructions below.

Wired Ethernet

This method of connection requires that you have a 10/100 Mbps Ethernet network interface card installed in your computer. Connect one end of the provided Ethernet cable to the Ethernet port on the gateway and the other end to the Ethernet port on your computer. (For the location of the Ethernet port on the gateway, see Back panel on page 17.)

Wireless LAN

This method requires that you have an 802.11 capable computer or a 802.11 wireless PCI or PCMCIA card installed in your desktop or laptop computer. The wireless settings listed below are compatible with the gateway in its default configuration. (For information on configuring your card, consult the manufacturer’s documentation.)

- IP Network Settings: obtain automatically (DHCP Client)
- ESSID: attach to any ESSID automatically or specifically use CellularGateway
- Security Setting: no security (open system)

Connecting multiple Ethernet computers

In order to connect multiple computers with Ethernet, you must purchase a 10/100 hub or switch and additional Ethernet cables. This product works with all hubs and switches. Connect the Uplink port on your hub or switch to the 10/100 port of the Cellular Gateway. Use additional cables to connect your computers to the hub.

Customizing your gateway

The gateway provides Internet access once you have configured the cellular connection. There are three ways to configure it:

- Through the Web Interface, which allows you to configure many features using your Web browser, as described in Direct browser access below.
- Through the Alliant Networks Discovery Tool, which must be installed from the CD.This tool finds the gateway then launches your web browser for configuration, as described in Using the Discovery Tool below.

- Through the Command Line Interface, which allows access to all features. This tool, which is meant only for the most sophisticated configuration tasks, is described in the *Advanced Operations Guide*.

Direct browser access

If the gateway is set to the factory defaults and your computer is set to acquire its IP address from DHCP, follow these steps:

1. Connect the gateway to your computer as described in Wired Ethernet or Wireless LAN sections.
2. Turn on your computer in order to acquire an IP address from the gateway.
3. Launch your browser and point it to http://192.168.0.1 (the gateway's default IP address).

   You will be prompted for a user name and password. The default password is: public. The default user name is admin. The configurable items are described in Using the Web Configuration Interface on page 39.

   T-Mobile users must follow the instructions in the next section.

Configuring the GPRS Connection (T-Mobile only)

If you purchased a T-Mobile cellular data plan, an additional step is required to enable the gateway. T-Mobile must provide you with the appropriate APN and you must add the APN to the device configuration. If you do not know your APN, contact T-Mobile customer support.

To add the APN to the gateway configuration, follow these steps:

1. From the Web pages, Click *Network*.
2. In the Network page, click *GPRS*.
3. In the GPRS page, locate the APN field and enter the APN you received from the service provider. (An example APN is internet2.voicestream.com.)
4. Click *Change*.

After about 60 seconds, you should be able to browse the Internet.

Using the Discovery Tool

Selecting maximum or custom will install the Alliant Discovery Tool. The Discovery Tool helps you find and configure the gateway. This tool is usually only needed when installing the gateway in a corporate environment, the gateway has already been configured and the IP information is unknown or on a non 192.168.X.X subnet.

1. To install the Alliant Networks Discovery Tool select custom or maximum installation. During the installation you will be prompted to install Java as well.
2. Start the discovery tool, select the gateway, and right-click to launch the configuration. (If a password is set on the gateway, enter it when prompted. The default user name is admin and the default password is public.) The configurable items are described in Using the Web Configuration Interface on page 39.
3. To launch the Alliant Discovery Tool

   Under start, Programs, Alliant, CG 1000, select Discovery Tool.

   The Discovery Tool window appears.
4. Select the Discovery Devices button. The gateway should appear below.
5. Right mouse-click and select browser(user) to launch you web browser. Now you can use the Web interface to configure the device, see Using the Web Configuration Interface on page 39.

After you change and save the configuration, disconnect the gateway from the computer and connect it in its permanent place in the network. If you have difficulty discovering the device connect your computer directly to the gateway with the supplied Ethernet cable.

Using the Web Configuration Interface

If the configuration that was set at the factory does not meet your network requirements, or if you want to customize the settings, you can use the Alliant Networks Web Configuration Interface to change the configuration.

Launching a gateway configuration

You can only configure gateways that are on the same subnet as your computer. The installation instructions assume that your computer is configured to acquire its IP address from a DHCP server. This guarantees that your computer and the gateway have the same IP information, because when it is connected to the gateway, your computer acquires its IP information from the gateway. If your network does not allow this situation, the Alliant Discovery Tool can help you find and configure the gateway.

The two ways to launch a gateway configuration are described below.

Direct browser access

Make sure that the gateway is either wired to the same network, associating with the same wireless network, or connected directly to the computer, and that the gateway is connected to power.

If you know that the gateway is on the same subnet as your computer, and you know the gateway IP address, enter the IP address in your browser address pane. (The factory default IP address is 192.168.0.1.) The gateway Web configuration start page appears in your browser window. (The default user name is admin and the default password is password.)

Using the Discovery Tool

Initially, the gateway may not match your network's subnet. This prevents your computer from accessing the gateway configuration web pages. The Alliant Discovery Tool solves this problem by finding the gateway on your network and allowing you to assign it an IP address on the same subnet as your computer, and launch the gateway configuration pages in a Web browser. The Discovery Tool must be installed on a computer that has an Ethernet adapter or a wireless card.

After the Discovery Tool is installed on your computer (see Using the Discovery Tool), make sure that the gateway is either wired to the same network, associating with the same wireless network, or connected directly to the computer, and that the gateway is connected to power. If more than one gateway is connected, make a note of the MAC address of the gateway you want to select so that you can identify it in the Discovery Tool.

1. To launch the Alliant Discovery Tool:

   Windows: Select *Start /Programs /Alliant / Discovery Tool*.

   Unix: From a shell, enter the following command: **discHost**

   The Discovery Tool window appears.

2. Click *Discover devices*.

   All detected Alliant Networks gateways on the network are listed in the Device List pane.

3. In the Device List pane, select the gateway you want to configure. If more than one gateway is listed, you can identify the one you want by its MAC address. To select the gateway, click anywhere in its listing.

   In the Device Properties list, make a note of the gateway IP address and subnet mask. Enter a new IP address in the space provided. (The default is: 192.168.0.1)

   Optionally, you can enter the Subnet mask for the gateway.

4. Right click anywhere in the Discovery Tool window to launch the Web configuration interface.

The gateway Web configuration start page appears in your browser. (If a password is set on the gateway, enter it when prompted. The default user name is admin and the default password is password.)

5. Change the configuration as desired, and save the changes.
6. Back in the Discovery Tool, click *Discover devices*.
7. Locate the gateway and restore the IP address, subnet mask, and gateway to their original settings.
8. To end the Discovery Tool session, select *File:Exit*.

The following table describes the functions of the buttons in the Alliant Discovery Tool window.

Item	Description
File menu	Contains the Exit command, which ends the Discovery Tool session.
Edit menu	Contains the following commands:
	Configure: Sets the browser. Enter one of the following browser names (in lower case characters) for the Browser Application: iexp, mozilla, or netscape.
	ADP (Alliant Discovery Protocol):
About	Displays the version of the Discovery Tool.

About the Web configuration interface

The interface has a row of links across the top that lead to major configuration pages. Each major page has an associated menu of links on the left browser pane. The menu links lead to subpages, which are displayed to the right. On each subpage, you can change properties by entering values in the fields, selecting from lists, and clicking radio buttons.

Configuration pages have two buttons, *Change* and *Revert*, which function as follows:

- *Change* stores the settings permanently in the device nonvolatile memory. After you click *Change*, the new configuration settings take effect and you can see the changes on the System Summary page.
- *Revert* returns the settings to their last previous values.

NOTE: If you forget to click *Change* before moving to a new configuration page or closing your browser, your changes are lost.

The following table shows a summary of the Web configuration pages.

Major page	Configurable items
Network	Basic (IP, subnet mask, gateway and DNS); DHCP server; Cellular (cellular interface); NAT (Network address translation)
System	Web (Enable, SSL, Device password); Backup and Restore; Upgrade; Serial CL; Telnet CLI; SNMP; SYSLOG; ADP; CDP; Log, Advanced, Information
Security	RADIUS, Acess List, 802.11 Encryption (WEP and AES wireless encryption); 802.11 Authentication; Ethernet Supplicant
M2M	Serial Passthrough network and hardware settings
Link	802.11, PQ Mapping, User Classification, Protocol Filter, Statistics; Ethernet Protocol Filer and Statistics; Bridge 802.11 Static MACS and Ethernet Static MACS

Network

From the start page, click *Network*. The network pages allow you to configure IP features (layer 3 and 4), such as DHCP server and NAT. These features are global in nature. Their configuration affects all interfaces on the device and how the device communicates through the inside Ethernet (eth0) and the outside cellular routing (cell0) interfaces. These features should not be confused with layer 2 features found on the Link pages.

Basic

From the Network page, click *Basic*. The following table describes the basic network properties.

When you are finished, click *Change*.

Setting	Description
Device name	Specify a name to identify the device.
Device location	Specify the real-world location of the device.
DHCP client	Click *Obtain an IP address from a DHCP Server* to enable the DHCP client feature. Click *Specify IP information below* to specify a static IP address.
IP address	Specify static IP information for this device. If you change the IP address information and click *Change*, you cannot continue to configure the device using the old IP address. The browser will lose connection. To reestablish a connection, enter the new IP address into the browser:
Subnet mask	Specify the subnet mask for this device.
Gateway	Specify the IP address of the Gateway for this device. To specify that this device’s cellular link will be the Gateway, use the keyword cell0.
Primary DNS	Specify the IP address of a DNS server for this device. To indicate that you want to use the Primary DNS retrieve from the cellular link use the keyword cell0.
Secondary DNS	Specify the IP address of a secondary DNS server for this device. To indicate that you want to use the Secondary DNS retrieve from the cellular link use the keyword cell0.

Setting	Description
Current Gateway	This is the Gateway IP Address that is given out to DHCP clients. This is how you know the IP adress when the Gateway is set to cell0.
Current Primary DNS	This is the Primary DNS that is given out to DHCP clients. This is how you know the IP adress when the Primary DNS is set to cell0.
Current Secondary DNS	This is the Secondary DNS that is given out to DHCP clients. This is how you know the IP adress when the Secondary DNS is set to cell0.
DNS-proxy	Click the radio button to enable or disable DNS proxy for this device.

DHCP Server

From the Network page, click *DHCP Server*. This page allows you to set properties for the device DHCP server feature.

When you are finished, click *Change*.

Setting	Description
DHCP server	Click to enable or disable the device DHCP server feature. If enabled, the DHCP client feature (specified on the Network:Basic page) is disabled automatically.
Is running	Indicates DHCP server status.
IP Address	Specify static IP information for this device. If you change the IP address information and click *Change*, you cannot continue to configure the device using the old IP address. The browser will lose connection. To reestablish a connection, enter the new IP address into the browser:
Subnet Mask	Specify the subnet mask for this device.
Primary DNS server	Specify an IP address for the primary DNS server, or specify LOCAL.

Setting	Description
Secondary DNS server	Specify an IP address for the optional secondary DNS server, or specify LOCAL.
Domain name	Specify the domain name to be given out to DHCP clients.
IP range	Specify the pool of IP addresses to be given out to DHCP clients. The default IP range is from (low) 192.168.0.3 to (high) 192.168.0.254. The gateway’s default IP address is 192.168.0.1. The subnet mask is taken from eth0 interface setting.
Lease time	Specify the maximum length of time (in days, hours, and minutes) that a client has to renew its IP address before the IP address is placed back into the pool of available IP addresses. Normally clients renew their IP addresses when they reach half the lease time.

Cellular

From the Network page, click *Cellular*. This page allows you to configure settings for the cellular interface.

When you are finished, click *Change*.

Setting	Description
Cellular Type	This displays the type of cellular device being used by the Gateway. For the CGW103 product, this information reflects the type of PC-card inserted.
Mode	Select one of the following options from the list: **manual**: The *Start* button must be used to bring up the interface manually. **automatic**: The interface comes up automatically at boot time.
Current operator	Indicates the cellular service provider.

Setting	Description
Username	Specify the Username which is provided from the service provider. Not all service provider's require a username.
Password	Specify the Password which is provided from the service provider. Not all service provider's require a password.
APN	Specify the Access Point Network (from the service provider).
Signal strength	Indicates the strength of the cellular interface signal.
Status	Indicates the status of the cellular interface.
Start and *Stop* buttons	Click to start or stop connection to the cellular network.
Statistics button	Click to view how many packets have gone in and out and how many bytes have gone in and out since the Gateway was last restarted.

NAT

From the Network page, click *NAT*. This page allows you to configure settings to control Network Address Translation between the Ethernet interface(eth0) and the cellular interface (cell0). Network Address Translation remaps outbound traffic from internal interfaces to a single IP address and a random port. This gives the perception that outbound traffic originates from a single node, allowing you to provide Internet access to an entire IP subnetwork with one outbound link. All devices in the subnetwork appear to come from a single IP address established by the outbound link.

When you are finished, click *Change*.

Setting	Description
Status	Specify whether NAT should be enabled or disabled. If NAT is disabled, only one computer can use the cellular link.
Maximum connections	Specify the total number of connections allowed from inside computers through the cellular link. This is not the number of computers allowed to access the Internet; a computer generates several connections. Up to 1024 connections are allowed.
Translation timeout	Specify the length of time communication can be idle before a NAT connection is closed, allowing internal resources to be reclaimed. This timeout value should be increased if traffic is extremely intermittent.

System

From the start page, click *System*. These pages allow you to perform administrative tasks.

Web

From the System page, click *Web*. This page allows you to control the device web server. When you are finished, click *Change*.

Setting	Description
Enable	Click to specify whether the web server is enabled or disabled. If on, you can configure the device through a web browser. If off, you can only configure the device through Serial CLI, Telnet CLI, or SNMP.

Setting	Description
SSL	Click to specify whether Secure Socket Layer (SSL) technology is used to encrypt information between the computer and the device during a configuration session. When this option is turned on, data is protected during the configuration session. When it is turned off, data could be intercepted during the configuration session. When this option is on, you must specify https:// in the browser address pane to reach the configuration.

Backup & Restore

From the System page, click *Backup & Restore*. The gateway maintains the current configuration in FLASH memory. Once you have configured the gateway to your preferred functionality, it is useful to store a backup copy of the configuration so that you can restore it if necessary, or copy it to another gateway.

A backup operation stores the current configuration in a plain text file on a TFTP server. All information is transferred, including sensitive information such as the password of the device. Sensitive information is encrypted and stored as such in the file.

This page has the following buttons:

- *Backup*—Copies the entire configuration and stores it in the specified location.
- *Full Restore*—Replaces the entire configuration with the specified file.
- *Partial Restore*—Replaces the items identified in the configuration file as partial.This is useful for setting up a group of standard parameters for use across multiple devices. The device merges its current configuration with any new values transferred in the configuration file.

Setting	Description
TFTP Server’s IP address	Specify the IP address of a TFTP server where the configuration is to be stored. Make sure that you can reach the TFTP server and that the server accepts connections from any client.
File name	Specify the full path name of file being written or restored. The path must exist on the server. The file name extension is arbitrary, but it is recommended that you use the extension .arf

Upgrade

From the System page, click *Upgrade*. This page allows you to replace the current firmware either from a firmware image stored on a TFTP server or from an image stored on the local computer. To ensure uninterrupted operation, the gateway stores two firmware images. This command automatically replaces the oldest image. On the next reboot, the latest firmware image is automatically used.

To upgrade from a firmware image stored on a TFTP server:

1. In the *TFTP Server’s IP address* field, specify the IP address of a TFTP server where the firmware image is to stored. Make sure that you can reach the TFTP server and that the server accepts connections from any client. (For details on setting up a TFTP server, see the *Advanced Operations Guide*.)
2. In the upper *File name* field, specify the full path name of firmware image file.
3. Click *Upgrade*.

To upgrade from a firmware image stored on the local computer:

1. Click *Browse*. In the File Upload window, navigate to the firmware image file. Select the file and click *Open*.
2. Click *Upgrade*.

Serial CLI

From the System page, click *Serial CLI*. This page allows you to enable or disable the Serial CLI feature. The Serial CLI must be disabled if Serial Passthrough is in use.

When you are finished, click *Change*.

Setting	Description
Enable on Reboot	Click to specify whether the Serial CLI is enabled (on) or disabled (off) at startup.
Timeout	Specify the length of time to wait before disabling Serial CLI.
Currently Running?	Shows the current status of the Serial CLI
Start and *Stop* buttons	Click to enable of disable the serial cli.

Telnet CLI

From the System page, click *Telnet CLI*. This page allows you to enable or disable the Telnet CLI feature.

When you are finished, click *Change*.

Setting	Description
Enable	Click to specify whether the Telnet CLI is enabled (on) or disabled (off).
Timeout	Specify the length of time to wait before disabling Telnet CLI.
Who is connected	Identifies the IP address of the Telnet connection.
Close button	Click to terminate a Telnet CLI session immediately.

SNMP

From the System page, click *SNMP*. This page allows you to configure SNMP settings.

Simple Network Management Protocol (SNMP) is the standard for device management. This device supports SNMP versions V1, V2c, and V3. SNMP V2c adds additional error reporting over V1; V3 adds security via password-based authentication and encryption. The use of V3 is required for any write actions (and for most read actions) by default. While it may be disabled, the use of SNMP V3 is recommended. (For more information on SNMP, see the *Advanced Operations Guide*.)

When you are finished, click *Change*.

Setting	Description
Enable	Click to specify whether SNMPis enabled (on) or disabled (off).
Read community string	Specify the community string used for accessing the public read-only MIBs.
Write community string	Specify the community string used for accessing all of the MIBs with the ability to write to the writable MIBs.
Require V3	Choose ON to specify that SNMP V3 is required to access the write community MIBs (recommended).
Enable authentication traps	Click to specify whether or not SNMP Authentication traps are enabled (on) or disabled (off). Traps can be enabled on a primary and a secondary server. The following fields can be configured for each server: **Community**: Sets the community string used for authenticating trap events to the server. **IP Address**: Sets the IP address of the trap server to send trap events. **Port**: Sets the destination port used for sending traps (the UDP port on the trap server).

SYSLOG

From the System page, click *SYSLOG*. This page allows you to enable or disable the SYSLOG logging feature.

When you are finished, click *Change*.

Setting	Description
Enable	Specify whether logging is enabled (on) or disabled (off).
Primary IP address	Specify the IP address of the primary SYSLOG server.
Secondary IP address	Specify the IP address of the secondary SYSLOG server.
Severity threshold	Controls by severity which events are sent to the SYSLOG servers. Events less than or equal to this value are sent to the SYSLOG server. The highest priority is 0 and the lowest priority is 7. Only severity levels 0, 3, 6 and 7 occur on this gateway. Severity 6 events are strictly informative. They occur during bootup and shutdown and describe the gateway’s functional behavior. Errors (severity 3) indicate failures that are not catastrophic but do affect gateway functionality. For details on the severity levels, see the Advanced Operations Guide.

ADP

From the System page, click *ADP*. This page enables or disables Alliant Discovery Tool and sets the port used by the tool.

When you are finished, click *Change*.

Setting	Description
Enable	Specify whether the Discovery Tool is enabled (on) or disabled (off).
Port	Identifies the port used by the Discovery Tool. This value must match the port setting on the Tool.

CDP

From the System page, click *CDP*. This page enables or disables Cisco Discovery Protocol. When you are finished, click *Change*.

Setting	Description
Enable	Specify whether the protocol is enabled (on) or disabled (off).
Period	Identifies the rate at which CDP packets are sent.
Hold	Identifies the length of time, in seconds, that remote CDP-aware products store information in the device.

Log

From the System page, click *Log*. This page displays a log of information about device activity.

Setting	Description
Logging Threshold	Select the level of events to be logged.

Setting	Description
Uptime	This is how long they Gateway has been running since it was last turned on or reset.

Advanced

From the System page, click *Advanced*. This page allows you to reset the device or restore the configuration to factory defaults.

Button	Description
Reset	If the gateway stops responding correctly, click to perform a reset, which disrupts the network temporarily, but does not affect gateway configuration settings that have already been applied with *Change*. (Changes stored only in cache memory are lost in a reset.)
Restore	Click to restore the configuration to the factory defaults (which are stored on the gateway) and reset the gateway. This command deletes any user defined configuration information from the gateway. See Restoring factory defaults on page 71

Information

From the system page, click *Information* to view your Gateway's model number, serial number, manufacturing date, manufacturing ID, vendor name, product name, hardware version, software version, MAC address, cellular type, cellular ID, and firmware information.

Security

From the start page, click *Security*. The Security page appears, where you can configure security settings. All but the supplicant settings affect only 802.11 wireless clients. To maintain wireless association, the settings on wireless clients and the device must match exactly.

This product provides numerous encryption and authentication solutions. The acceptable combination of authentication and encryption options are captured in the table below. Client support is also required. Notably XP users should note the EAP-PEAP authentication with Pairwise WEP encryption, refer to Configuring XP Advanced Wireless Security on page 76

			Encryption		
Authentication	**None**	**Shared WEP**	**Pairwise WEP**	**Pairwise TKIP**	**WPA Pairwise TKIP**
Open	Yes	Yes			Yes
Shared WEP		Yes			
EAP-RADIUS	Yes	Yes	Yes		
EAP-TTLS-PAP			Yes		
EAP-TTLS-MS-CHAPv2			Yes		
EAP-PEAP			Yes		
WPA-RADIUS				Yes	
WPA-TTLS-PAP				Yes	

	Encryption				
Authentication	**None**	**Shared WEP**	**Pairwise WEP**	**Pairwise TKIP**	**WPA Pairwise TKIP**
WPA-TTLS-MS-CHAPv2				Yes	
WPA-PEAP				Yes	

802.11 Encryption

From the Security page, click *Encryption*. The Encryption page appears, where you can configure the settings for wireless encryption. You can change the settings by clicking the radio buttons and entering values in the fields. When you are finished, click *Change*.

The following table describes the encryption modes.

Setting	Description
Encryption mode	**Open**: No encryption. This mode is the default. **Shared-WEP**: Supported only to maintain compatibility with legacy equipment. Not recommended, due to security problems with the algorithm. **Pairwise-WEP**: Sometimes known as dynamic key encryption. Uses the WEP algorithm, but dynamically generates encryption keys during the authentication process. Can only be used with IEEE 802.1X authentication modes (eap-radius, eap-ttls). **Pairwise-TKIP**: A dynamic key encryption mode which uses larger encryption keys and a more secure key negotiation protocol. Only usable for RSN or WPA authentication modes (rsn-radius, rsn-ttls, wpa-radius, wpa-ttls).

Setting	Description
	Pairwise-AES-Comp: Another dynamic key encryption mode which uses the AES algorithm for encryption, and a more secure key negotiation protocol. Only usable for RSN or WPA authentication modes (rsn-radius, rsn-ttls, wpa-radius, wpa-ttls).
WEP shared index	Select the WEP key to use for Shared-WEP.
Encryption length	Select the encryption length to use for Shared-WEP.
Key 1, Key 2, Key 3, Key 4	Specify the keys to use for Shared-WEP. Each key must be either a string of 5 to 13 characters with no spaces, or a hexadecimal value of 10 or 26 hex digits, starting with “0x”. All four keys must match for any received data.

802.11 Authentication

From the Security page, click *Authentication*. The Authentication page appears, where you can configure authentication for the 802.11 wireless interface. You can change the authentication by selecting one of the drop-down settings.

When you are finished, click *Change*.

Setting	Description
Authentication mode	**Open**: No authentication is performed. **Shared Wep**: A legacy mode only applicable to using shared WEP encryption. **EAP-RADIUS**: Authentication is performed as an IEEE 802.1X Authenticator, using a centralized RADIUS Server as a backend authentication server. This mode may or may not require encryption settings. Note that the Pairwise-TKIP encryption mode is not an option with this authentication mode.

Setting	Description
	EAP-TTLS-PAP: Authentication is performed as an IEEE 802.1X Authenticator, using an on-device EAP-TTLS backend authentication server. This mode generates pairwise encryption keys, and it is highly recommended that wireless interfaces enable the pairwise-wep encryption mode when using this authentication mode. In that case, make sure the supplicants have their Encryption mode set to "WEP" and the box "Key will be generated automatically" is checked. There are multiple possible settings for TTLS. Supplicant credentials are verified using the PAP authentication method **Note** that the Pairwise-TKIP encryption mode is not an option with this . **EAP-TTLS-MS-CHAPv2**: Authentication is performed as an IEEE 802.1X Authenticator, using an on-device EAP-TTLS backend authentication server. This mode generates pairwise encryption keys, and it is highly recommended that wireless interfaces enable the Pairwise-WEP encryption mode when using this authentication mode. In that case, make sure the supplicants have their Encryption mode set to "WEP" and the box "Key will be generated automatically" is checked. There are multiple possible settings for TTLS. Credential verifiaction uses the MS-CHAPv2 authentication verification. **EAP-PEAP**: Authentication is performed as an IEEE 802.1X Authenticator, using an on-device EAP-PEAP backend authentication server. This mode generates pairwise encryption keys, and it is highly recommended that wireless interfaces nable the pairwise-wep encryption mode when using this authentication mode. In that case, make sure the supplicants have their Encryption mode set to "WEP" and the box "Key will be generated automatically" is checked. **WPA-RADIUS**: Authentication is performed as a WPA Authenticator, using a centralized RADIUS Server as a backend authentication server. This authentication mode requires the use of the Pairwise-TKIP encryption mode. **WPA-TTLS**: Authentication is performed as a WPA Authenticator, using an on-device EAP-TTLS backend authentication server. This authentication mode requires the use of the pairwise-tkip encryption mode.

Setting	Description
	WPA-PEAP: Authentication is performed as an IEEE 802.1X Authenticator, using an on-device EAP-PEAP backend authentication server. This mode generates pairwise encryption keys, and it is highly recommended that wireless interfaces nable the Pairwise-TKIP encryption mode when using this authentication mode. In that case, make sure the supplicants are configured for WPA association and TKIP encryption.

Certificate

This command lets you load a new certificate. Click on browse to find the file, or type in its name, then click on “Update” to update your certificate.

RADIUS

From the Security page, click *RADIUS*. The RADIUS page appears, where you can configure the settings for RADIUS authentication and accounting. You can change the settings for primary and optional secondary servers by clicking the radio buttons and entering values in the fields.

When you are finished, click *Change*.

Authentication

The RADIUS authentication grouping provides settings for a RADIUS authentication server.

Setting	Description
Primary Column	Specify the primary RADIUS authentication server IP address, port and shared secret.

Setting	Description
Secondary Column	Specify the optional secondary RADIUS authentication server. If the primary cannot be contacted, the gateway will attempt to communicate with the secondary.

Accounting

The RADIUS accounting grouping provides settings for a RADIUS accounting server. NOTE: Accounting is only applicable if the authentication mode is not “Open”.

Setting	Description
Accounting enable	Click to enable (on) or disable (off) RADIUS accounting.
Update interval	Specify how often (in seconds) that RADIUS Accounting will send interim-update messages to the RADIUS Accounting Server.
Primary	Specify the primary RADIUS accounting server IP address, port and shared secret.
Secondary	Specify the optional secondary RADIUS accounting server. If the primary cannot be contacted, the gateway will attempt to communicate with the secondary.

Access List

Is a database of user names and passwords stored on the device. Primarily this list is used for local TTLS. Local TTLS provides the same level of security as a RADIUS server without the need to set up another computer, the RADIUS server.

From this page, users can be added, removed or you can change their password. The device always has the admin user, which can never be removed.

Add a user

1. Type in a name in the User Name field.
2. Type in the password in the Password field
3. Type in the password again in the Confirm Password field.
4. Click Add/Change

The new name should appear in the table.

Change password

1. Select a row in the table. The user name will appear in the user name field.
2. Type in the password in the password field
3. Type in the password again in the Confirm password field.
4. Click Add/Change

The table will not change but the password will be updated in the device.

Remove a user

1. Select a row in the table. The user name will appear in the user name field.
2. Click Remove

The user name will be removed from the table.

Ethernet Supplicant

From the Security page, click *Supplicant*. The Supplicant page appears, where you can configure authentication for the 802.3 Ethernet interface. You can change the authentication by selecting one of the drop-down settings. For settings other than Open, enter a user name and password.

When you are finished, click *Change*.

Setting	Description
Supplicant mode	**Open**: No authentication is performed. **Supplicant-MD5**: Authentication is performed as an IEEE 802.1X Supplicant, using EAP-MD5 as the authenticating protocol.
User name	Specify the user name to use for authentication (a string from 1 to 32 characters containing no spaces).
Password	Specify the password to use for authentication (a string from 1 to 32 characters containing no spaces).

M2M

From the start page, click *M2M*. The M2M page appears, where you can configure network and hardware settings for the Serial Passthrough feature.

Network settings

From the M2M page, click *Network settings*. The Serial Passthrough page appears, where you can configure network settings for the serial passthrough feature.

When you are finished, click *Change*.

Setting	Description
Enable on reboot	Click on to specify that the passthrough application should restart itself when a disconnection occurs. Otherwise, click off. This overrides the Serial CLI’s enable on reboot.
Socket type	Sets the socket type to use for the passthrough application: **TCP listen**: A socket that accepts connections from remote systems. **TCP connect**: A TCP socket that initiates a connection with a remote system. **UDP**: A UDP socket type.
Local port	Specify the local port number for use with UDP and TCP-Listen modes.
Remote IP address	Specify the IP address of the remote system that will be communicating with the serial interface.
Remote port	Specify the port number of the remote system that will be communicating with the serial interface.
Network Timeout	Specify the length of time to wait (in milliseconds) for data from the network before automatically disconnecting.
Serial Timeout	Specify the length of time to wait (in milliseconds) for data from the serial device before sending it to the socket.
Line length	Specify the length of the serial input buffer, defining how many characters will be read from the serial port before sending the data to the socket.
Start and *Stop* buttons	Start or stop the Serial Passthrough feature.

Hardware settings

From the M2M page, click *Hardware settings*. The Serial Passthrough:Hardware Settings page appears, where you can configure hardware settings for the serial port.

When you are finished, click *Change*.

Setting	Description
Baudrate	Select a baud rate from the list.
Data bits	Select the number of data bits from the list.
Parity	Select a parity from the list.
Stop bits	Select the number of stop bits from the list.
Flow control	Select the type of flow control from the list.

Link

From the start page, click *Link*. The Link pages allow you to configure layer 2 features.

802.11

From the Link page, click *802.11*. This page allows you to set the 802.11 radio device name, location, and service area for the inside wireless network (not to be confused with the cellular gateway).

When you are finished, click *Change*.

Setting	Description
Service area	The ESSID is the identifying name of an 802.11b wireless network. By specifying the ESSID in your client setup is how you make sure that you connect to your wireless network instead of your neighbors network by mistake.
Supported clients	Controls which clients are allowed to connect. By default, both b and g clients are allowed to connect.
Channel	Controls the frequency this product uses. Clients must be setup to use the same frequency. Changing this value can avoid interference from other wireless devices.
Basic rates	This option controls the support data rates. Unchecking any boxes prevents clients from using that specific data rate.
Data preamble	A shorter preamble improves network effeincey since less control data is sent. However older clients or slower data rates may not operate with a short-preamble.
Beacon period	The time between this device sending a beacon. Clients listen for beacons to find networks.
Receive radio antenna diversity	Antenna diversity enabled can improve network performance.
Transmit power	A rough control on how much power is used to send traffic
Transmit ESSID in beacon	When disabled the ESSID is not sent in beacons.

802.11 PQ Mapping

From the Link page, click *PQ Mapping*. The VLAN mapping table is displayed.

The gateway supports the QoS model described in the 802.11 Task Group E. This group is responsible for defining QoS for wireless traffic. 802.11 traffic can be given a priority from 0 to 7. By default, VLAN priorities map to the matching 802.11 priority number. For example, VLAN priority 1 maps to 802.11 priority 1. You can change this mapping by clicking Enable and changing the values in the 802.11 Priority column. When you are finished, click *Change*.

802.11 User classification

From the Link page, click *User Classification*.

User classification provides a means of classifying or dropping frames. Classification provides privileges to higher priority frames, which are sent before lower priority frames.

User Classification is only available for the 802.11 interface (eth1).

The user classification page provides a way for users to construct a tree of rules, known as a decision tree. The goal is for each frame to migrate through the decision tree. Eventually, a frame gets to a rule indicating a classification, dropped, or no action. The decision tree is presented as a table where each row has an index value. The first row is 0, and so on.

Each rule identifies a field in the frame, an operator, one or more values, a true rule index, and a false rule index. The operator identifies how to compare the field in the frame against the value(s).

The fields that are applicable to the rules are:

- SRC/DST MAC Address
- Ethernet II Ether Type
- IP Protocol
- TCP and UDP source ports
- TCP and UDP destination ports
- 802.1 P/Q priority

PQ mapping is applied to frames before User Classification rules are applied. The Priority field refers to the frame’s current priority. If the frame has already been classified, the frame’s priority will be between 0 and 7, otherwise it will be -1 for a nonclassified frame. Nonclassified frames are treated as the lowest priority frame.

These simple rules govern the classification rules in the order presented:

1. Rule 0 is applied first to the frame.
2. If the field does not exist in the frame, then the result is always FALSE. This is determined by parsing through the frame. For example, an Ether II frame does not contain an IP port and would fail if the rule required one.
3. If the field exists, then the operator is applied along with the provided values. If the result is true, then the rule identified by the true index is used next. If the result is false, then the rule identified by the false index is used next.
4. If a row does not exist, then this is equivalent to do nothing (see below).

Eventually a leaf node is reached. In which case, one of three actions can occur:

- The frame can be classified. A priority is assigned to the frame and it is then sent to the next DISC.
- The frame is dropped.
- Do nothing.

Even though the rules are conceptually a tree, they are organized in a table with six columns. The table below shows how users can classify UDP frames not already classified that are destined to ports between 1 and 90 to a priority of 3.

Index	Frame Field	Operator	Value1	Value2	True	False
1	Priority	==	unassigned		2	5
2	IP	==	UDP		3	5
3	Dst Port	Between	1	90	4	5

4	Classify		3			
5	nothing					

Setting	Description
User classification	Click to enable or disable classification.
Index	The row in the table to add a frame rule.
Frame field	Select one of the following: **SRC MAC**: Use the source MAC address of the frame to compare against the mac_address value(s). **DST MAC**: Use the destination MAC address of the frame to compare against the mac_address value(s). **Ether Type**: Use the Ethernet type from the frame to compare against the integer value(s). **IP Protocol**: The IP protocol field of the frame. **SRC Port**: Use the UDP or TCP source port of the frame to compare against the integer value(s). **Dst Port**: Use the UDP or TCP destination port of the frame to compare against the integer value(s). **Priority**: Compare the frame’s current priority against the integer value(s).
Operator	Select one of the following: **!=**: Not equal. **==**: Equal. **<**: Less than.

Setting	Description
	>: Greater than. **<=**: Less than or equal. **>=**: Greater than or equal. **between**: Between two values. This operator requires two values. Values depend on the field selected in the rule. **do nothing**: Add a rule to the table to do nothing. **drop**: Set a rule to drop a frame. **classify**: Add a rule to classify a frame.
Value 1	An integer or MAC address in the form of AA:BB:CC:DD:EE:FF to compare against the ether_type, src_port, dst_port or priority fields.
Value 2	An integer or MAC address in the form of AA:BB:CC:DD:EE:FF to compare against the ether_type, src_port, dst_port or priority fields. Required only with the **between** operator.
True index	The next row to compare against if the field, operator and values are true.
False index	The next row to compare against if the field, operator and values are false.
Add button	Click to add a new rule.
Remove buttons	Enter an index number from the table and click to remove that rule.

802.11 Protocol Filter

From the Link page, click *Protocol Filter*. The Protocol Filter page allows you to filter out Ethernet packet frames that match the selected Ethernet protocol types.

1. Click Enable to enable filtering for reception (IN) or transmission (OUT).

2. Select the filtering action from the **Mode** list:
   allow - allow packets of this type to pass through
   drop - drop packets of this type
3. Check the boxes of the protocols that you want to filter.
4. When you are finished, click *Change*.

802.11 Statistics

From the Link page, click *Statistics*. A table of statistics and values for the 802.11 interface is displayed.

Ethernet Protocol Filter

From the Link page, click *Protocol Filter*. The Protocol Filter page allows you to filter out Ethernet packet frames that match the selected Ethernet protocol types.

1. Click Enable to enable filtering for reception (IN) or transmission (OUT).
2. Select the filtering action from the **Mode** list:
   allow - allow packets of this type to pass through
   drop - drop packets of this type
3. Check the boxes of the protocols that you want to filter.
4. When you are finished, click *Change*.

Ethernet Statistics

From the Link page, click *Statistics*. A table of statistics and values for the 802.3 interface is displayed.

Bridge

From the Link page, click *Bridge*. The forwarding table is displayed.

802.11 Static MACs

MAC addresses in this list are never removed from the forwarding table. They are placed in the forwarding table during boot up, initializing the forwarding table.

Setting	Description
MAC address	To add a MAC address, enter the MAC address in this field and hit add. To remove a MAC address, select one from the table and hit remove.

Ethernet Static MACs

MAC addresses in this list are never removed from the forwarding table. They are placed in the forwarding table during boot up, initializing the forwarding table.

Setting	Description
MAC address	To add a MAC address, enter the MAC address in this field and hit add. To remove a MAC address, select one from the table and hit remove.

Restoring factory defaults

You can restore gateway settings to the defaults that were set at the factory either manually or through software.

To restore the settings manually, insert a pointed object (such as the end of a straightened paper clip) into the reset hole to press the Configuration button. Press and hold the button for 10 seconds.

Through the web pages:

1. In the start page, click *System*.
2. In the System page menu, click *Advanced*.
3. Click *Restore*.

If the gateway was using an IP address setting other than the default, restoring the factory defaults will change the IP address back to 192.168.0.1 and a subnet mask of 255.255.255.0. Discovery tool can help find the device and assist in configuration, do the following:

1. Close your browser.
2. Return to the Alliant Discovery Tool and click *Discover* device.
3. Select the device and right-click to start a new configuration session.

Upgrading the System

You can download firmware and configuration management system upgrades from the Alliant Web site and install those upgrades on the gateway.

To locate an upgrade file and download it to your computer:

1. Log on to the Alliant Web site at http://www.alliantnetworks.com.
2. Locate the download file and download the file into a directory on your computer (or move the file to the TFTP server upload/download directory).

To install an upgrade from a TFTP server:

1. From the System page, click *Upgrade*.

2. In the *TFTP server's IP address* field, specify the IP address of a TFTP server where the firmware image is to stored. Make sure that you can reach the TFTP server and that the server accepts connections from any client. (For details on setting up a TFTP server, see the *Advanced Operations Guide*.
3. In the upper *File name* field, specify the full path name of firmware image file.
4. Click *Upgrade*.

To upgrade from a firmware image stored on the local computer:

1. From the System page, click *Upgrade*.
2. Click *Browse*. In the File Upload window, navigate to the firmware image file. Select the file and click *Open*.
3. Click *Upgrade*.

Backing up a Configuration

As part of system maintenance, you should save and back up the configurations of individual gateways in case you need to reload them in the future. The backup saves all the parameters of the selected gateway in a file on your computer. The file can be used later to restore the full configuration on this gateway or a partial configuration on another gateway.

The configuration is stored in a structured, plain text file, called a *configuration file*. Sensitive information is encrypted in the file.

1. On the System page, click *Backup & Restore* gateway.
2. Specify an IP address of the TFTP server and a name of the backup file, and click *Backup*.

Restoring a Configuration

Restoring a configuration facilitates two useful purposes:

- The first is to return a gateway to a known state. The restore process fully replaces the gateway's configuration to a known state from a previously created backup file.
- Alternatively, the gateway supports a partial restore, where only part of the configuration file is used to replace the settings. It is useful to create a single file with standard settings that can be used to configure all the gateways in your environment. Moreover, the configuration file can be altered and used as an alternative means of configuring a gateway through a partial restore.

If you have stored a backup configuration on your computer, you can restore the configuration as follows:

1. From the System page, click *Backup & Restore*.
2. In the spaces provided, specify the IP address of the TFTP server where the configuration is stored, and the full path name of the file. Make sure that you can reach the TFTP server and that the server accepts connections from any client.
3. Click one of the following buttons:

   Full Restore—Replaces the entire configuration with the specified file.

   Partial Restore—Replaces the items identified in the configuration file as partial.This is useful for setting up a group of standard parameters for use across multiple devices. The device merges its current configuration with any new values transferred in the configuration file.

   The configuration is restored and activated on the gateway. This operation may cause the gateway to reboot.

When restoring the gateway's configuration from a file, the IP address may be changed. If you want to continue configuring the gateway, do the following:

1. Close your browser.
2. Return to the Alliant Discovery Tool and click *Discover device*.
3. Select the device and right-click to start a new configuration session.

Solving Problems

If you have difficulty using the gateway, refer to the following topics for information on how to diagnose and solve problems.

Configuring XP Advanced Wireless Security

Microsoft XP can manage your wireless PC Cards and provide advance wireless security. Configuration requires two major stages. First, configure the Cellular Gateway, afterwhich you'll loose wireless access till the XP client is configured. Don't worry. You can always access the Cellular Gateway through the Ethernet interface. Second, configure your wireless card.

You'll need to add your login user name and password to the CellularGateway, which requires that the password is at least eight characters. If your password is less than eight characters, change it on your computer before proceeding.

On the Gateway,

1. Assuming you have not changed the Cellular Gateway's default IP address, browse to http://192.168.0.1
2. Select Security
3. Select Access List
4. Enter your user name and password. Make sure to click Add/Change
5. Select Authentication.
6. Configure authentication to be EAP-PEAP. Make sure to click Change.
7. Select Encryption
8. Configure encryption to be Pairwise WEP.Make sure to click Change.

On an XP client:

1. Edit properties for the 802.11 interface
2. Select "Wireless Networks" at the top of the window
3. Make sure that “Use Windows to configure my wireless network settings” at the top of the page is checked.
4. Make sure the AP you want to use is in the "Preferred Networks" list-if its not, add it.
5. Select the wireless network you will be using for this test, then click the properties button below the list.
6. Check the box for "Data encryption(WEP enabled)"
7. Check the box for "The key is provided for me automatically"
8. Select the "Authentication" tab at the top of the window
9. Check the box for "Enable IEEE 802.1x authentication for this network"
10. Uncheck “Authenticate as computers when computer inforation is available.”
11. Set the EAP type to "Protected EAP(PEAP)
12. Click the Properties button
13. Uncheck the box for "Validate server certificate"
14. Select Authentication Method as "Secured password (EAP-MSCHAP v2)
15. Uncheck the box for "Enable Fast Reconnect"
16. Click the Configure button to the right of the pulldown for Authentication Method.
17. Check the box for "Automatically use my Windows logon name and password"
18. Keep clicking "OK" until all windows are closed
19. Verify network connectivity by pinging the bridge and other devices on the network.

Configuring your Ethernet Network

Unable to access the Internet

First check to see if the device is connected. From the Web pages, select Network then Cellular. The Status link should say connected. If not then try the following:

- Make sure the PC Card is inserted.
- If the status is Stopped, click Start once then use the refresh button to see the current status.
- If the Mode is manual, then either click Start or change the mode to Automatic.
- If you have just turned on the unit, connecting to the cellular network might take several minutes. Select refresh periodically to check the current status of the connection. If after 10 minutes you still are not connected try the next bulleted item.
- Make sure the PC card was inserted before plugging in the device. If you are not sure, unplug the device, insert the PC card, then plug in the device.

Restore to factory defaults

Restoring the configuration of the device to manufacturing defaults guarantees an operational configuration. This operation can be completed through a management interface or manually, through the configuration hole on the side of the device.

To restore to factory defaults through the WEB interface:

1. Select the **System** link.
2. Select the **Advanced** link.
3. Press the **Restore** button.

To restore to factory defaults manually:

1. Power on the device.
2. As soon as the middle LED comes on, insert a paper clip into the configuration hole and hold the button until three LEDs are lit.
3. Release the paper clip. The device can take up to 30 seconds to resume operation.

Getting FTP to work

FTP clients must enable passive mode when accessing an FTP server through our product. Most clients use passive mode by default with the exception of the client that ships with all Microsoft Windows platforms.

Index