USRobotics® Wireless MAXg Access Point: User Guide

The USRobotics Wireless ***MAX*g** Access Point is the one solution to your home and small business wireless connectivity needs. MAXg technology provides the maximum 802.11g range in the industry, delivering optimal wireless connections to your PCs, laptops, and other wireless devices. MAXg also provides the maximum speed – up to 125 Mbps – delivering large files like MP3s, digital photos, and digital video through your network fast and efficiently. And with MAXg, your network will be protected with a maximum security suite of capabilities, including Stateful Packet Inspection firewall for protection from network intrusions, Wi-Fi Protected Access (WPA and WPA2), WPA2/802.11i, TKIP and AES Encryption, MAC address authentication, and more.

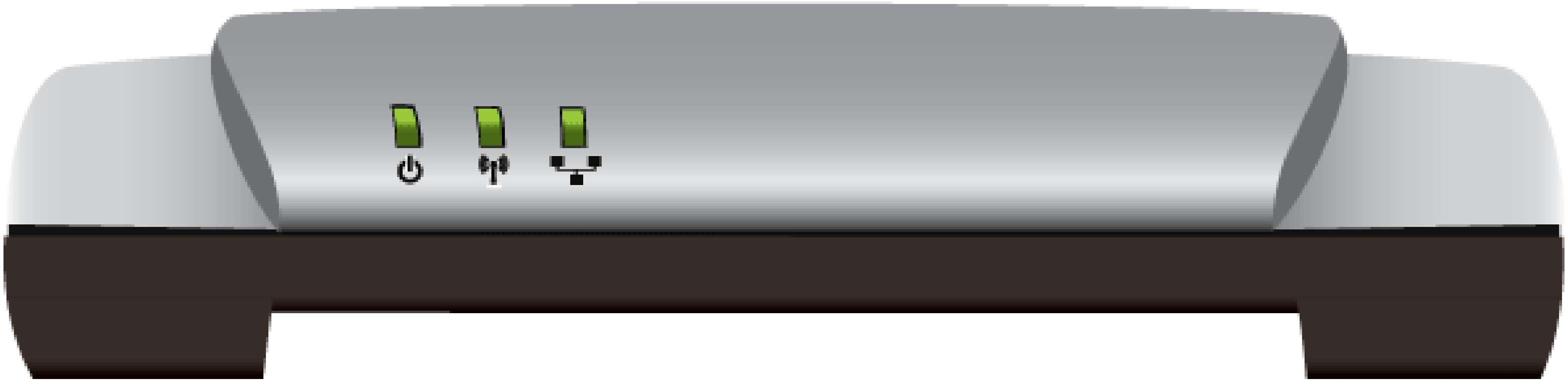
System Requirements

- A computer with an Ethernet adapter installed

- A router with Dynamic Host Configuration Protocol (DHCP) enabled
- A Ethernet-based cable or DSL modem or other WAN connection for Internet access
- An HTML 4.01-compliant Web Browser with JavaScript enabled

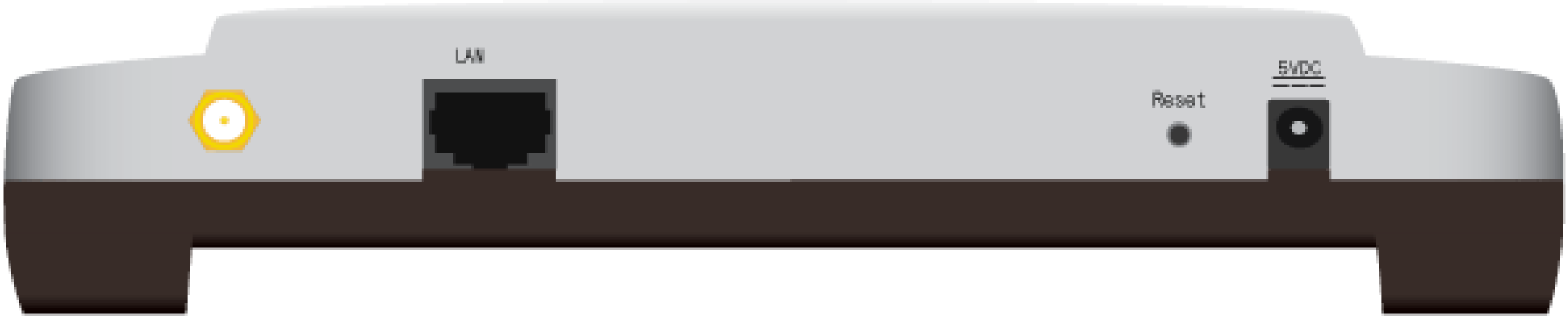
Product Views

Front



Symbol	Name	State	Condition
⏻	Power	Off	Not receiving power.
		Solid	Receiving power.
📶	WLAN (Wireless Network)	Off	Wireless connection is disabled.
		Solid	Wireless connection is enabled.
		Flashing	Sending and receiving data.
🖧	LAN	Off	No LAN connection.
		Solid	LAN link is achieved.
		Flashing	Sending and receiving data.

Back



Item	Function
⊙	Connects an antenna to the access point.
LAN	Connects the access point to a networking device.
Reset	Reboots your access point or restores your access point to its factory default settings. • To reboot your access point without changing your current settings, press and hold the Reset button for 1 second. • To restore your access point to the factory default settings, press and hold the Reset button for 7 seconds.
5VDC	Connects the power adapter to your access point.

R46.1703.00
rev 0 04/07

USRobotics® *Wireless MAXg Access Point: User Guide*

Product Specifications

- AP Management through standard Web browsers
- Roaming capability
- Dynamic IP Address assignment via DHCP or Static IP address assignment through the Web User Interface
- AP firmware upgrades available through the Web User Interface
- One RJ-45, 10/100 Mbps auto-sensing and auto-switching Ethernet LAN port
- Complies with IEEE 802.11g 54 Mbps wireless radio standard
- Security Features:
    - WPA and WPA2 (Wi-Fi Protected Access) in Access Point mode
    - 64/128-bit WEP (Wired Equivalent Privacy) data encryption with Open/ Shared Key
    - Full Support for 802.11g Open and Shared key Authentication
    - Ability to disable SSID Broadcast
    - MAC address filtering

Acknowledgements

This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

USRobotics® *Wireless MAXg Access Point:*

User Guide

U.S. Robotics Corporation Two (2) Year Limited Warranty

1.0 GENERAL TERMS:

1.1 This Limited Warranty is extended only to the original end-user purchaser (CUSTOMER) and is not transferable.

1.2 No agent, reseller, or business partner of U.S. Robotics Corporation (U.S. ROBOTICS) is authorised to modify the terms of this Limited Warranty on behalf of U.S. ROBOTICS.

1.3 This Limited Warranty expressly excludes any product that has not been purchased as new from U.S. ROBOTICS or its authorised reseller.

1.4 This Limited Warranty is only applicable in the country or territory where the product is intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

1.5 U.S. ROBOTICS warrants to the CUSTOMER that this product will be free from defects in workmanship and materials, under normal use and service, for TWO (2) YEARS from the date of purchase from U.S. ROBOTICS or its authorised reseller.

1.6 U.S. ROBOTICS sole obligation under this warranty shall be, at U.S. ROBOTICS sole discretion, to repair the defective product or part with new or reconditioned parts; or to exchange the defective product or part with a new or reconditioned product or part that is the same or similar; or if neither of the two foregoing options is reasonably available, U. S. ROBOTICS may, at its sole discretion, provide a refund to the CUSTOMER not to exceed the latest published U.S. ROBOTICS recommended retail purchase price of the product, less any applicable service fees. All products or parts that are exchanged for replacement will become the property of U.S. ROBOTICS.

1.7 U.S. ROBOTICS warrants any replacement product or part for NINETY (90) DAYS from the date the product or part is shipped to Customer.

1.8 U.S. ROBOTICS makes no warranty or representation that this product will meet CUSTOMER requirements or work in combination with any hardware or software products provided by third parties.

1.9 U.S. ROBOTICS makes no warranty or representation that the operation of the software products provided with this product will be uninterrupted or error free, or that all defects in software products will be corrected.

1.10 U.S. ROBOTICS shall not be responsible for any software or other CUSTOMER data or information contained in or stored on this product.

2.0 CUSTOMER OBLIGATIONS:

2.1 CUSTOMER assumes full responsibility that this product meets CUSTOMER specifications and requirements.

2.2 CUSTOMER is specifically advised to make a backup copy of all software provided with this product.

2.3 CUSTOMER assumes full responsibility to properly install and configure this product and to ensure proper installation, configuration, operation and compatibility with the operating environment in which this product is to function.

2.4 CUSTOMER must furnish U.S. ROBOTICS a dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) for any warranty claims to be authorised.

3.0 OBTAINING WARRANTY SERVICE:

3.1 CUSTOMER must contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre within the applicable warranty period to obtain warranty service authorisation.

3.2 Customer must provide Product Model Number, Product Serial Number and dated

Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) to obtain warranty service authorisation.

3.3 For information on how to contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre, please see the U.S ROBOTICS corporate Web site at: www.usr.com

3.4 CUSTOMER should have the following information / items readily available when contacting U.S. ROBOTICS Technical Support:

- Product Model Number
- Product Serial Number
- Dated Proof of Purchase
- CUSTOMER contact name & telephone number
- CUSTOMER Computer Operating System version
- U.S. ROBOTICS Installation CD-ROM
- U.S. ROBOTICS Installation Guide

4.0 WARRANTY REPLACEMENT:

4.1 In the event U.S. ROBOTICS Technical Support or its authorised U.S. ROBOTICS Service Centre determines the product or part has a malfunction or failure attributable directly to faulty workmanship and/or materials; and the product is within the TWO (2) YEAR warranty term; and the CUSTOMER will include a copy of the dated Proof of Purchase (original purchase receipt from U.S. ROBOTICS or its authorised reseller) with the product or part with the returned product or part, then U.S. ROBOTICS will issue CUSTOMER a Return Material Authorisation (RMA) and instructions for the return of the product to the authorised U.S. ROBOTICS Drop Zone.

4.2 Any product or part returned to U.S. ROBOTICS without an RMA issued by U.S. ROBOTICS or its authorised U.S. ROBOTICS Service Centre will be returned.

4.3 CUSTOMER agrees to pay shipping charges to return the product or part to the authorised U.S. ROBOTICS Return Centre; to insure the product or assume the risk of loss or damage which may occur in transit; and to use a shipping container equivalent to the original packaging.

4.4 Responsibility for loss or damage does not transfer to U.S. ROBOTICS until the returned product or part is received as an authorised return at an authorised U.S. ROBOTICS Return Centre.

4.5 Authorised CUSTOMER returns will be unpacked, visually inspected, and matched to the Product Model Number and Product Serial Number for which the RMA was authorised. The enclosed Proof of Purchase will be inspected for date of purchase and place of purchase. U.S. ROBOTICS may deny warranty service if visual inspection of the returned product or part does not match the CUSTOMER supplied information for which the RMA was issued.

4.6 Once a CUSTOMER return has been unpacked, visually inspected, and tested U.S. ROBOTICS will, at its sole discretion, repair or replace, using new or reconditioned product or parts, to whatever extent it deems necessary to restore the product or part to operating condition.

4.7 U.S. ROBOTICS will make reasonable effort to ship repaired or replaced product or part to CUSTOMER, at U.S. ROBOTICS expense, not later than TWENTY ONE (21) DAYS after U.S. ROBOTICS receives the authorised CUSTOMER return at an authorised U.S. ROBOTICS Return Centre.

4.8 U.S. ROBOTICS shall not be liable for any damages caused by delay in delivering or furnishing repaired or replaced product or part.

5.0 LIMITATIONS:

5.1 THIRD-PARTY SOFTWARE: This U.S. ROBOTICS product may include or be bundled with third-party software, the use of which is governed by separate end-user license agreements provided by third-party software vendors. This U.S. ROBOTICS Limited Warranty does not apply to such third-party software. For the applicable warranty refer to the end-user license agreement governing the use of such software.

5.2 DAMAGE DUE TO MISUSE, NEGLECT, NON-COMPLIANCE, IMPROPER INSTALLATION, AND/OR ENVIRONMENTAL FACTORS: To the extent permitted by applicable law, this U.S. ROBOTICS Limited Warranty does not apply to normal wear and tear; damage or loss of data due to interoperability with current and/or future versions of operating system or other current and/or future software and hardware; alterations (by persons other than U. S. ROBOTICS or authorised U.S. ROBOTICS Service Centres); damage caused by operator error or non-compliance with instructions as set out in the user documentation or other accompanying documentation; damage caused by acts of nature such as lightning, storms, floods, fires, and earthquakes, etc. Products evidencing the product serial number has been tampered with or removed; misuse, neglect, and improper handling; damage caused by undue physical, temperature, or electrical stress; counterfeit products; damage or loss of data caused by a computer virus, worm, Trojan horse, or memory content corruption; failures of the product which result from accident, abuse, misuse (including but not limited to improper installation, connection to incorrect voltages, and power points); failures caused by products not supplied by U.S. ROBOTICS; damage cause by moisture, corrosive environments, high voltage surges, shipping, abnormal working conditions; or the use of the product outside the borders of the country or territory intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

5.3 TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. U.S. ROBOTICS NEITHER ASSUMES NOR AUTHORISES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, WARRANTY, OR USE OF ITS PRODUCTS.

5.4 LIMITATION OF LIABILITY. TO THE FULL EXTENT ALLOWED BY LAW, U.S. ROBOTICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF U.S. ROBOTICS OR ITS AUTHORISED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT U.S. ROBOTICS OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

6.0 DISCLAIMER:

Some countries, states, territories or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to CUSTOMER. When the implied warranties are not allowed by law to be excluded in their entirety, they will be limited to the TWO (2) YEAR duration of this written warranty. This warranty gives CUSTOMER specific legal rights, which may vary depending on local law.

7.0 GOVERNING LAW:

This Limited Warranty shall be governed by the laws of the State of Illinois, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL, 60173
U.S.A

USRobotics **Wireless MAXg Access Point: User Guide**

Regulatory Information

Declaration of Conformity

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL 60173
U.S.A.

declares that this product conforms to the FCC's specifications:

Part 15, Class B

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

This equipment complies with FCC Part 15 for Home and Office use.

Caution to the User: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Detachable Antenna Information

FCC Part 15, Subpart C, Section 15.203 Antenna requirement

5455 users: An intentional radiator shall be designed to ensure that no antenna other than that furnished by the responsible party shall be used with the device. The use of a permanently attached antenna or of an antenna that uses a unique coupling to the intentional radiator shall be considered sufficient to comply with the provisions of this section. The manufacturer may design the unit so that a broken antenna can be replaced by the user, but the use of a standard antenna jack or electrical connector is prohibited.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio and Television Interference:

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. If this equipment is not installed and used in accordance with the manufacturer’s instructions, it 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 to 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.

USR declares 5455 is limited in CH1~11 from 2412 to 2462 MHz by specified firmware controlled in USA.

UL Listing/CUL Listing:

This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for the uses described in the User Guide. Use this product only with UL Listed Information Technology Equipment (ITE).

This product is intended to be supplied by a UL Listed Direct Plug-in Power Unit rated 15 VDC, 1200 mA maximum.

For Canadian Users

Industry Canada (IC)

This equipment complies with RSS-210 of the Industry Canada Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding.

Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropic Radiated Power (EIRP) is not more than that required for successful communication.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

Radiation Exposure Statement: This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE0560 (!)

CE Compliance

Declaration of Conformity

We, U.S. Robotics Corporation of 935 National Parkway, Schaumburg, Illinois, 60173-5157 USA, declare under our sole responsibility that the product, USRobotics Wireless ***MAX*g** Access Point, Model 5455, to which this declaration relates, is in conformity with the following standards and/or other normative documents.

EN300 328
EN301 489-1
EN301 489-17
EN60950-1
EN61000-3-2
EN61000-3-3
EN50392

We, U.S. Robotics Corporation, hereby declare the above named product is in compliance and conformity with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The conformity assessment procedure referred to in Article 10 and detailed in Annex IV of Directive 1999/5/EC has been followed.

This equipment is in compliance with the European recommendation 1999/519/ECC, governing the exposure to the electromagnetic radiation.

This product can be used in the following countries:

- **European Union countries**: Germany, Austria, Belgium, Netherlands, Luxembourg, Italy, France, UK, Ireland, Spain, Portugal, Sweden, Denmark, Finland, Czech Republic, Poland, Hungary, and Greece.
- **Non-European Union countries**: Switzerland, Norway, and Turkey.

An electronic copy of the original CE Declaration of Conformity is available at the U.S. Robotics website: www.usr.com.

Regarding IEEE 802.11b/g frequencies, we currently have the following information about restrictions in the European Union (EU) countries:

- Italy

  Please be aware that use of the wireless device is subject to the following Italian regulation:

  1. D.Lgs 1.8.2003, number 259, articles 104 (activities where General Authorization is required) and 105 (free use), for private use;

  2. D.M 28.5.03 and later modifications, for the supplying to public RadioLAN access for networks and telecommunication services

- France

  In France metropolitan, outdoor power is limited to 10mW (EIRP) within 2454MHz – 2483, 5MHz frequency band

  In Guyana and Reunion Islands, outdoor use is forbidden within 2400MHz –

2420MHz frequency band

Regulatory Channel Frequency

Channel	Frequency (MHz)	FCC	Canada	ETSI
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467			X
13	2472			X

Operating Channels:	• IEEE 802.11g compliant • 11 channels (US, Canada) • 13 channels (ETSI)

EU Health Protection

This device complies with the European requirements governing exposure to electromagnetic radiation. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This wireless device is a transmitter/receiver and has been designed and manufactured to comply with the exposure limits recommended by the Council of the European Union and the International

Commission on Non-Ionizing Radiation Protection (ICNIRP, 1999) for the entire population. The exposure standard for portable equipment uses the "Specific Absorption Rate" as unit of measure. The maximum SAR value of this wireless device measured in the conformity test is 1.58mw/g(10g).

EU Detachable Antenna Information

This USRobotics wireless device has been designed to operate with the antenna included in this package only. Together this device and antenna combination has been tested and approved by a European Agency conforming with the European R&TTE directive 1999/5/EC to meet the radiated power level requirement of 100mW (EIRP). Replacement of this antenna must only be done with an authorized USRobotics component that has been designed and tested with the unit to the requirements of directive 1999/5/EC. Please refer to the U.S. Robotics Web site to get product antenna ordering information.

Go to www.usr.com to see the most recent channel restriction information.

Wireless MAXg Access Point: User Guide

Copyright Information

U.S. Robotics Corporation
935 National Parkway
Schaumburg, Illinois
60173-5157
USA

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as a translation, transformation, or adaptation) without written permission from U.S. Robotics Corporation. U.S. Robotics Corporation reserves the right to revise this documentation and to make changes in the products and/ or content of this document from time to time without obligation to provide notification of such revision or change. U.S. Robotics Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or ! LICENSE.TXT. If you are unable to locate a copy, please contact U.S. Robotics and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101 (a) and as such is provided with only such rights as are provided in U.S. Robotics standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987) whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this Quick Installation Guide.

Installing the Access Point

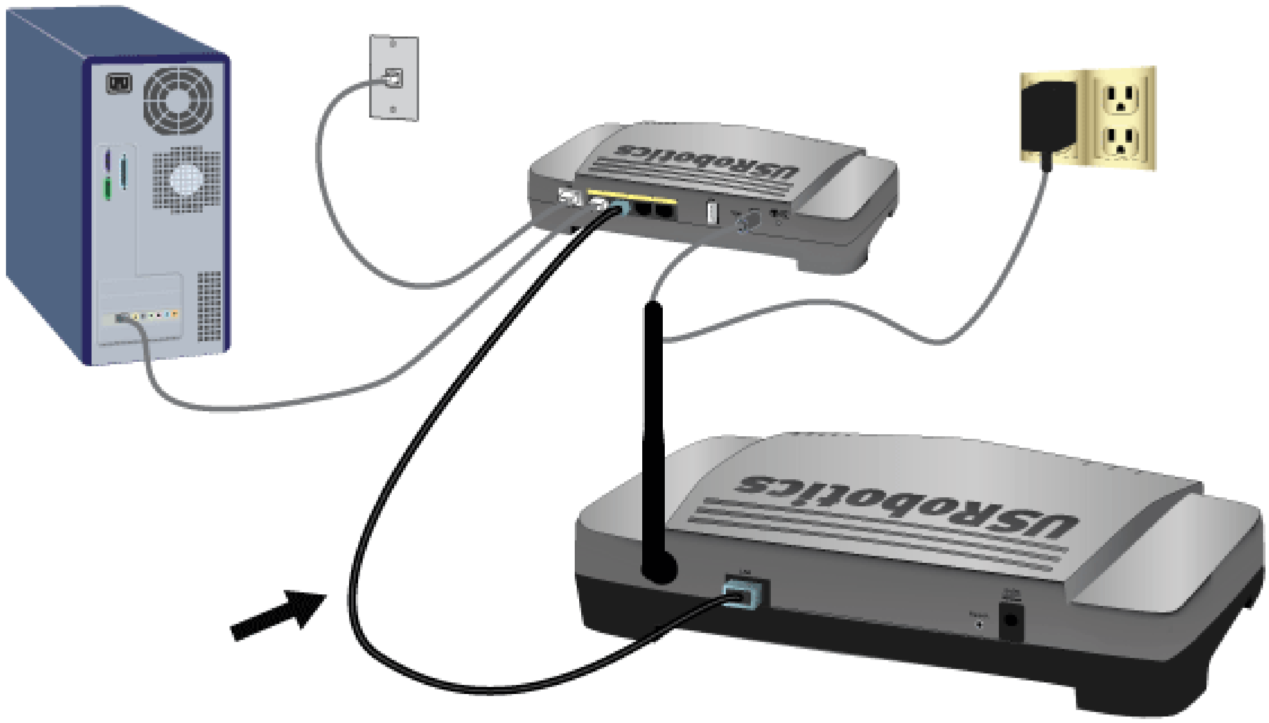
If you are connecting the access point to a router or other networking device without a DHCP server, see The networking device I am using does not have a DHCP server in the "Troubleshooting" section of this User Guide.

Step One: Connect the Access Point

1. Look at the label on the bottom of the access point and note its LAN MAC address. You may need it to distinguish the access point from other devices on your network.

2. Connect the provided antenna to the back of the access point if it is not already connected.

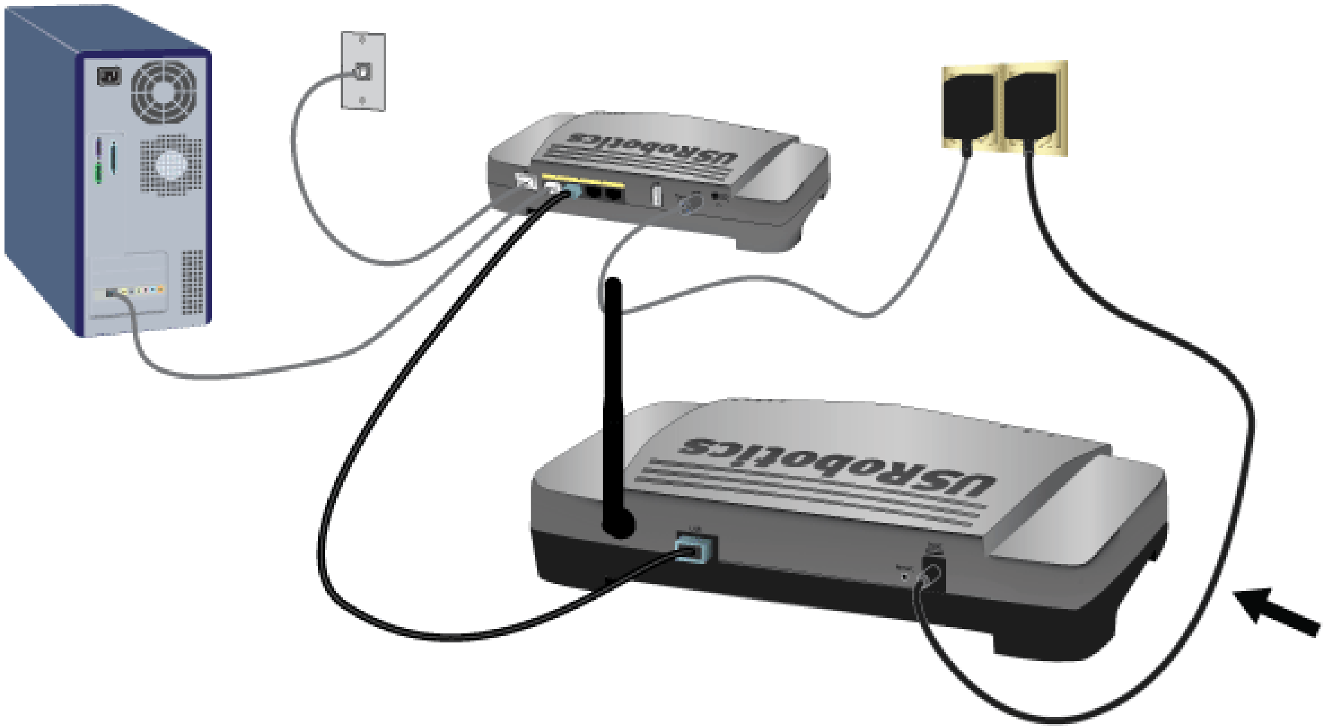
3. Use the supplied Ethernet cable to connect the LAN port on the access point to a LAN port on your networking device.



4. Supply power to the access point as follows:

Note to UK Users: With the power adapter unplugged, connect the appropriate power plug for your country on to the power adapter. Apply enough pressure to cause a click and firmly seat the plug.

A. Connect the supplied power adapter to the **9VDC** port on the access point.



B. Plug the power adapter into a standard power outlet.

Note: This product is intended to be supplied by a Listed Direct Plug-in Power Unit marked Class 2 and rated 9VDC, 1200 mA.

Step Two: Start the Setup Wizard

The setup wizard makes it easy for you perform basic setup of the access point. To start the wizard using an operating system other than Windows, go to Setup Wizard for Non-Windows Users.

Setup Wizard for Windows Users

If you are using a Windows operating system, you can use the setup program on the USRobotics

Installation CD-ROM to install and run the USRobotics Wireless MAXg Detection Utility and configure basic settings in one easy, continuous process:

1. Insert the USRobotics Installation CD-ROM into the CD-ROM or DVD drive.

   If the CD doesn't start automatically, start it manually as follows:

   A. **Windows Vista:** Click Windows **Start > Computer**.

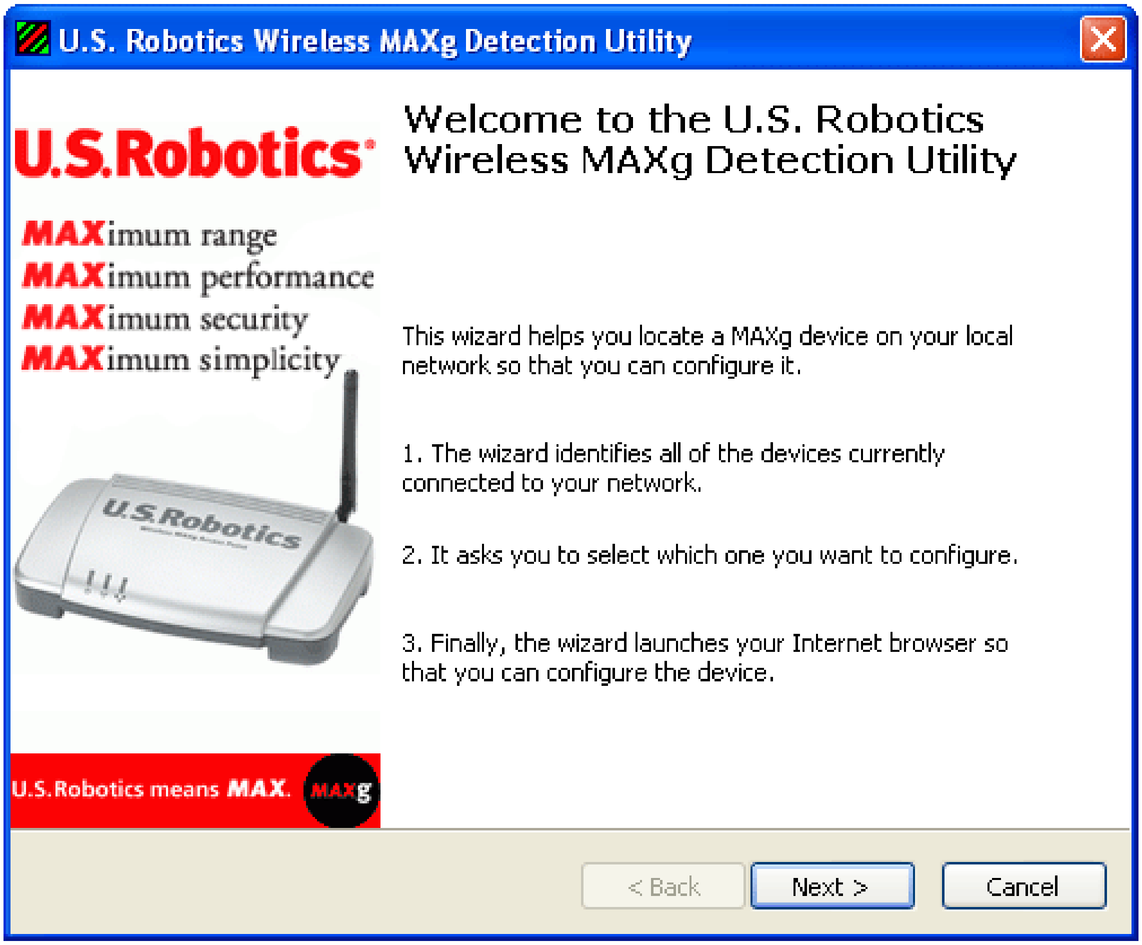
      Windows XP: Click Windows **Start > My Computer**.

      Windows 2000: On the desktop, double-click **My Computer**.

   B. Double-click the CD drive.

2. Follow the on-screen instructions to install the detection utility.

   When the utility is installed, it starts automatically:



U.S. Robotics Wireless MAXg Detection Utility

Welcome to the U.S. Robotics Wireless MAXg Detection Utility

This wizard helps you locate a MAXg device on your local network so that you can configure it.

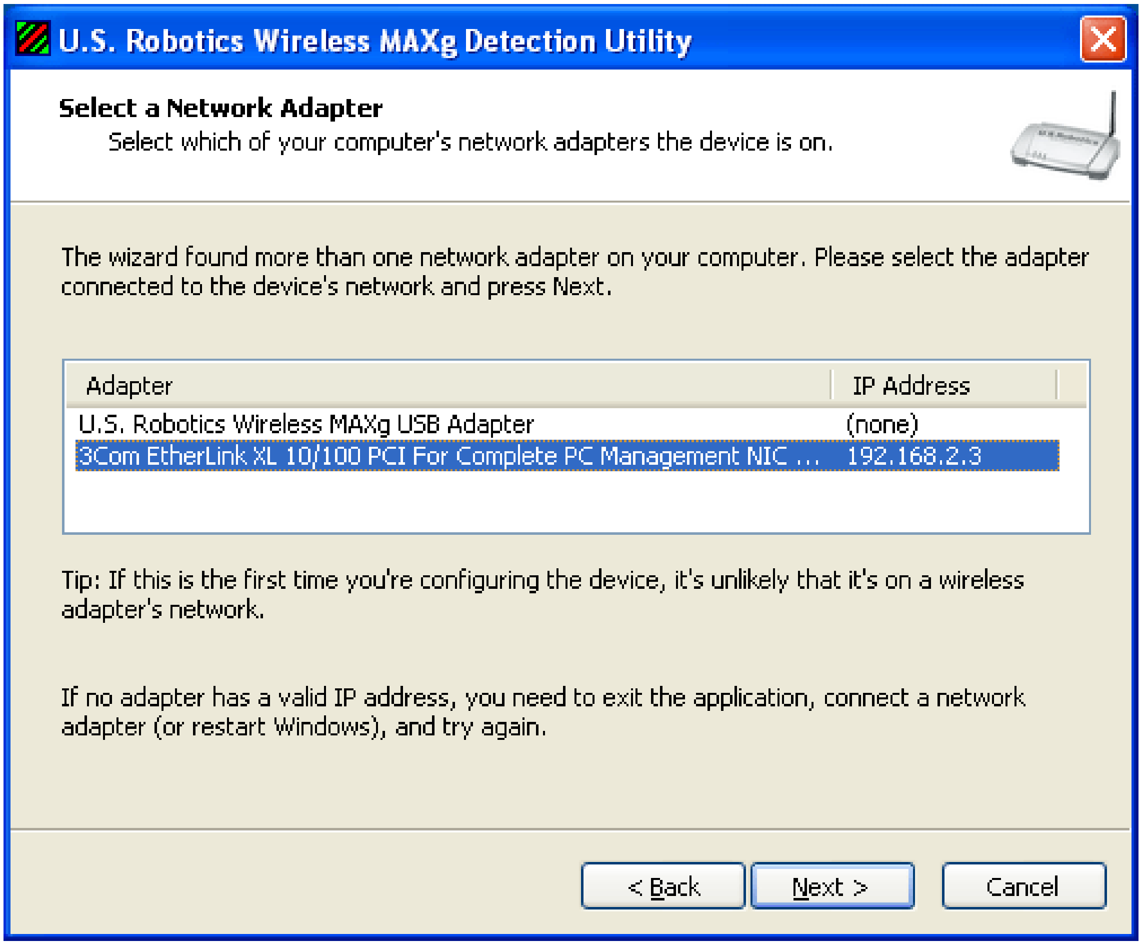
1. The wizard identifies all of the devices currently connected to your network.

2. It asks you to select which one you want to configure.

3. Finally, the wizard launches your Internet browser so that you can configure the device.

3. Click **Next**.

   If the computer has more than one network adapter, the detection utility lists them:



U.S. Robotics Wireless MAXg Detection Utility

Select a Network Adapter

Select which of your computer's network adapters the device is on.

The wizard found more than one network adapter on your computer. Please select the adapter connected to the device's network and press Next.

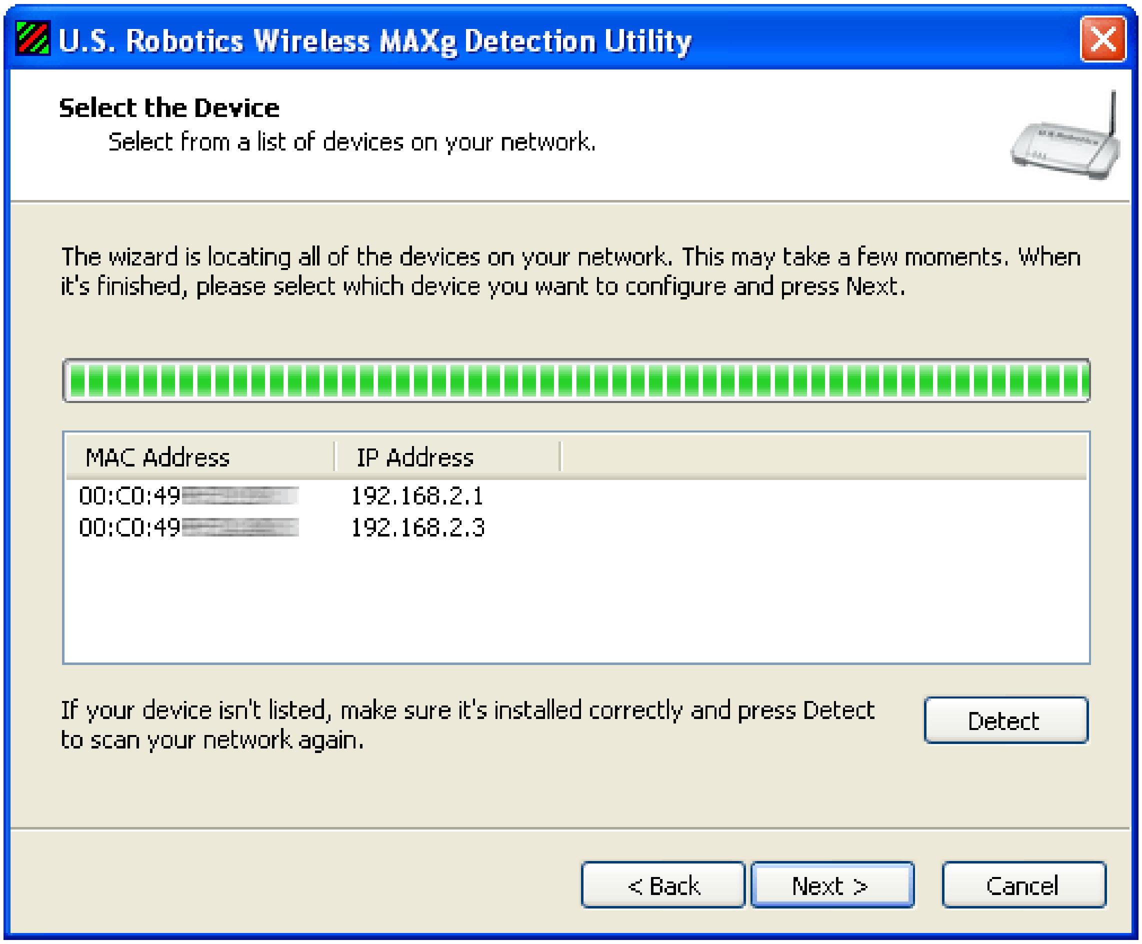
Adapter	IP Address
U.S. Robotics Wireless MAXg USB Adapter	(none)
3Com EtherLink XL 10/100 PCI For Complete PC Management NIC ...	192.168.2.3

Tip: If this is the first time you're configuring the device, it's unlikely that it's on a wireless adapter's network.

If no adapter has a valid IP address, you need to exit the application, connect a network adapter (or restart Windows), and try again.

4. Select the adapter that is connected to the access point's network and Click **Next**.

   The detection utility lists the access point as well as any other USRobotics devices that were found:



U.S. Robotics Wireless MAXg Detection Utility

Select the Device

Select from a list of devices on your network.

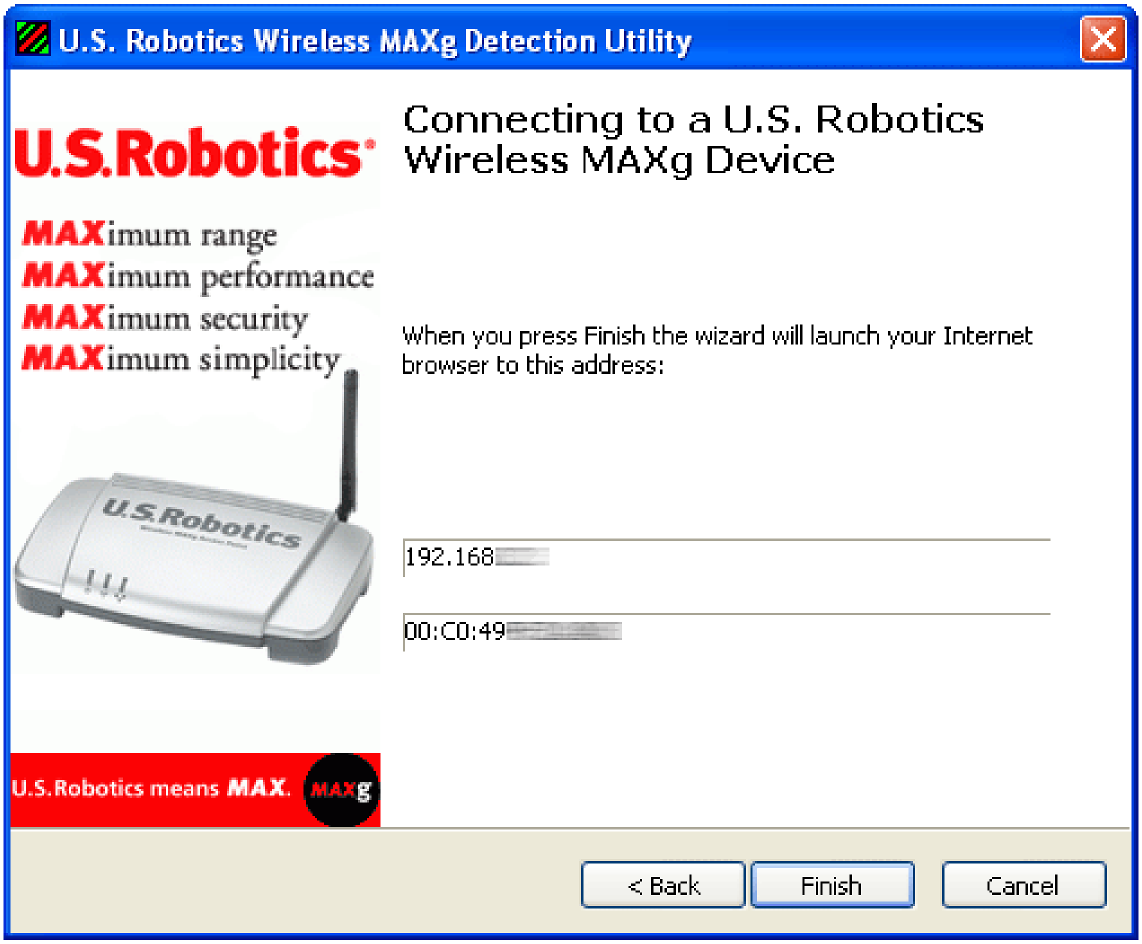
The wizard is locating all of the devices on your network. This may take a few moments. When it's finished, please select which device you want to configure and press Next.

MAC Address	IP Address
00:C0:49[redacted]	192.168.2.1
00:C0:49[redacted]	192.168.2.3

If your device isn't listed, make sure it's installed correctly and press Detect to scan your network again.

5. Select the device whose MAC address matches the LAN MAC address on the bottom of the access point, and click **Next**.

   The locator displays the IP address and LAN MAC address of the access point:



Connecting to a U.S. Robotics Wireless MAXg Device

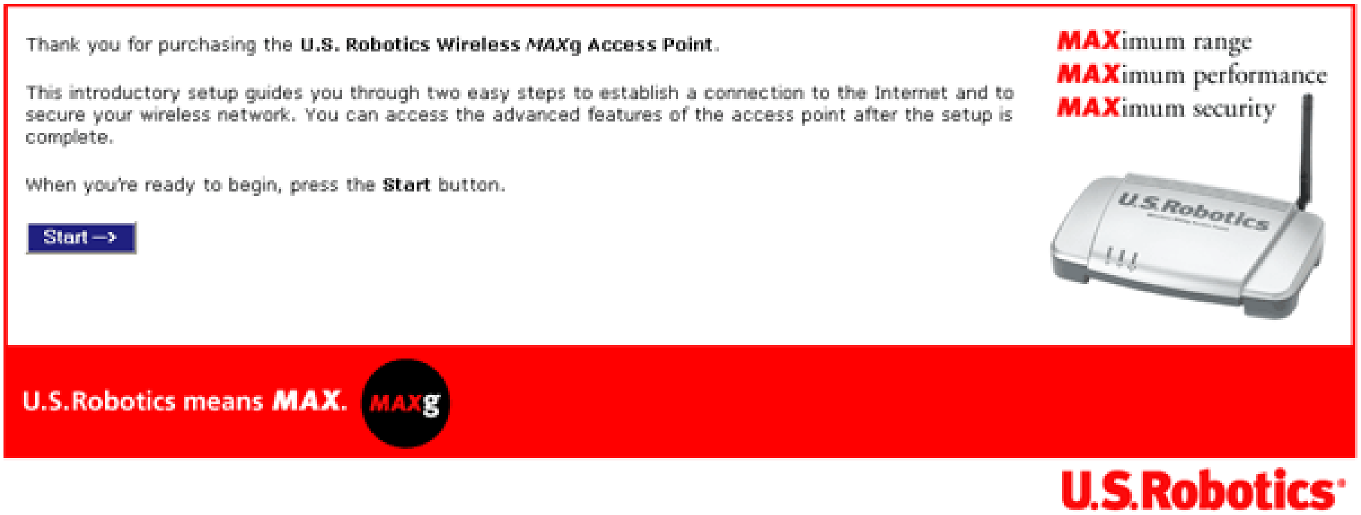
When you press Finish the wizard will launch your Internet browser to this address:

192.168[redacted]

00:C0:49[redacted]

6. Click **Finish**.

The detection utility starts the setup wizard for the access point:



Thank you for purchasing the **U.S. Robotics Wireless *MAXg* Access Point**.

This introductory setup guides you through two easy steps to establish a connection to the Internet and to secure your wireless network. You can access the advanced features of the access point after the setup is complete.

When you're ready to begin, press the **Start** button.

Proceed to "Step Three: Configure Basic Settings".

Setup Wizard for Non-Windows Users

If you are using an operating system other than Windows, you first need to find the IP address of the access point. Then you can start the setup wizard to configure the basic settings of the access point.

Find the IP Address of the Access Point

The networking device to which you connected the access point assigns IP addresses on your local network. To find the IP address of the access point:

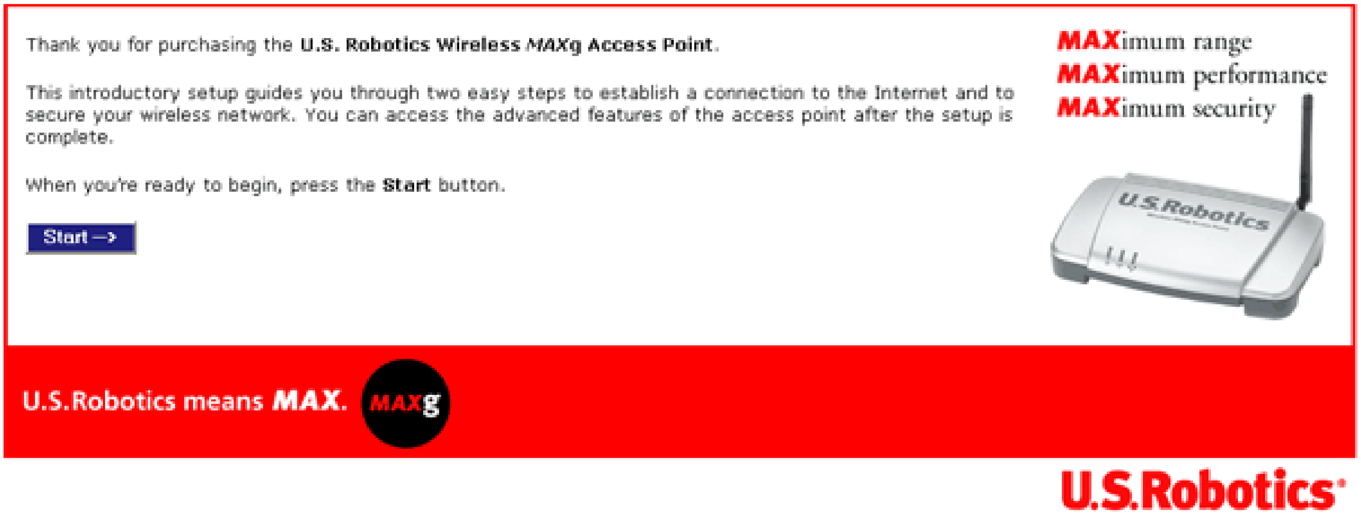
1. Access the configuration program or configuration pages of the networking device. For detailed instructions, consult the documentation for the networking device.
2. Find the list of clients associated with the networking device.
3. On the client list, find the LAN MAC address of the access point.

   You can find the LAN MAC address of the access point on the label on the bottom of the access point.
4. Note the IP address associated with the LAN MAC address of the access point.

Run the Setup Wizard

1. Start your Web browser.
2. In the location or address line, type the IP address of the access point and press ENTER.

   The wizard displays its welcome page:



Thank you for purchasing the **U.S. Robotics Wireless *MAXg* Access Point**.

This introductory setup guides you through two easy steps to establish a connection to the Internet and to secure your wireless network. You can access the advanced features of the access point after the setup is complete.

When you're ready to begin, press the **Start** button.

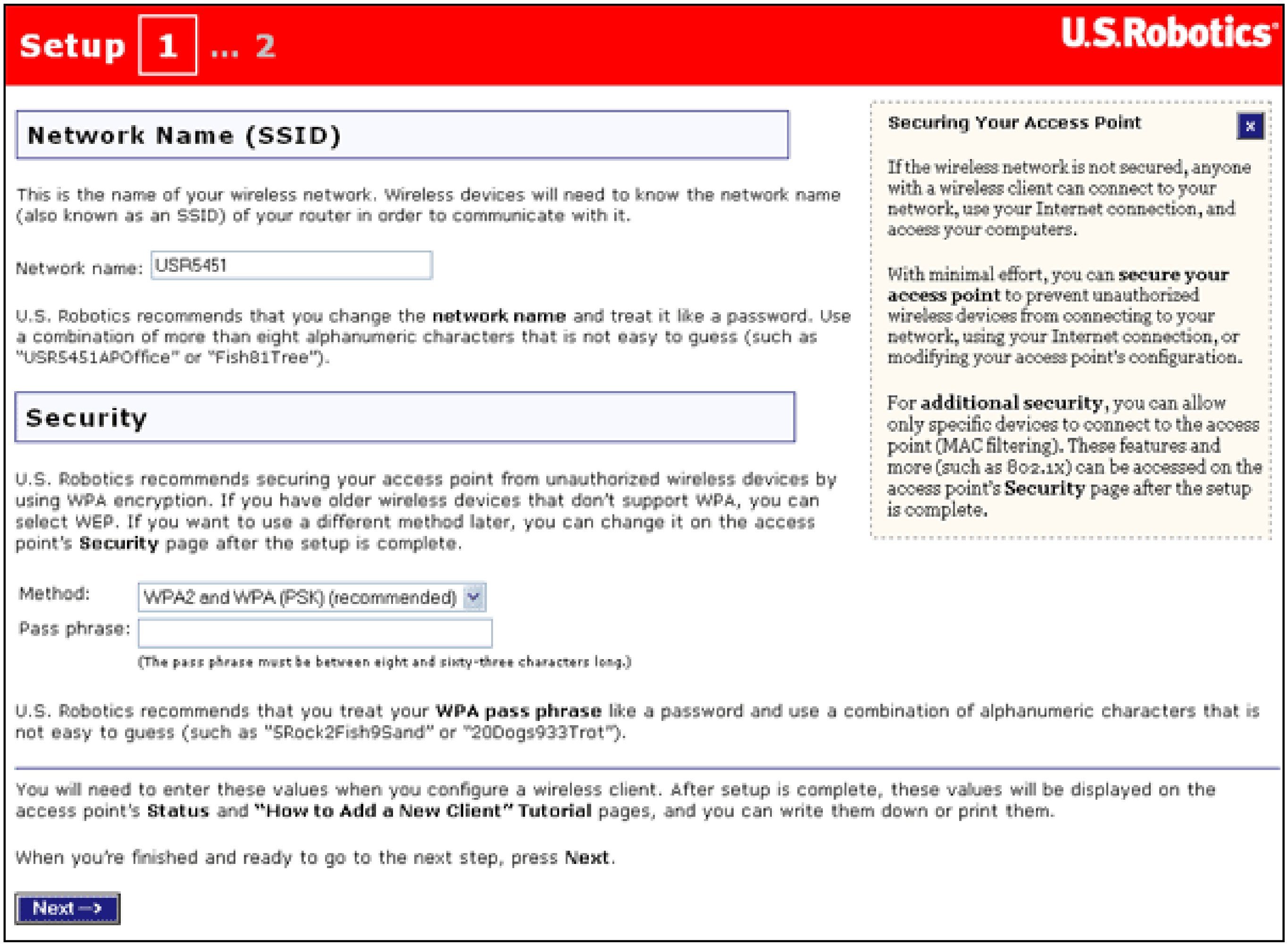
Step Three: Configure Basic Settings

In the setup wizard, follow the on-screen instructions to complete the initial setup of the access point as follows:

> **Note**: If you see a “Page Not Found” error at any time while using the setup wizard, press the **Back** button in your Web browser or refresh the page.

1. Click **Start**.

   The setup wizard displays the first setup page:



Network Name (SSID)

This is the name of your wireless network. Wireless devices will need to know the network name (also known as an SSID) of your router in order to communicate with it.

Network name: USR5451

U.S. Robotics recommends that you change the **network name** and treat it like a password. Use a combination of more than eight alphanumeric characters that is not easy to guess (such as "USR5451APOffice" or "Fish81Tree").

Security

U.S. Robotics recommends securing your access point from unauthorized wireless devices by using WPA encryption. If you have older wireless devices that don't support WPA, you can select WEP. If you want to use a different method later, you can change it on the access point's **Security** page after the setup is complete.

Method: WPA2 and WPA (PSK) (recommended)

Pass phrase:

(The pass phrase must be between eight and sixty-three characters long.)

U.S. Robotics recommends that you treat your **WPA pass phrase** like a password and use a combination of alphanumeric characters that is not easy to guess (such as "5Rock2Fish9Sand" or "20Dogs933Trot").

You will need to enter these values when you configure a wireless client. After setup is complete, these values will be displayed on the access point's **Status** and **"How to Add a New Client" Tutorial** pages, and you can write them down or print them.

When you're finished and ready to go to the next step, press **Next**.

Securing Your Access Point

If the wireless network is not secured, anyone with a wireless client can connect to your network, use your Internet connection, and access your computers.

With minimal effort, you can **secure your access point** to prevent unauthorized wireless devices from connecting to your network, using your Internet connection, or modifying your access point's configuration.

For **additional security**, you can allow only specific devices to connect to the access point (MAC filtering). These features and more (such as 802.1x) can be accessed on the access point's **Security** page after the setup is complete.

2. Enter a new **Network Name**.

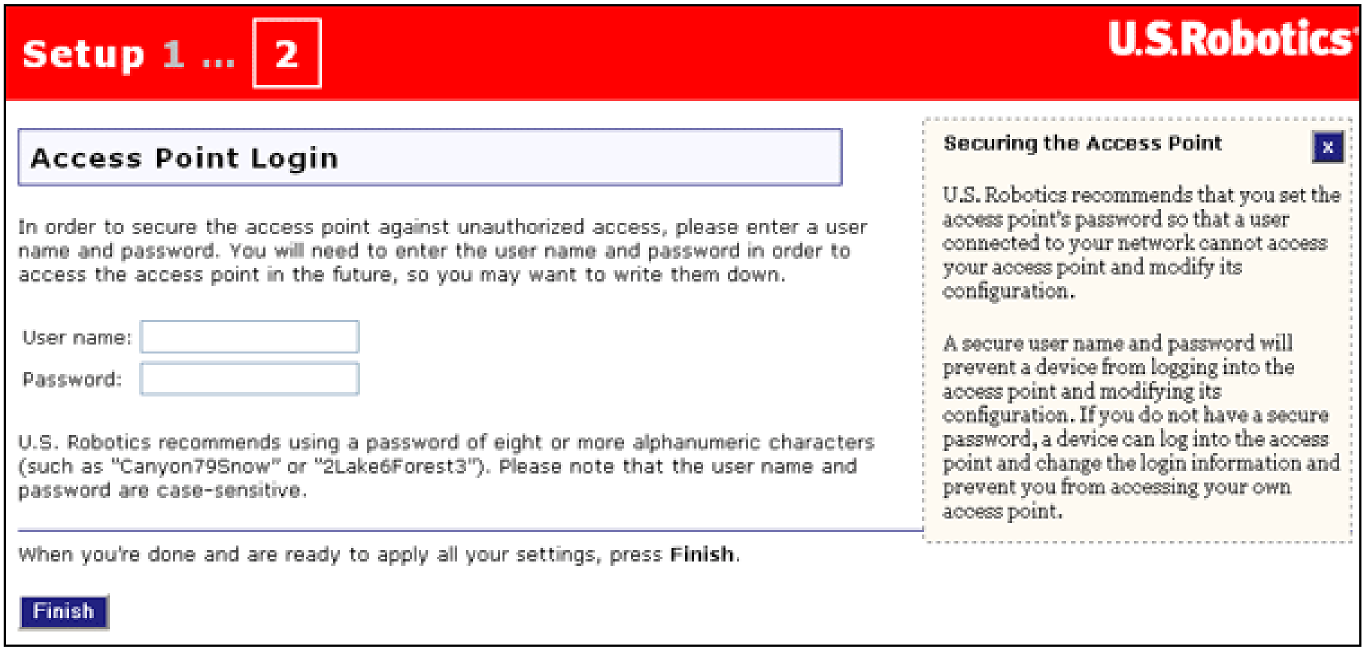
   This is the name that will identify the Wireless ***MAXg*** Access Point to wireless clients on a wireless network.

3. Select a security **Method** and enter a pass phrase.

Note: For your wireless security settings, it is recommended that you select the **WPA2 and WPA (PSK)** wireless security method using **TKIP and AES** encryption for the most secure wireless network.

4. Click **Next**.

   When your security settings are complete, the setup wizard displays the login setup page:



Access Point Login

In order to secure the access point against unauthorized access, please enter a user name and password. You will need to enter the user name and password in order to access the access point in the future, so you may want to write them down.

User name:

Password:

U.S. Robotics recommends using a password of eight or more alphanumeric characters (such as "Canyon79Snow" or "2Lake6Forest3"). Please note that the user name and password are case-sensitive.

When you're done and are ready to apply all your settings, press **Finish**.

Securing the Access Point

U.S. Robotics recommends that you set the access point's password so that a user connected to your network cannot access your access point and modify its configuration.

A secure user name and password will prevent a device from logging into the access point and modifying its configuration. If you do not have a secure password, a device can log into the access point and change the login information and prevent you from accessing your own access point.

5. Enter a **User name** and **Password** and click **Finish**.

Note: Remember the user name and password that you enter. You will need it whenever you access the configuration pages of the access point.

The access point displays its status page. If you intend to connect wireless devices to the access point manually, you will need the information on the status page. Consider bookmarking the page for easy access to the required information.

You have successfully completed the installation procedure. You can verify your network connection by registering your Wireless ***MAXg*** Access Point at www.usr.com/productreg/.

To connect a client to the access point, see Connecting a Wireless Client in this user guide.

Backing Up Your Configuration Settings

Having a backup reduces the effort required in reapplying your configuration settings should you ever restore your access point to its factory default settings. USRobotics recommends that you back up your settings now.

1. In the configuration pages, click the **Device** tab and scroll down to **Back Up Settings**.
2. Click **Back Up**.

   Your system prompts you to save or open the file.

3. Click **Save**.

USRobotics *Wireless MAXg Access Point:*

User Guide

Wi-Fi Protected Setup™ Configuration

The Wireless ***MAX*g** Access Point supports Wi-Fi Protected Setup™ (WPS). You can use WPS to configure your wireless network using a push button or PIN code.

Only certain wireless adapters in Windows Vista and Windows XP, Service Pack 2, can use Wi-Fi Protected Setup. See the documentation for your wireless adapter to determine whether your wireless client can configure the Wireless ***MAX*g** Access Point using Wi-Fi Protected Setup.

To configure the access point for WPS, follow these steps:

Note to reviewers: This draft requires two perspectives for WPS: using an external registrar and using an internal registrar. Please ignore the following set of steps.

1. Be ready to start WPS on your wireless adapter.

   Once you reboot the access point during this procedure, you have 2 minutes to start the WPS setup on your wireless adapter.

2. Reboot the access point by disconnecting and then reconnecting its power supply.

3. Start a web browser.

4. Log in to configuration pages for the access point.

5. In the lower right corner of the page is an eight-digit WPS PIN. Note the PIN because you need it in oder to configure the router using WPS.

6. In the configuration utility for your WPS wireless adapter, enter the PIN from the router's start page. For instructions on installing your wireless adapter, see your wireless adapter’s documentation.
7. The wireless adapter detects the WPS settings of the access point and negotiates a secure (WPA2) wireless connection to the network.
8. If the WPS connection does not complete, unplug the disconnec and then reconnecting the access point's power supply, then repeat the installation procedure using the new PIN code on the access point's start page.?.

If you use an external registrar to configure the access point using WPS, all devices connecting to the access point must do so via the external registrar.

You have successfully completed the installation procedure. Please register the access point at www.usr.com/productreg/.

USRobotics *Wireless MAXg Access Point: User Guide*

Connecting a Wireless Client

1. Ensure that the wireless adapter to be connected to the network is set to infrastructure mode. For instruction in changing your adapter's wireless mode, see your wireless adapter's documentation.

2. Set the network name or SSID in the wireless adapter's settings to the network name that is used on the access point. You can find the network name for the access point on the **Status** page.

3. Ensure that the wireless security settings for the wireless adapter match those that you set on the access point. You can find the wireless security settings for the access point on the **Status** page. For instruction in changing your adapter's wireless security settings, see your wireless adapter's documentation.

USRobotics *Wireless MAXg Access Point:*

User Guide

Configuration Pages

The Wireless ***MAXg*** Access Point provides configuration pages so that you can manage and monitor the access point from any computer on the network. Under normal operating conditions, you do not need to change the basic configuration that you established when you installed your access point. However, if your network environment changes, you may decide to reconfigure your access point to reflect the new environment.

The topics below address the following aspects of using the configuration pages:

- Configuring Your Web Browser
- Logging in to the Configuration Pages
- Configuration Page Reference

Configuring Your Web Browser

You may need to disable the HTTP Proxy feature of your Web browser so the configuration pages will display the most current information.

Internet Explorer users:

1. Click **Tools** > **Internet Options**, and select the **Connections** tab.
2. Select **Never dial a connection**, then click **Apply**.
3. Click **OK**.
4. Click **Tools** > **Internet Options**, and select the **Connections** tab again.

5. Click the **LAN Settings** button.

6. Clear all the check boxes and click **OK**.

7. Click **OK** again.

Netscape Navigator 8.x users:

1. Click **Tools** > **Options** > **General**.

2. Click the **Connection Settings** button.

3. Select **Direct connection to the Internet**, then click **OK**.

Logging In to the Configuration Pages

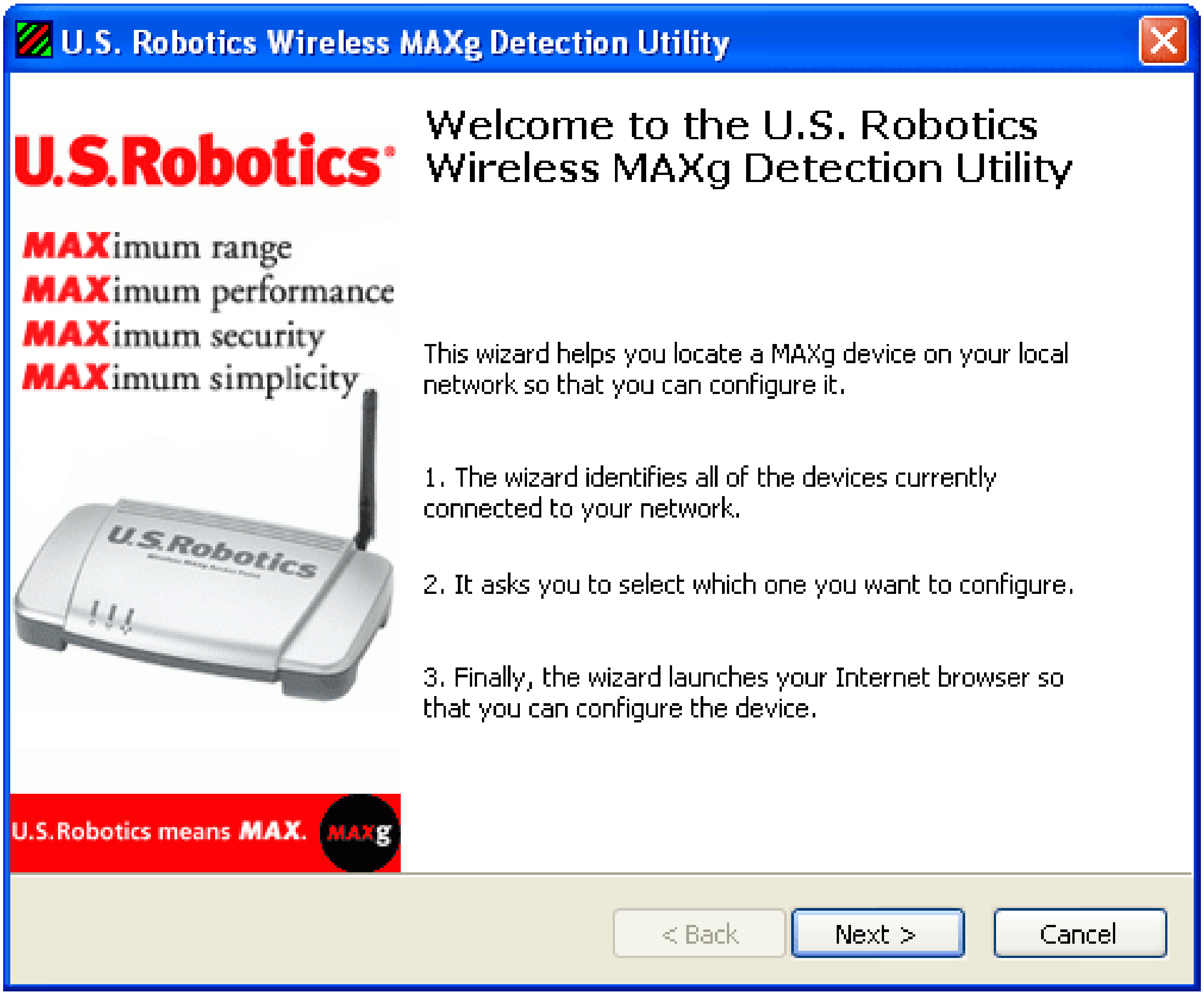
If you know the IP address of the access point, simply type it in your Web browser's location or address line and press ENTER. If you do not know the IP address of the access point, follow one of the procedures below to find it:

Using the Detection Utility(Windows Users Only)

1. **Windows Vista or XP:** Click Windows **Start > All Programs > U.S. Robotics Wireless MAXg Device Detection Utility.**

   All Other Windows Operating Systems: Click Windows **Start > Programs > U.S. Robotics Wireless MAXg Device Detection Utility**.

   The detection utility displays its welcome screen:



Welcome to the U.S. Robotics Wireless MAXg Detection Utility

This wizard helps you locate a MAXg device on your local network so that you can configure it.

1. The wizard identifies all of the devices currently connected to your network.

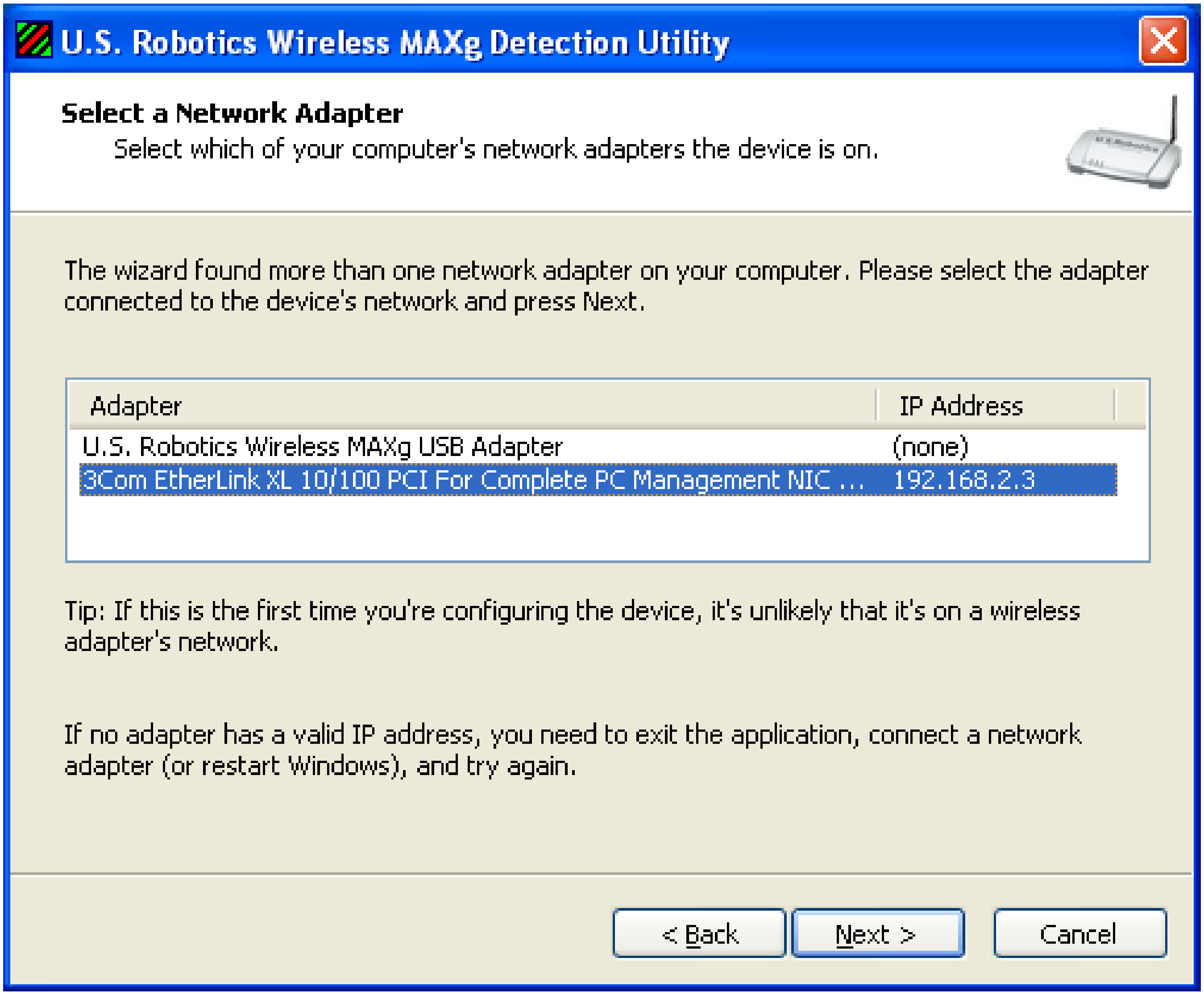
2. It asks you to select which one you want to configure.

3. Finally, the wizard launches your Internet browser so that you can configure the device.

2. Click **Next**

.

The locator lists the access point as well as any other USRobotics devices that were found:



U.S. Robotics Wireless MAXg Detection Utility

Select a Network Adapter

Select which of your computer's network adapters the device is on.

The wizard found more than one network adapter on your computer. Please select the adapter connected to the device's network and press Next.

Adapter	IP Address
U.S. Robotics Wireless MAXg USB Adapter	(none)
3Com EtherLink XL 10/100 PCI For Complete PC Management NIC ...	192.168.2.3

Tip: If this is the first time you're configuring the device, it's unlikely that it's on a wireless adapter's network.

If no adapter has a valid IP address, you need to exit the application, connect a network adapter (or restart Windows), and try again.

3. Find the Wireless ***MAXg*** Access Point in the list. (If you have more than one Wireless ***MAXg*** Access Point, find the device whose MAC address matches the LAN MAC address on the bottom of the access point that you are trying to access). Note the IP address associated with the LAN MAC address of the access point.

4. Click **Next**.

Manually Finding the IP Address of the Access Point

The networking device to which you connected the access point assigns IP addresses on your local network. To find the IP address of the access point:

1. Access the configuration program or configuration pages of the networking device. For detailed instructions, consult the documentation for the networking device.

2. Find the list of clients associated with the networking device.

3. On the client list, find the LAN MAC address of the access point.

4. Make a note the IP address associated with the LAN MAC address of the access point.

Configuration Page Reference

The configuration pages are divided into the functional areas shown on its tabs and listed below; for the description of a page, click one of the following links:

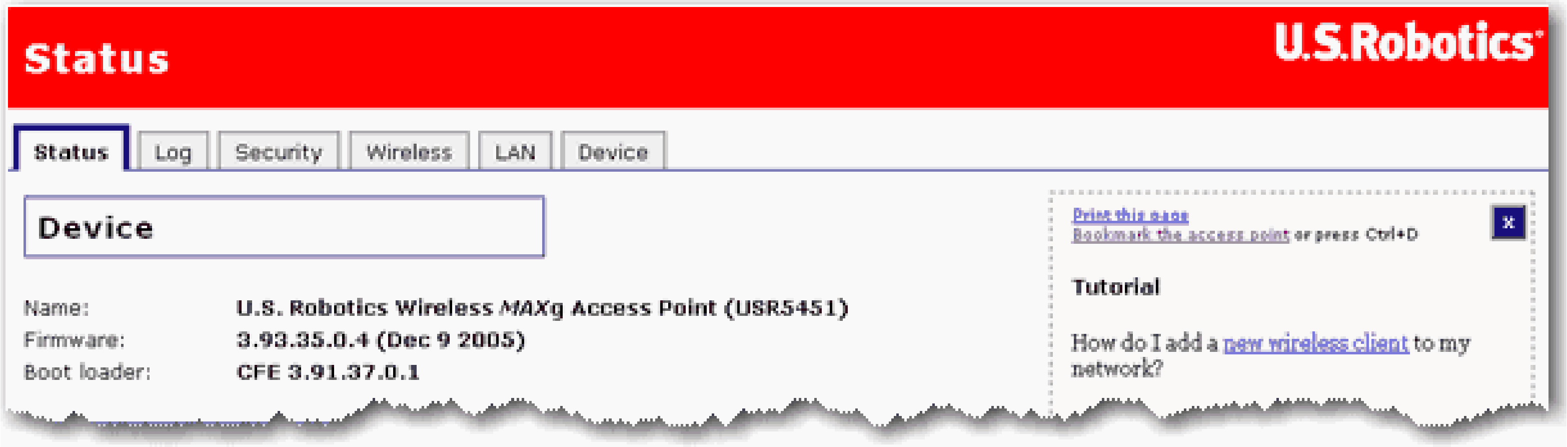
- Status
- Log
- Security
- Wireless
- LAN
- Device

Access Point Status Information

From **Status** page, you can view the current status of your access point and its features.

Refresh: Click **Refresh** at the bottom of the page to update the page with current information.

Device



Device

Name:	U.S. Robotics Wireless MAXg Access Point (USR5451)
Firmware:	3.93.35.0.4 (Dec 9 2005)
Boot loader:	CFE 3.91.37.0.1

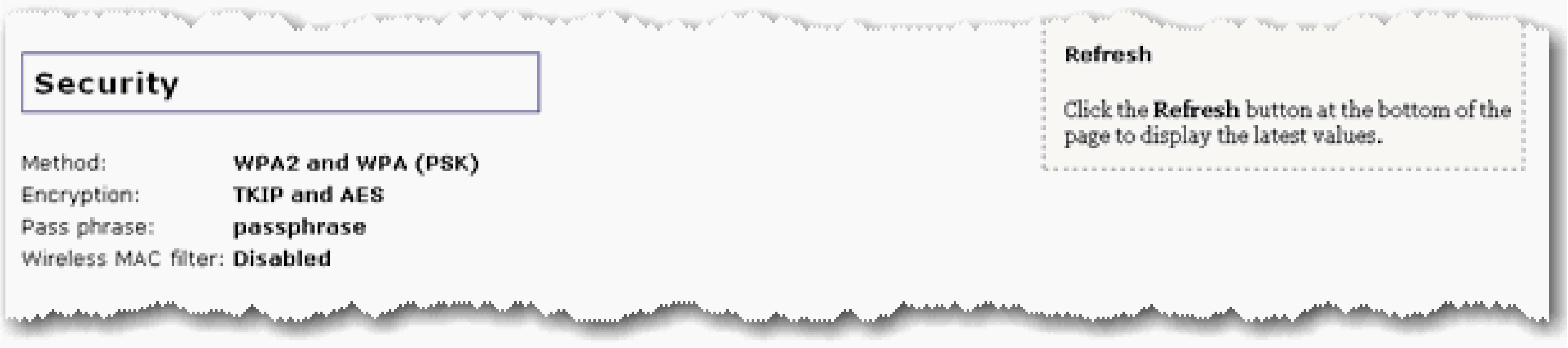
Print this page
Bookmark the access point or press Ctrl+D

Tutorial

How do I add a new wireless client to my network?

- **Name:** The name of the access point.
- **Firmware**:The current firmware version on your access point.
- **Boot loader**:The boot loader version that is running on your access point.

Security



Security

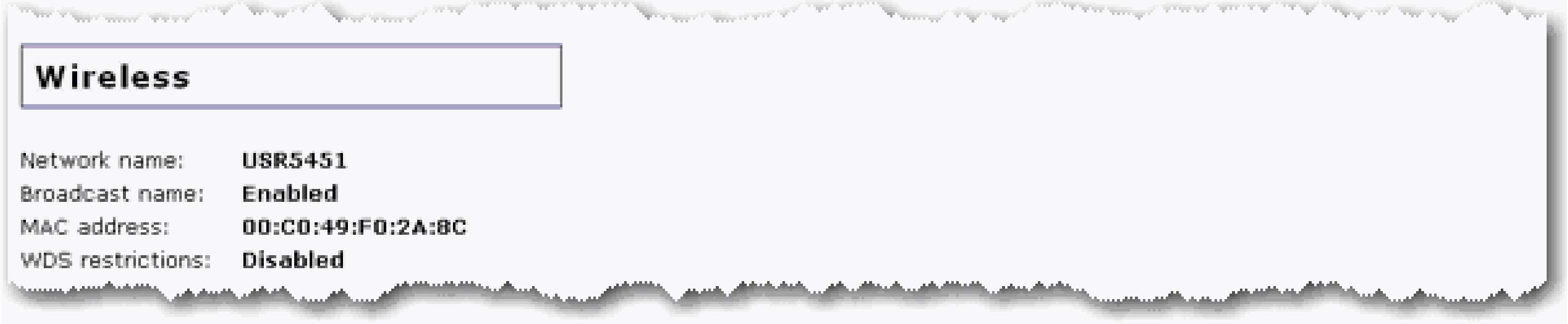
Method: WPA2 and WPA (PSK)
Encryption: TKIP and AES
Pass phrase: passphrase
Wireless MAC filter: Disabled

Refresh

Click the **Refresh** button at the bottom of the page to display the latest values.

- **Method**: The security method for your access point. This information can be configured from the **Wireless** section of the Security page.
- **Encryption**: The encryption type for your access point. This information can be configured from the **Wireless** section of the Security page.
- **Pass Phrase**: The Pass phrase or Key for your access point. This information can be configured from the **Wireless** section of the Security page.
- **Wireless MAC filter** (Access Point and Range Extender modes only): Displays whether the wireless MAC Filter is **Enabled** or **Disabled** on your network. This information can be configured from the **Wireless** section of the Security page.

Wireless

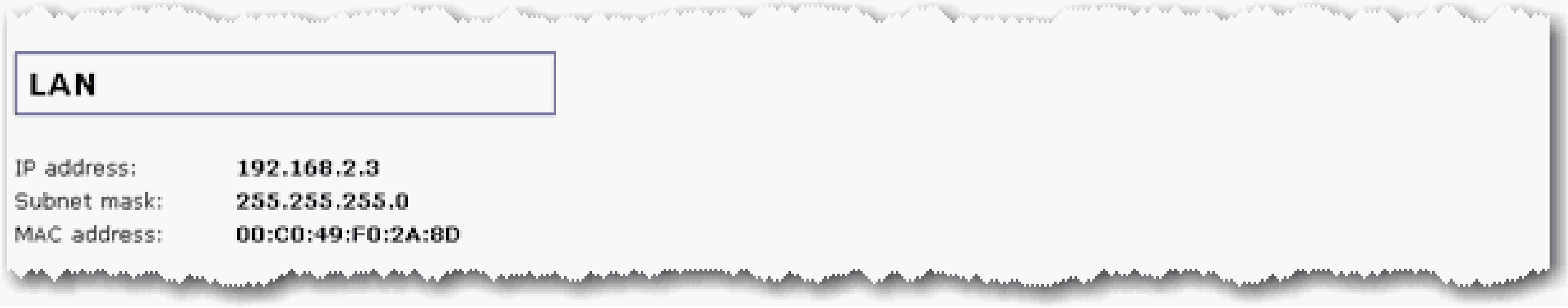


Wireless

Network name: USR5451
Broadcast name: Enabled
MAC address: 00:C0:49:F0:2A:8C
WDS restrictions: Disabled

- **Network name:** The Network name of the access point that is broadcast for wireless connections. This can be configured from the **Wireless** page.
- **Broadcast name:** Whether the broadcasting of the network name is **Enabled** or **Disabled**. This can be configured from the **Wireless** page.
- **MAC address:** The wireless (WLAN) MAC address of the access point.
- **WDS restrictions:** The status of WDS restrictions on the access point, either **Enabled** or **Disabled.**

LAN



LAN

IP address: 192.168.2.3

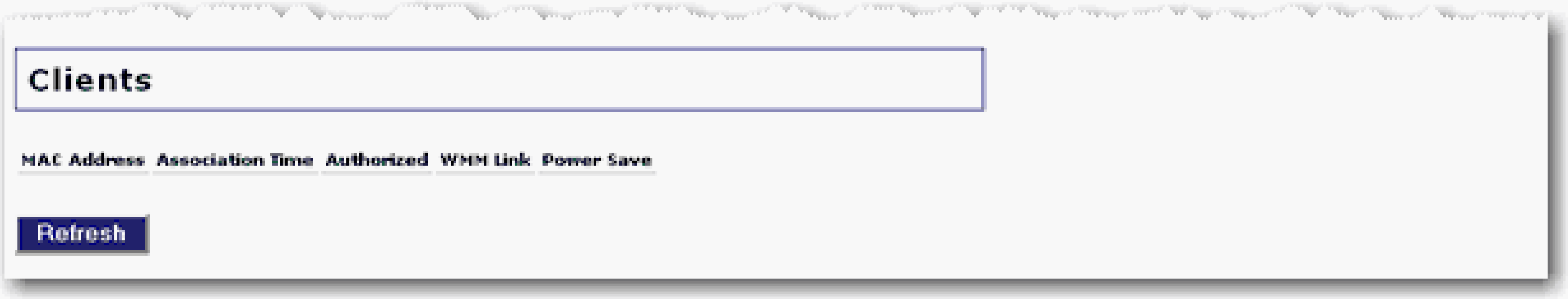
Subnet mask: 255.255.255.0

MAC address: 00:C0:49:F0:2A:8D

- **IP address:** The IP address that your access point uses on the LAN.
- **Subnet mask:** The LAN interface Subnet Mask of your access point.
- **MAC address:** The MAC address of your access point.

Clients

Note: Any devices connected to the access point that have static IP addresses will not show up in the **Clients** list. Also, devices that are connected through a WDS connection will be displayed as **wired** clients.



Clients

MAC Address	Association Time	Authorized	WMM Link	Power Save

- **MAC Address**: The MAC address of the connected device.
- **Association Time**: The time since the wireless client last associated with the access point.
- **Authorized**: If the client is authorized to connect to this access point, the status will display as **Yes**. If the client is not to connect to the networking device or Wireless ***MAX*g** Access Point, the status will display as **No**.
- **WMM Link**: If the client supports WMM, the status displays **Yes**. If the client does not support WMM, the status displays **No**.
- **Power Save**: If the client is running in Power Save mode, the status displays **Yes**. If the client is not in Power Save mode, the status displays **No**.

Log

This page lets capture system events in a log and send it to your syslog server.

To set up the log:

1. Select **System log**.

   The access point prompts you for a LAN IP address.

2. Enter a LAN IP address.

   The LAN IP address must identify a computer that is running a syslog daemon. Your syslog server (sometimes referred to as *daemon*) must be configured to run on port 514 using UDP protocol.

3. Click **Save**.

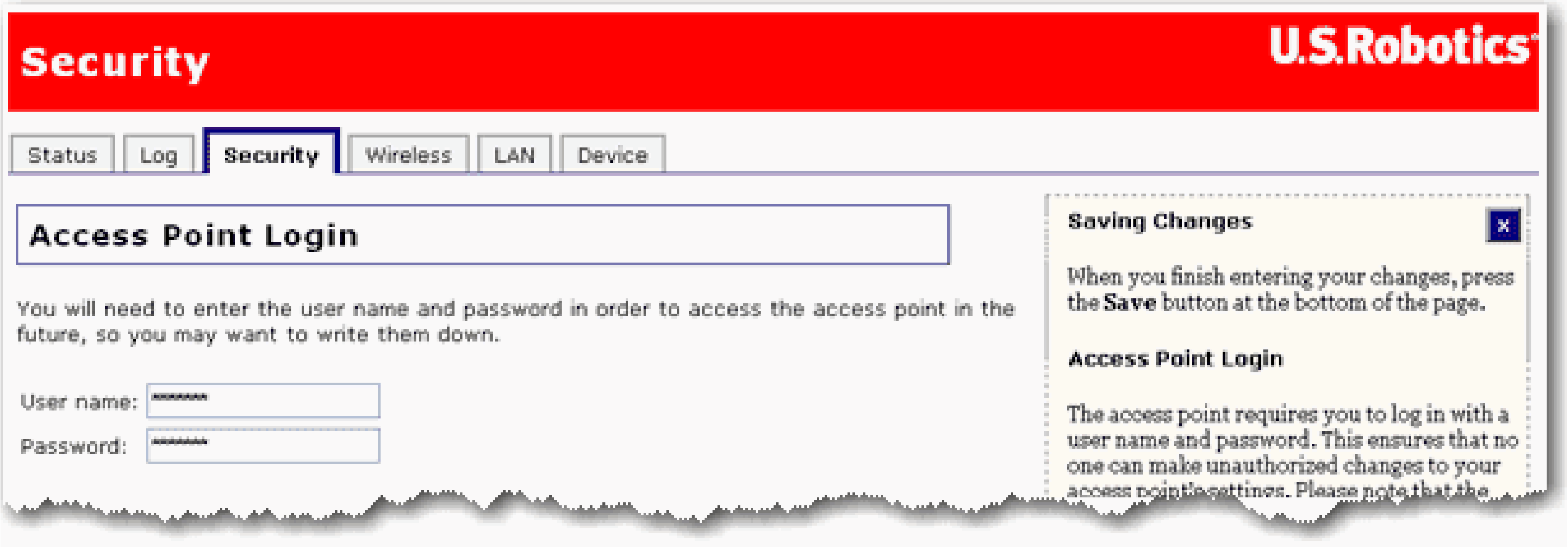
USRobotics ***Wireless MAXg Access Point: User Guide***

Security

The **Security** page lets you configure and change the security settings for the access point, including your wireless security settings, MAC address filtering options, and login information.

Access Point Login

This section lets you change the user name and password required to use the configuration pages in the access point. To change these fields, enter the new user name and password and click **Save** at the bottom of the page. Then use the new name and password to log in to your access point.



Access Point Login

You will need to enter the user name and password in order to access the access point in the future, so you may want to write them down.

User name: ********

Password: ********

Saving Changes

When you finish entering your changes, press the **Save** button at the bottom of the page.

Access Point Login

The access point requires you to log in with a user name and password. This ensures that no one can make unauthorized changes to your access point's settings. Please note that the

Password Rules:

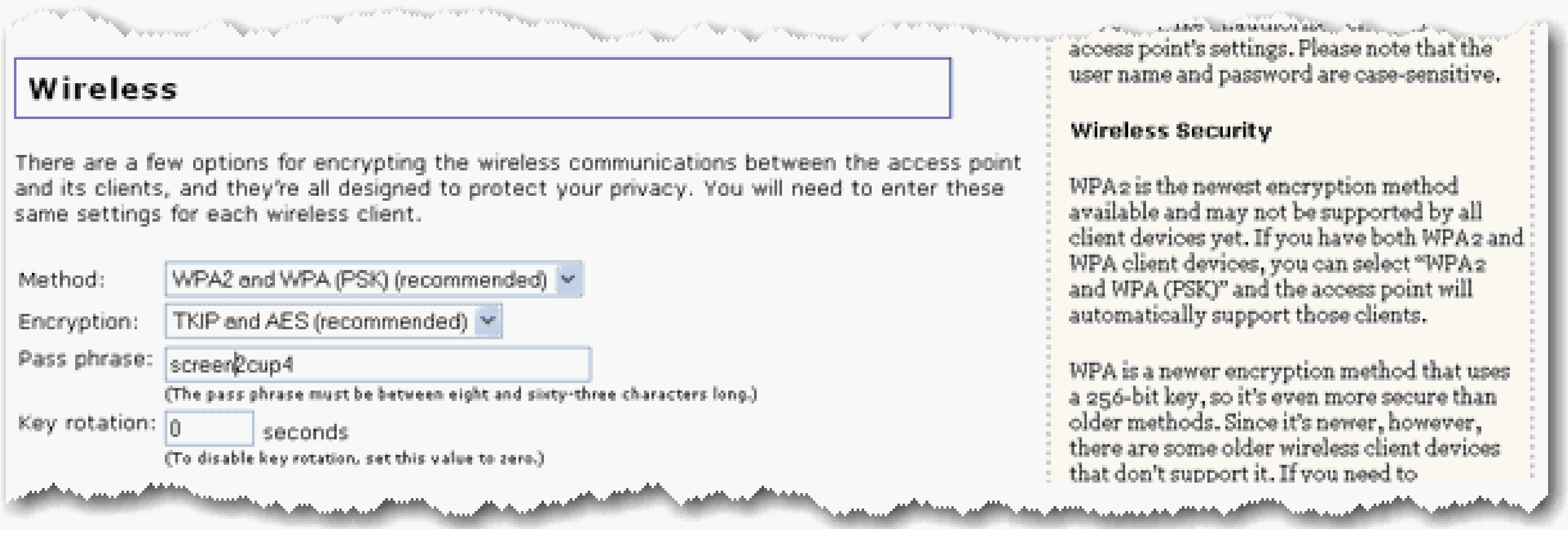
1. You can set a password up to 15 characters long. The most secure passwords are

usually between 8 and 15 characters long.

2. You can enter a space or other punctuation in your password.
3. Use a mixture of upper (**A** through **Z**) and lower (**a** through **z**) case letters.
4. Adding numbers **0** through **9** to a password increases security.
5. Use ASCII symbols, such as **~ ! @ # $ % & ^ ***, etc, to further increase the security of your password.

Wireless

In this section you can enable the wireless security features. USRobotics strongly recommends that you enable some form of wireless security so that unauthorised clients are not able to access your network.



Wireless

There are a few options for encrypting the wireless communications between the access point and its clients, and they're all designed to protect your privacy. You will need to enter these same settings for each wireless client.

Method: WPA2 and WPA (PSK) (recommended)

Encryption: TKIP and AES (recommended)

Pass phrase: screen2cup4

(The pass phrase must be between eight and sixty-three characters long.)

Key rotation: 0 seconds

(To disable key rotation, set this value to zero.)

access point's settings. Please note that the user name and password are case-sensitive.

Wireless Security

WPA2 is the newest encryption method available and may not be supported by all client devices yet. If you have both WPA2 and WPA client devices, you can select "WPA2 and WPA (PSK)" and the access point will automatically support those clients.

WPA is a newer encryption method that uses a 256-bit key, so it's even more secure than older methods. Since it's newer, however, there are some older wireless client devices that don't support it. If you need to

For your wireless security settings, it is recommended that you select the **WPA2 and WPA (PSK)** or the **WPA2 and WPA with 802.1x (RADIUS)** (if you have a RADIUS server and are in **Access Point** mode) wireless security method using **TKIP and AES** encryption for the most secure wireless network.

> **Note**: All the wireless devices you want to connect to the network must have the same wireless security settings including the pass phrase or key that you use to secure your wireless network.

Select the encryption **Method** that you want the wireless network to use. You can select from the following options:

- WPA2 and WPA (PSK) (recommended)
- WPA2 (PSK)
- WPA (PSK)
- WEP open
- WEP shared
- WPA2 and WPA with 802.1x (RADIUS)
- WPA2 with 802.1x (RADIUS)
- WPA with 802.1x (RADIUS)
- None

Depending on the wireless security method you select, there are different encryption types and pass phrase or key settings.

WPA2 and WPA (PSK) Options

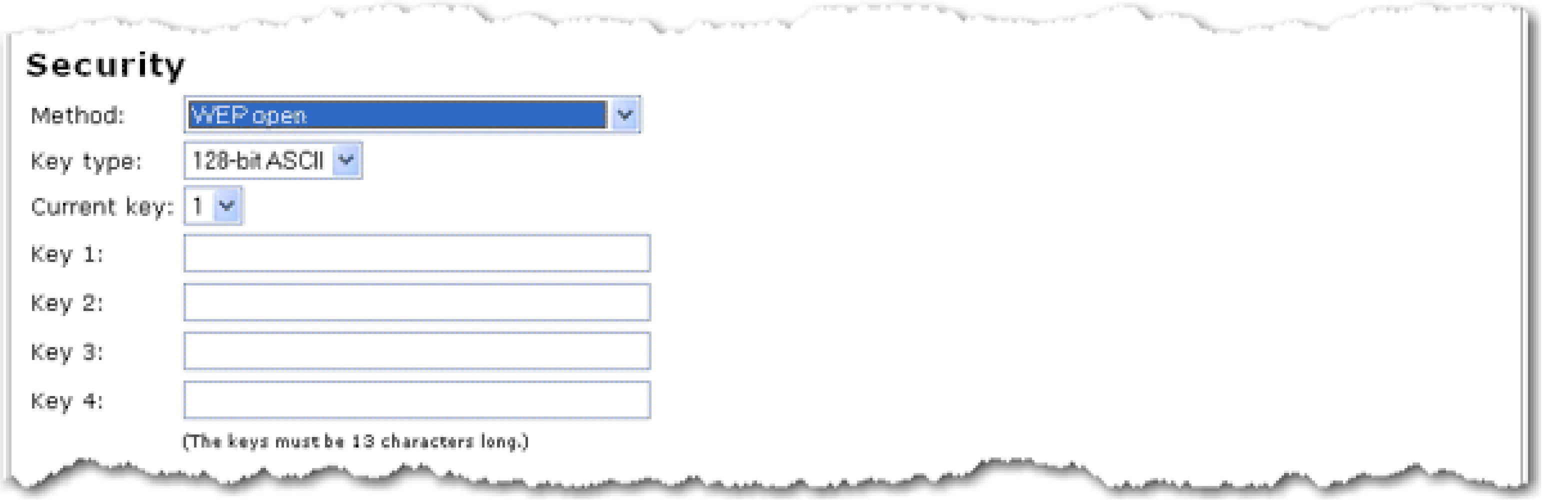
1. Select one of the following WPA2 and WPA options:
    - **WPA2 and WPA (PSK)**
    - **WPA2 (PSK)**
    - **WPA (PSK)**
2. Select your **Encryption** type: **TKIP and AES**, **AES**, or **TKIP**.

Note: Not all wireless clients support AES encryption when using WPA (PSK) security. TKIP encryption with WPA (PSK) is supported by most wireless clients. You can use **TKIP and AES** encryption to cover both AES and TKIP clients.

3. Enter a **Pass phrase** (which is also commonly called a *Network key*, *WPA key*, or *WPA Pre-shared key*). The pass phrase must be between eight and sixty-three characters long. This pass phrase must be the same on each computer that is connected to the wireless network.

4. You can also specify a **Key rotation**, in seconds, or enter **0** in the field to disable the option. Key rotation specifies how often the access point generates a new group key for broadcast and multicast packets.

WEP Options



Security

Method: WEP open

Key type: 128-bit ASCII

Current key: 1

Key 1:

Key 2:

Key 3:

Key 4:

(The keys must be 13 characters long.)

1. Select either of the following WEP options:
   - **WEP open**
   - **WEP shared**

2. Select your **Key type** as **128-bit ASCII, 128-bit hex, 64-bit ASCII** or **64-bit hex**.

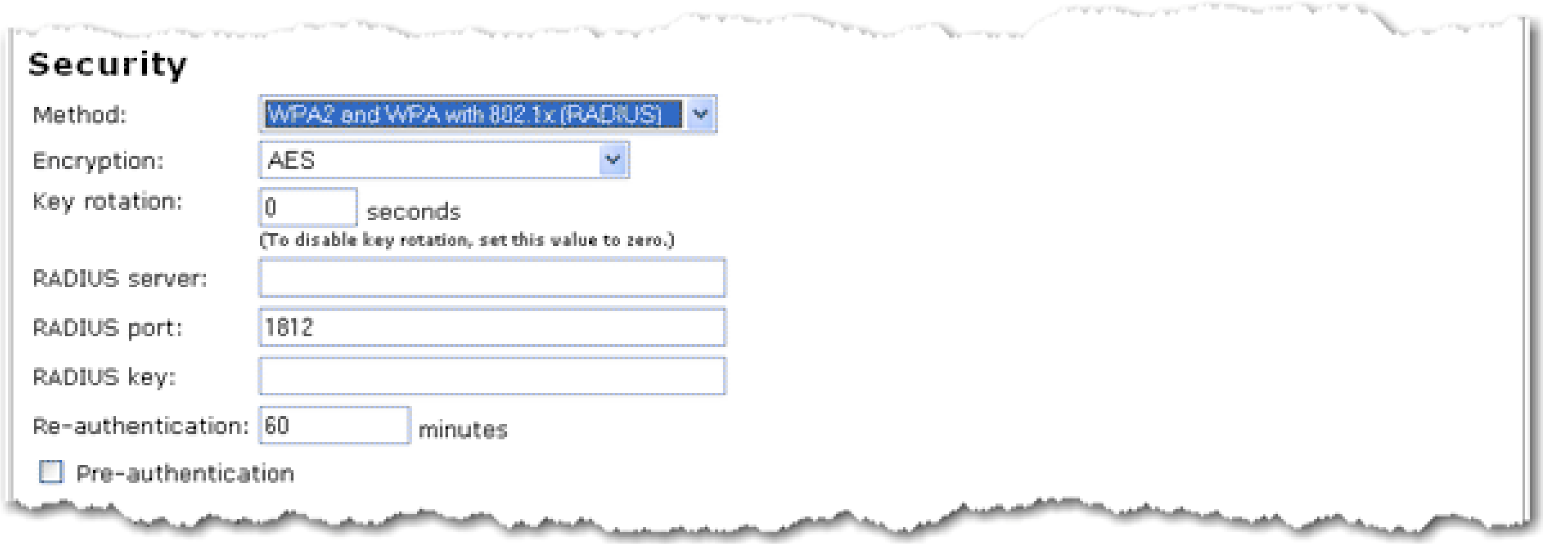
3. Enter at least one **Key** (which is also commonly called a *Network key*).

Each key must be 13 characters long for a 128-bit ASCII key type, 26 characters long for a 128-bit hex key type, and 5 characters long for a 64-bit ASCII key type or 10 characters long for a 64-bit hex key type.

If you enter multiple keys, select the **Current key** that should be used for wireless connections.

RADIUS Options

You can use the RADIUS options only if you have access to a RADIUS server.



Security

Method: WPA2 and WPA with 802.1x (RADIUS)

Encryption: AES

Key rotation: 0 seconds
(To disable key rotation, set this value to zero.)

RADIUS server:

RADIUS port: 1812

RADIUS key:

Re-authentication: 60 minutes

□ Pre-authentication

1. Select one of the following RADIUS options:
    - **WPA2 and WPA with 802.1x (RADIUS)**
    - **WPA2 with 802.1x (RADIUS)**
    - **WPA with 802.1x (RADIUS)**
2. Select your **Encryption** type: **TKIP and AES**, **AES**, or **TKIP**.

> **Note**: Not all wireless clients support AES encryption when using WPA (PSK) security. TKIP encryption with WPA (PSK) is supported by most wireless clients. You can use **TKIP and AES** encryption to cover both AES and TKIP clients.

3. Enter the **RADIUS server** IP address and **RADIUS Port** settings of your RADIUS server.

4. >Enter the **RADIUS key** of your RADIUS server.

5. Enter the **Re-authentication** time, in minutes.>

6. If required for your connection to the RADIUS server, select **Pre-authentication**. This option is not available with **WPA with 802.1x (RADIUS).**

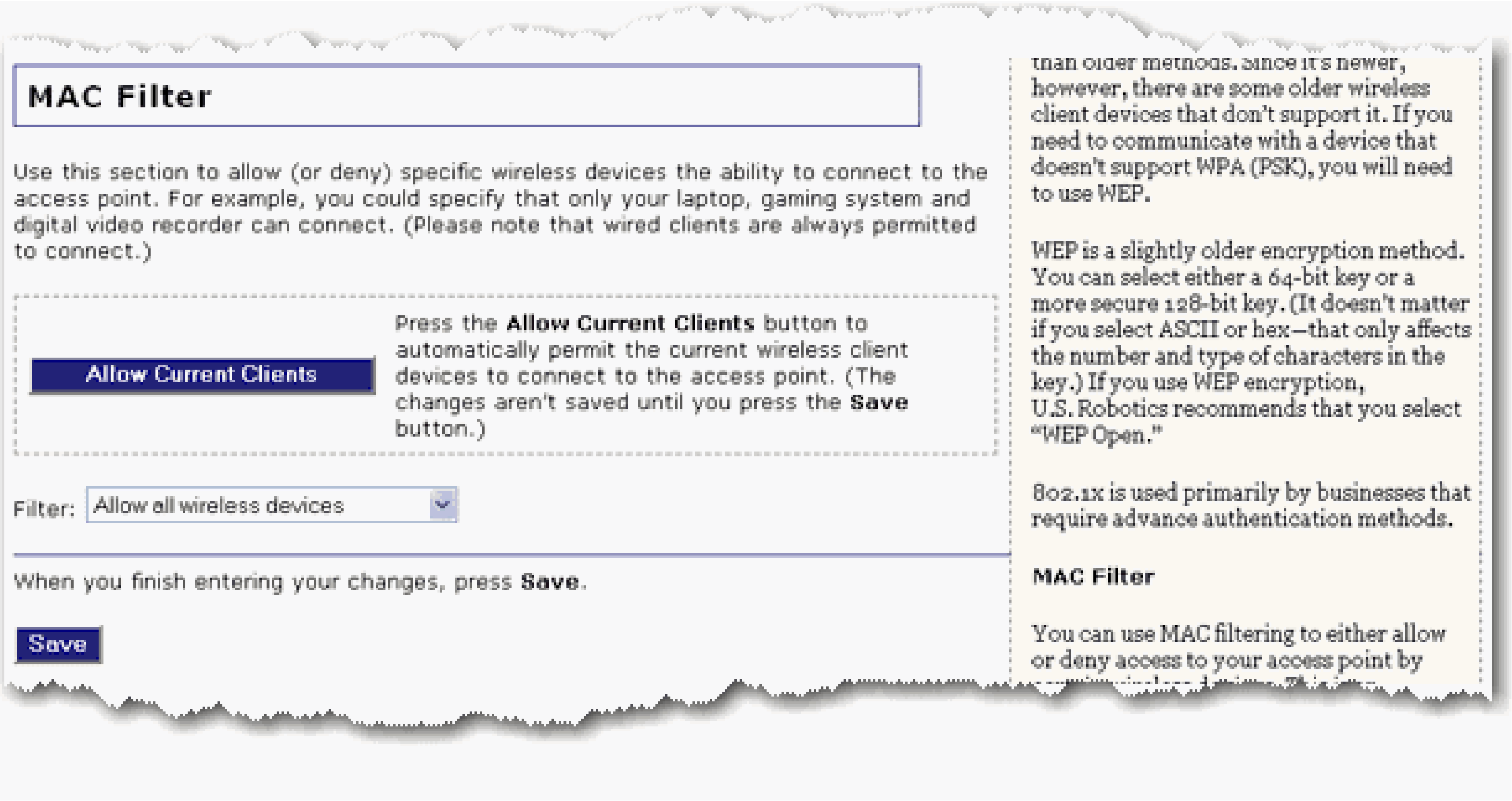
None

None disables all wireless security on your access point.

> **Note:** The setting of **None** is not recommended since without any encryption enabled, your network will be vulnerable to outside malicious attacks.

MAC Filter

In this area you can control which wireless devices are allowed or denied access to the access point based upon their MAC addresses. The MAC address can usually be found either on a label on the external wireless product or in the configuration utility of the wireless client, depending on the wireless device you are using.



MAC Filter

Use this section to allow (or deny) specific wireless devices the ability to connect to the access point. For example, you could specify that only your laptop, gaming system and digital video recorder can connect. (Please note that wired clients are always permitted to connect.)

Press the **Allow Current Clients** button to automatically permit the current wireless client devices to connect to the access point. (The changes aren't saved until you press the **Save** button.)

Filter: Allow all wireless devices

When you finish entering your changes, press **Save**.

than older methods. Since it's newer, however, there are some older wireless client devices that don't support it. If you need to communicate with a device that doesn't support WPA (PSK), you will need to use WEP.

WEP is a slightly older encryption method. You can select either a 64-bit key or a more secure 128-bit key. (It doesn't matter if you select ASCII or hex—that only affects the number and type of characters in the key.) If you use WEP encryption, U.S. Robotics recommends that you select "WEP Open."

802.1x is used primarily by businesses that require advance authentication methods.

MAC Filter

You can use MAC filtering to either allow or deny access to your access point by

You can click **Allow Current Clients** button to grant access to all wireless clients that are currently connected to the access point, or you can apply one of the following filters to determine which clients are allowed access:

- **Allow all wireless devices**: Any wireless client that has the correct security information will be allowed to connect to the access point. This is the default setting.
- **Allow only these devices:** Allows only devices with specific MAC addresses to establish a wireless connection with the access point.

    1. Enter the MAC address of the device that should be allowed connection to the access point.

    2. Click **Add**.

- **Deny only these devices**: Denies a wireless connection to the access point for devices with the specified MAC addresses. This can be used if you notice unauthorised wireless devices that are connected to your network.

    1. Enter the MAC address of the device that should be denied connection to the access point.

    2. Click **Add.**

Note: Click **Save** to apply all your new settings and reboot the access point after you have completed all your changes.

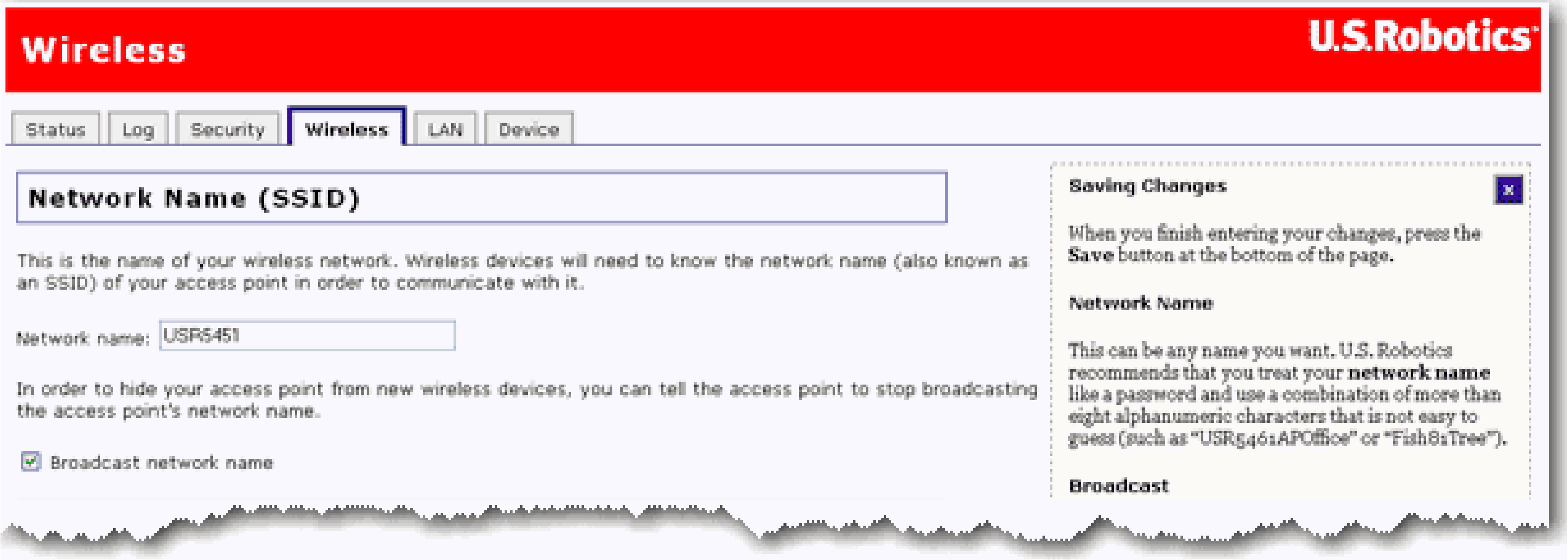
USRobotics ***Wireless MAXg Access Point: User Guide***

Wireless Settings

In this section you can change the wireless network settings of the access point.

Network Name (SSID)

Wireless clients use the **Network name** (SSID) to connect to your access point.



Network Name (SSID)

This is the name of your wireless network. Wireless devices will need to know the network name (also known as an SSID) of your access point in order to communicate with it.

Network name: USR5451

In order to hide your access point from new wireless devices, you can tell the access point to stop broadcasting the access point's network name.

☑ Broadcast network name

Saving Changes

When you finish entering your changes, press the **Save** button at the bottom of the page.

Network Name

This can be any name you want. U.S. Robotics recommends that you treat your **network name** like a password and use a combination of more than eight alphanumeric characters that is not easy to guess (such as "USR5461APOffice" or "Fish81Tree").

Broadcast

The default **Network name** of the access point is USR5455. If you have more than one Wireless ***MAXg*** Access Point and want to use each independently, you must configure a unique Network name for each access point.

Select **Broadcast network name** if you want wireless devices to be able to detect your access point when they perform a site scan.

If you deselect **Broadcast network name**, wireless devices will not be able to detect your wireless network during a site scan. Devices will have to manually enter the Network Name (SSID) of your access point to connect.

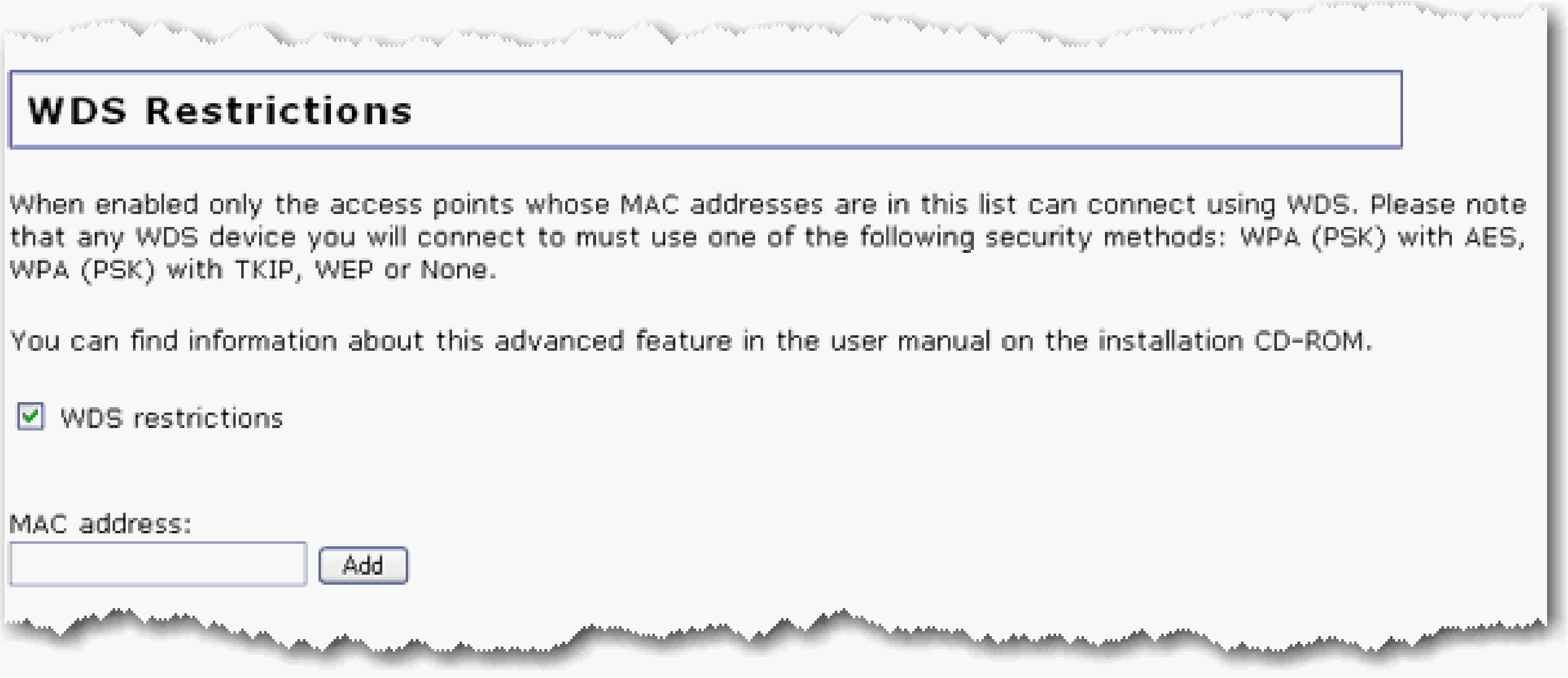
WDS Restrictions

WDS lets access points and wireless routers communicate with one another wirelessly, effectively creating a bridge between multiple networks. By connecting an access point or wireless router to each network and enabling the WDS feature, you enable wireless clients to roam throughout the range of both networks.

The access point and the other wireless networking device must have the same channel, network name (SSID), and wireless security settings. Each device must have the MAC address of the other device in its WDS Restrictions table.

With this type of wireless network, throughput may be reduced across the bridge. Therefore, bridged routers or access points that also allow wireless clients to connect to the network should not be used for high-volume traffic. Examples in which bridging may be useful include providing network access to parts of a building that cannot be connected using wires, or providing short-term network access to a conference area.

You can set restrictions for devices that connect through WDS (Wireless Distribution System). These restrictions apply only to devices that connect through WDS, not to all wireless devices that connect to the access point.



WDS Restrictions

When enabled only the access points whose MAC addresses are in this list can connect using WDS. Please note that any WDS device you will connect to must use one of the following security methods: WPA (PSK) with AES, WPA (PSK) with TKIP, WEP or None.

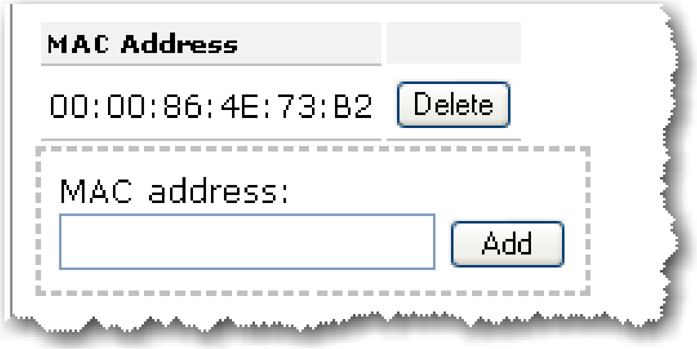
You can find information about this advanced feature in the user manual on the installation CD-ROM.

☑ WDS restrictions

MAC address:

If you select **WDS restrictions**, you must enter the MAC addresses of the wireless routers or access points that will connect to this access point and click the **Add** button.

To delete an existing WDS mapping, click the **Delete** button next to the MAC Address:



The access point's WDS connections do not support **WPA2 (PSK)**, any of the **RADIUS** security methods, and **TKIP and AES** encryption.

If your access point is set with one of the following security methods and encryption types, all WDS connections to the access point should use **WPA-PSK (TKIP)**:

- **WPA2 (PSK)** with **TKIP and AES**
- **WPA2 (PSK)** with **TKIP**
- **WPA (PSK)** with **TKIP and AES**
- **WPA (PSK)** with **TKIP**

If your access point is set with one of the following security methods and encryption types, all WDS connections to the access point should use **WPA (PSK)** with **AES**:

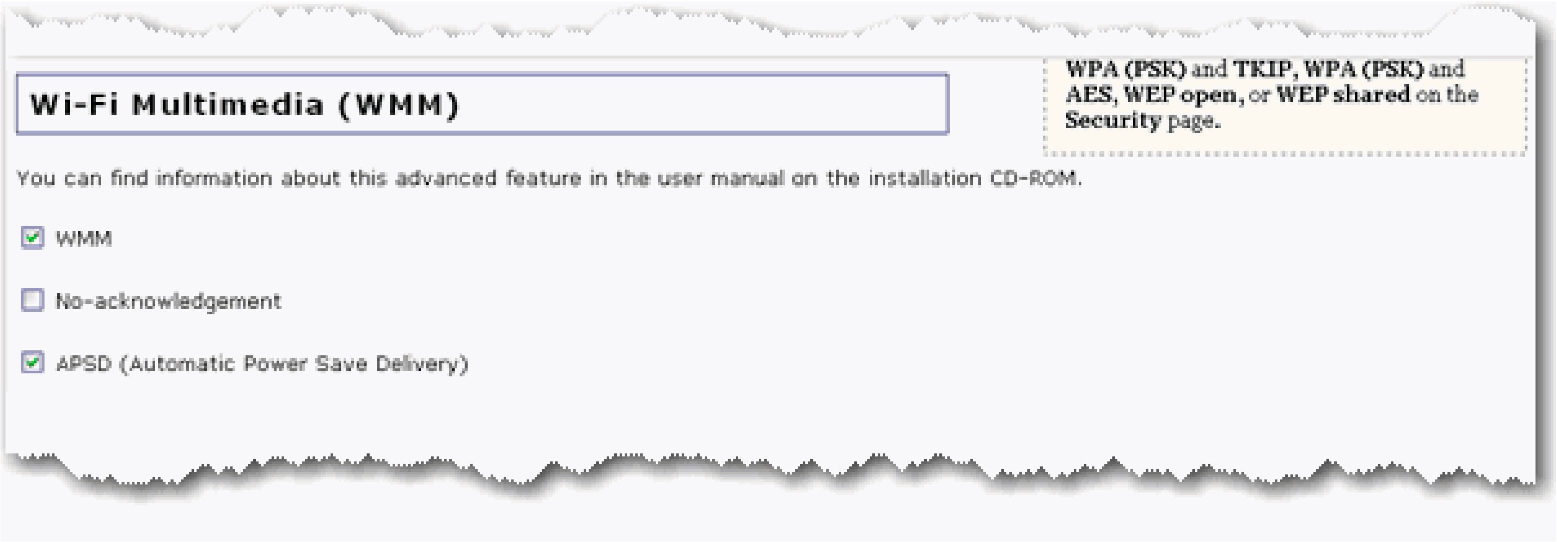
- **WPA2 (PSK)** with **AES**
- **WPA (PSK)** with **AES**

In both of these cases, the **Pass phrase** (which is also commonly called a *Network key*, *key*, or *Personal shared key*) you entered for the wireless security on your access point will be also used as the Personal Shared Key (PSK) for WDS connections. However, all wireless clients connecting to the access point should continue to use the same security method and encryption type that you configured on your access point.

Wi-Fi Multimedia (WMM)

This feature is disabled by default. If you want to enable this feature, select the checkbox next to **WMM** (Wi-Fi Multimedia). The other devices that you are connecting to in order to use this feature must also support WMM and have it enabled.

This feature enables the Quality of Service (QoS) function that is used for multimedia applications, such as Voice-over-IP (VoIP) and video. This allows the network packets of the multimedia application to have priority over regular data network packets, allowing multimedia applications to run smoother and with fewer errors.



WPA (PSK) and TKIP, WPA (PSK) and AES, WEP open, or WEP shared on the Security page.

Wi-Fi Multimedia (WMM)

You can find information about this advanced feature in the user manual on the installation CD-ROM.

☑ WMM

□ No-acknowledgement

☑ APSD (Automatic Power Save Delivery)

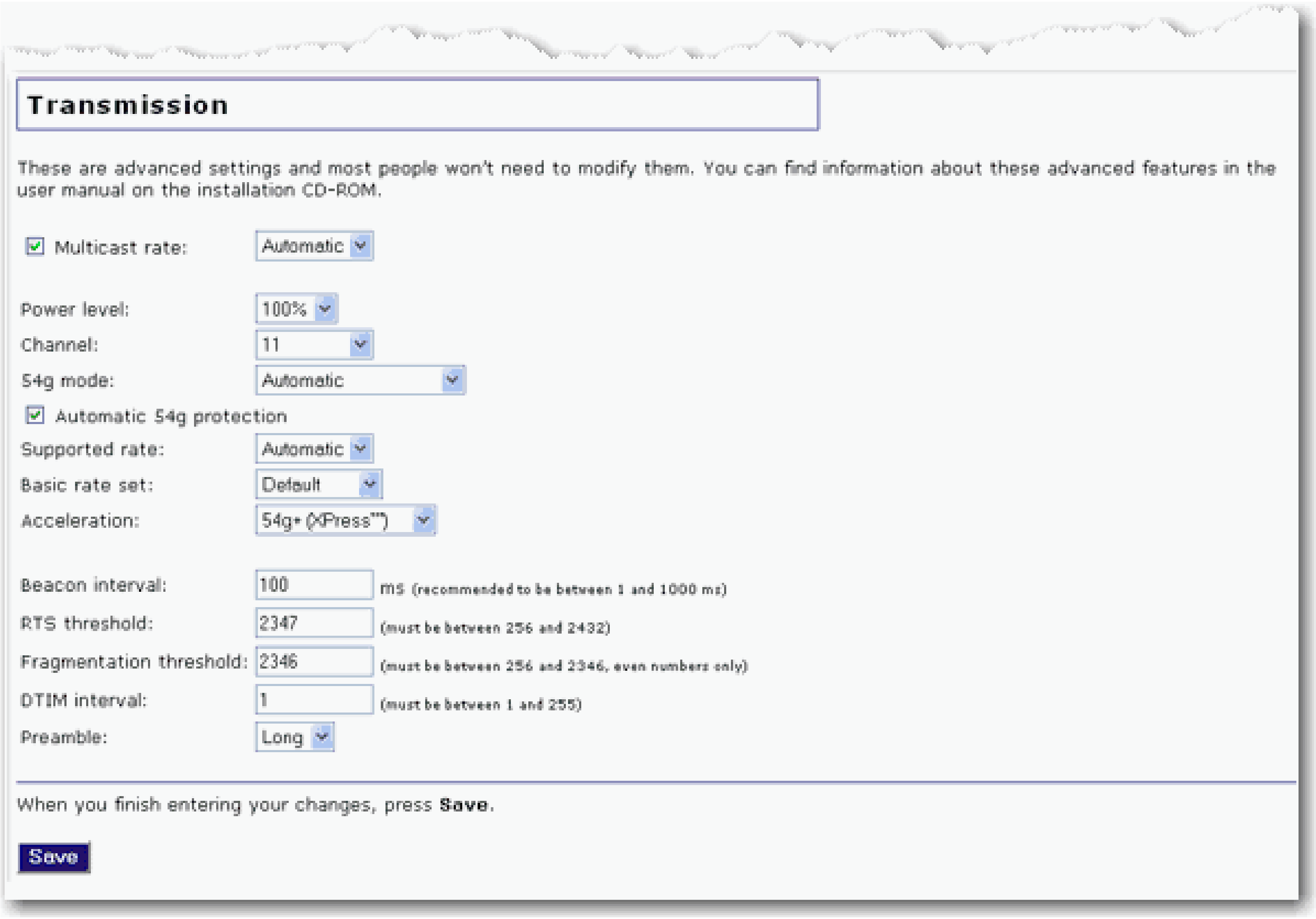
If you enable WMM, you can then select **No-acknowledgement**. No-Acknowledgement refers to the acknowledge policy used at the MAC level. Enabling no-acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.

With WMM enabled, you can also select **Enable APSD (Automatic Power Save Delivery)**. APSD manages radio usage for battery-powered devices to allow longer battery life in certain conditions. APSD allows a longer beacon interval until an application requiring a short packet exchange interval starts. Voice Over Internet Protocol (VoIP) is an example of application requiring a short packet exchange interval. APSD affects radio usage and battery life only if the wireless client also supports APSD.

Note: The **Acceleration** option **MAXg (125 Mbps)** is incompatible with WMM. To enable WMM, you must set the **Acceleration** option to **54g+ (Xpress™)**.

Transmission

The fields in this area are for more advanced wireless features that most people do not need to change. If you do want to change any of these settings, write down the default settings before you make any changes in case you experience any problems and need to change these settings back.



Transmission

These are advanced settings and most people won't need to modify them. You can find information about these advanced features in the user manual on the installation CD-ROM.

☑ Multicast rate: Automatic

Power level: 100%

Channel: 11

54g mode: Automatic

☑ Automatic 54g protection

Supported rate: Automatic

Basic rate set: Default

Acceleration: 54g+ (XPress™)

Beacon interval: 100 ms (recommended to be between 1 and 1000 ms)

RTS threshold: 2347 (must be between 256 and 2432)

Fragmentation threshold: 2346 (must be between 256 and 2346, even numbers only)

DTIM interval: 1 (must be between 1 and 255)

Preamble: Long

When you finish entering your changes, press **Save**.

- **Multicast rate**: Specify the rate at which multicast packets are transmitted and received on your wireless network. Multicast packets are used to send a single message to a set of recipients in a defined group. Teleconferencing, videoconferencing and group email are some examples of multicast applications. Specifying a high multicast rate may improve performance of multicast features. The rates are in Mbps. You can select **Automatic**, **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, **54**.

  To prevent the access point from transmitting multicast packets, clear the checkbox.

- **Power level**: Select 100%, 50%, or 25% from the drop-down menu. The Power level sets the strength of the wireless signal that the access point transmits. You would want a lower setting if you live in an area where your wireless signal could be overlapping with other wireless networks and want to reduce the interference you encounter.
- **Channel**: Sets the channel on which the access point is to operate. If you are

experiencing interference or wireless network problems, changing the channel may solve the problem.

- **54g mode**: Select **Automatic, 802.11g Performance,** or **802.11b Only**. If you are using all 802.11g equipment, **802.11g Performance** will provide the fastest performance. If you select **802.11b Only**, all clients that are capable of 802.11b will connect to the Wireless ***MAX*g** Access Point at 802.11b data rates.
- **Automatic 54g protection**: If you select this option, the access point will use Request to Send/Clear to Send (RTS/CTS) to improve the performance in 802.11 mixed environments. If this is not selected, the 802.11n performance will be maximized under most conditions while the other 802.11 modes (802.11b, etc.) will be secondary.
- **Supported rate:** Select the wireless link rate at which you want information transmitted and received on your wireless network. You can select **Auto**, **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, **54**.
- **Basic rate set**: Select the basic rate that wireless clients must support: **Default**, **All**, or **1 & 2 Mbps**.
- **Acceleration**: Select **None**, **54g+ (Xpress™)**, or **MAXg (125 Mbps)**. These features determine either normal speed rates or accelerated rates. Set the mode to **54g+ (Xpress™)** for the widest compatibility. The Wi-Fi Multimedia (WMM) feature is not available if you select MAXg (125 Mbps). 125 Mbps can only be achieved if all wireless clients are *MAX*g wireless clients and your wireless environment does not have interference from other radio devices.
- **Beacon Interval:** The amount of time between beacon transmissions. A beacon is basically a heartbeat for a wireless client or access point, sending out a signal informing the network that it is still active. This should be set between 1 and 1000 milliseconds. The default beacon interval is 100 ms.
- **RTS threshold**: The minimum size in bytes for which the Request to Send/Clear to Send (RTS/CTS) channel contention mechanism is used. In a network with significant radio interference or large number of wireless devices on the same channel, reducing the RTS Threshold might help in reducing frame loss. The RTS threshold is 2347 bytes by default, which is the maximum value.
- **Fragmentation threshold**: The maximum level that the access point will reach when sending information in packets before the packets are broken into fragments. Typically, if you are experiencing problems sending information, it is because there is other traffic on the network and the data being transmitted is colliding. This might be corrected by the information being broken into fragments. The lower the fragmentation threshold value, the smaller a packet has to be before it is broken into fragments. If the maximum is set (2346), fragmentation is essentially disabled. You should only change this level if you are an advanced user.
- **DTIM Interval**: The amount of time after which buffered broadcast and multicast frames will be delivered to the wireless clients. This allows mobile stations to conserve power. If you are using applications that use broadcast or multicast frames for delivering data, you should use a Delivery Traffic Indication Message (DTIM) Interval of 1 to minimize delay for real-time traffic, such as multicast audio and video streams.
- **Preamble**: Defines the length of the Cyclic Redundancy Check (CRC) block for communication between the access point and wireless clients. The preamble consists of the Synchronization and Start Frame Delimiter (SFD) fields. The sync field is used to indicate the delivery of a frame to wireless stations, to measure frequency of the

radio signal, to perform corrections if needed. The SFD at the end of the Preamble is used to mark the start of the frame.

If you are not using any 802.11b devices in your network, you can configure the Preamble type to **Short** for optimum performance. The **Long** Preamble type should be used when both 802.11g and 802.11b devices exist on your network.

Note: Click **Save** to apply all your new settings and reboot the access point after you have completed all your changes.

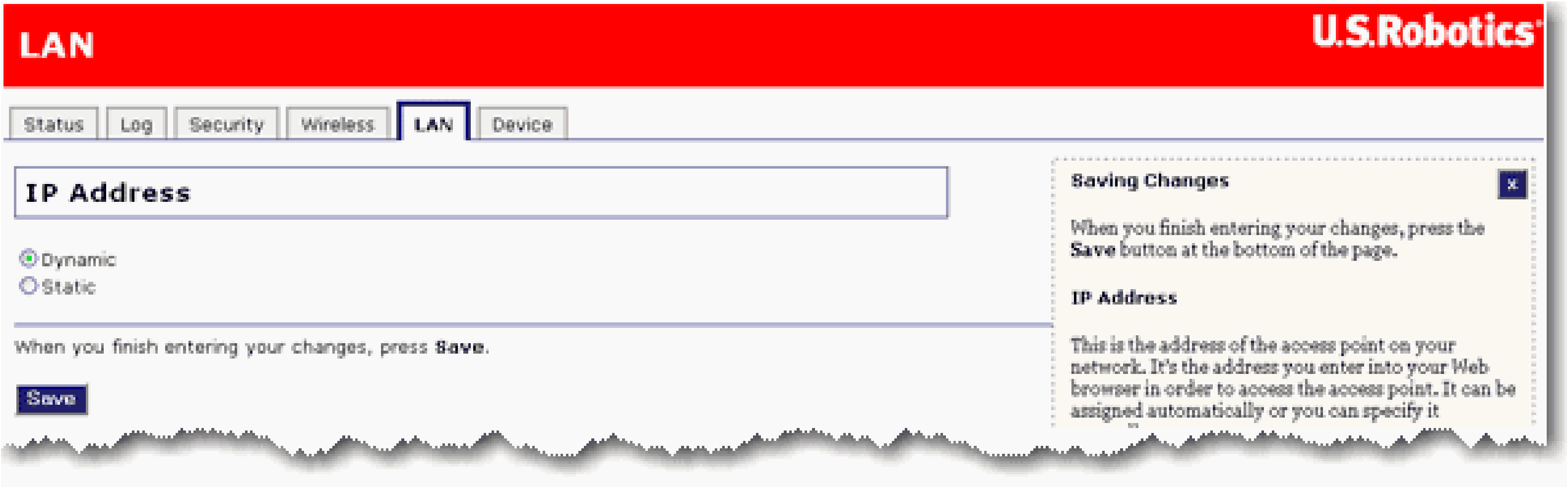
USRobotics *Wireless MAXg Access Point: User Guide*

Local Area Network (LAN) Settings

From the **LAN** page, you can view and modify the Local Area Network (LAN) settings of the access point. These settings apply only to your local network.

IP Address

You can set the IP address as **Dynamic** or **Static**.



IP Address

● Dynamic
○ Static

When you finish entering your changes, press **Save**.

Saving Changes

When you finish entering your changes, press the **Save** button at the bottom of the page.

IP Address

This is the address of the access point on your network. It's the address you enter into your Web browser in order to access the access point. It can be assigned automatically or you can specify it

- **Dynamic**: Select this option if your access point will obtain an IP address from a DHCP server on the network and click **Save** at the bottom of the page.
- **Static**: Select this option if the access point is to have a specific IP address. Enter your **IP address**, **Gateway**, **DNS server**, and **Subnet mask** and click **Save** at the bottom of the page.

When you change the IP address of your access point, you may need to reboot your wireless clients after the access point reboots with its new IP address.

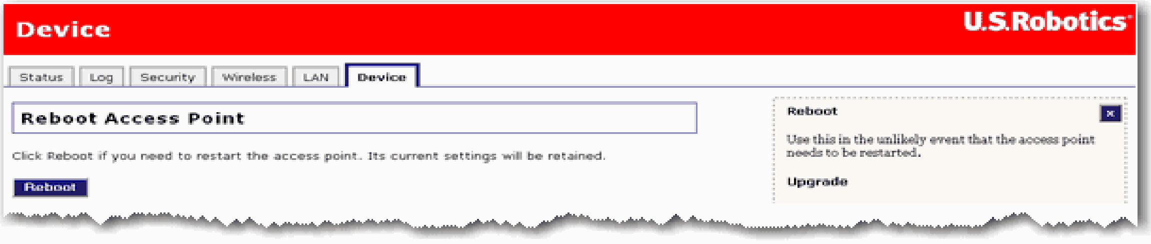
USRobotics *Wireless MAXg Access Point:*

User Guide

Device Settings

In the access point configuration pages, the **Device** page lets you access some of the basic settings of the access point and perform administrative functions.

Reboot Access Point



Device

U.S.Robotics

Reboot Access Point

Click Reboot if you need to restart the access point. Its current settings will be retained.

Reboot

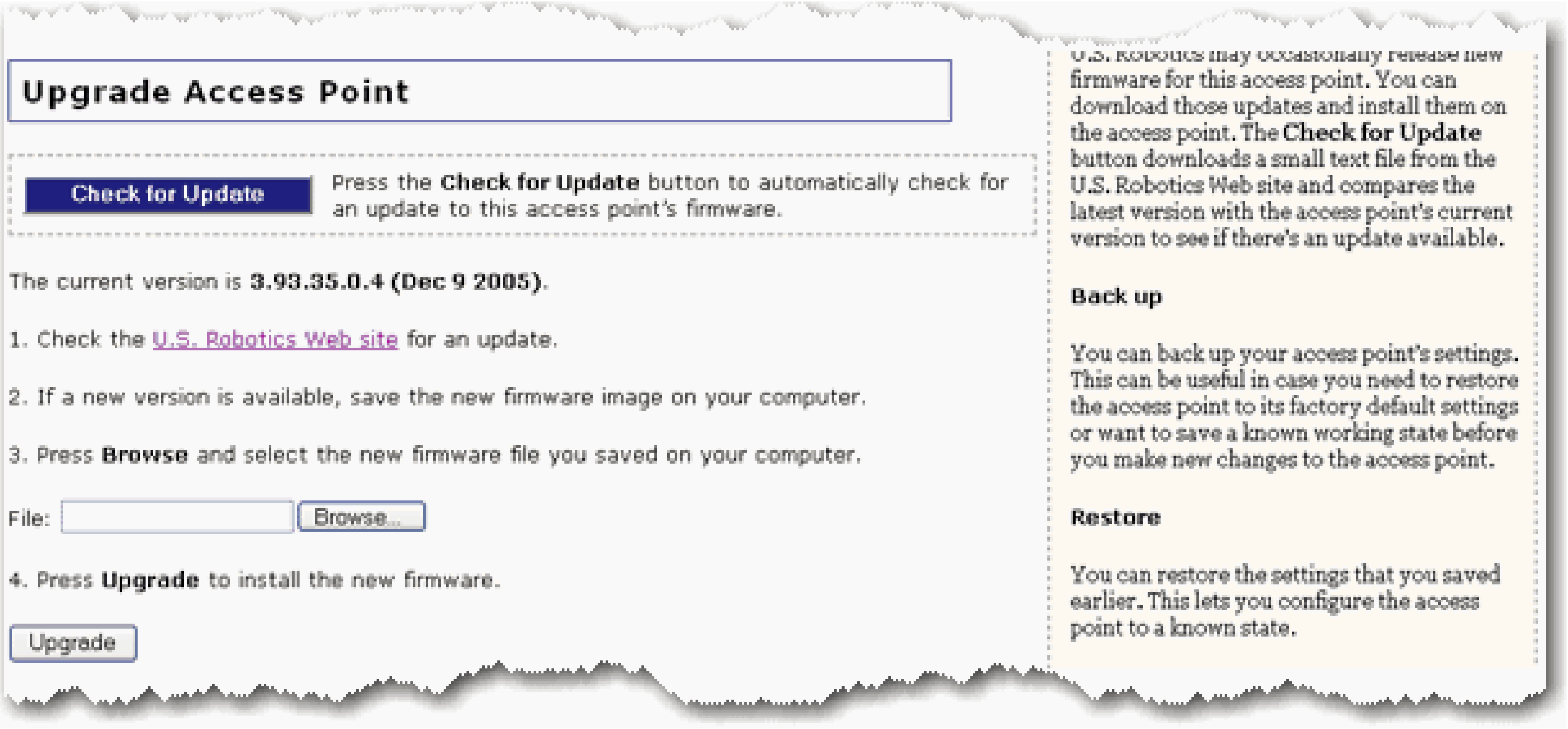
Use this in the unlikely event that the access point needs to be restarted.

Upgrade

If the access point is not functioning properly, you can click **Reboot** to restart the access point.

Upgrade Access Point

Firmware updates may be available on the USRobotics website to upgrade your device with new or improved features. If you are experiencing problems with your device, you may want to check for firmware updates.



Upgrade Access Point

Check for Update Press the **Check for Update** button to automatically check for an update to this access point's firmware.

The current version is **3.93.35.0.4 (Dec 9 2005)**.

1. Check the U.S. Robotics Web site for an update.
2. If a new version is available, save the new firmware image on your computer.
3. Press **Browse** and select the new firmware file you saved on your computer.

File: Browse...

4. Press **Upgrade** to install the new firmware.

Upgrade

U.S. Robotics may occasionally release new firmware for this access point. You can download those updates and install them on the access point. The **Check for Update** button downloads a small text file from the U.S. Robotics Web site and compares the latest version with the access point's current version to see if there's an update available.

Back up

You can back up your access point's settings. This can be useful in case you need to restore the access point to its factory default settings or want to save a known working state before you make new changes to the access point.

Restore

You can restore the settings that you saved earlier. This lets you configure the access point to a known state.

1. Click **Check for Update** to search for the latest firmware from www.usr.com and save the firmware file to your computer.

2. Click **Browse** to locate and select the new firmware file.

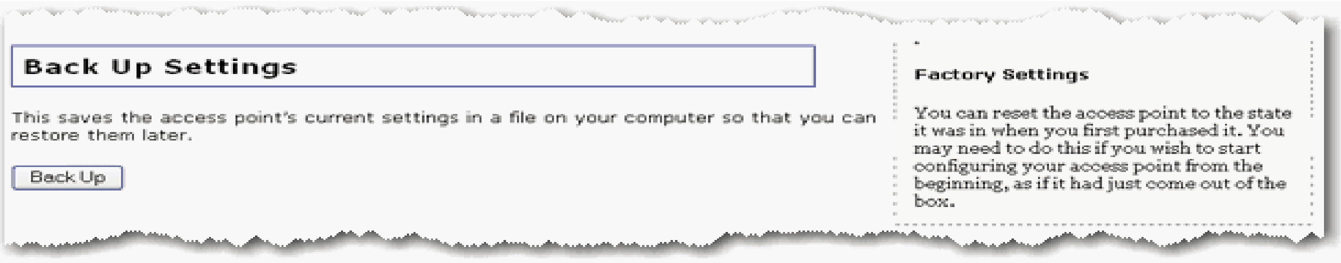
3. Click **Upgrade** to begin the update process.

   The access point may disconnect and reconnect to the Internet during the update. When complete, you will be prompted to log back in to the access point.

   You should then see the new version of firmware listed on the Status page. If you do not, repeat the upgrade procedure.

Back Up Settings

At any time, you can use Back Up Settings to save a backup file of your current access point configuration, such as before you make significant changes to your access point configuration, or after you have successfully applied changes.



Back Up Settings

This saves the access point's current settings in a file on your computer so that you can restore them later.

Factory Settings

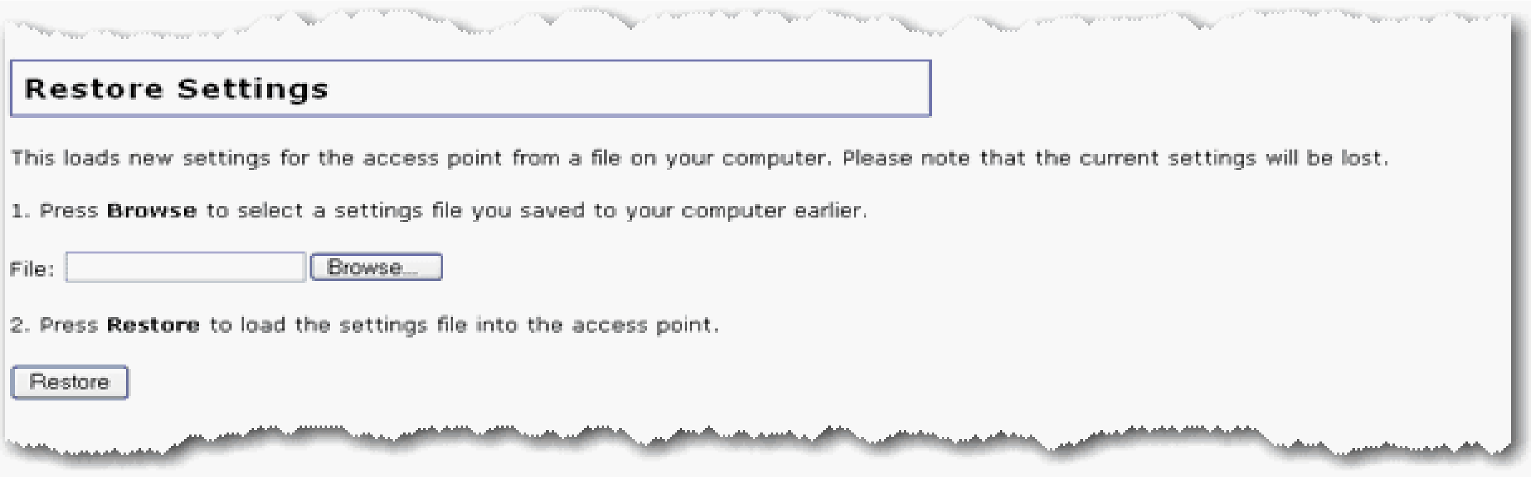
You can reset the access point to the state it was in when you first purchased it. You may need to do this if you wish to start configuring your access point from the beginning, as if it had just come out of the box.

To save your settings:

1. Select **Back Up**.
2. A window appears. Click **Save.**
3. Browse to the location at which you want the backup file saved and click **Save.**

Restore Settings

If you ever lose your settings or if your settings have changed and the access point is not functioning properly, you can restore your saved settings from a backup file. If you did not create a backup file, you may need to restore the default settings.



Restore Settings

This loads new settings for the access point from a file on your computer. Please note that the current settings will be lost.

1. Press **Browse** to select a settings file you saved to your computer earlier.

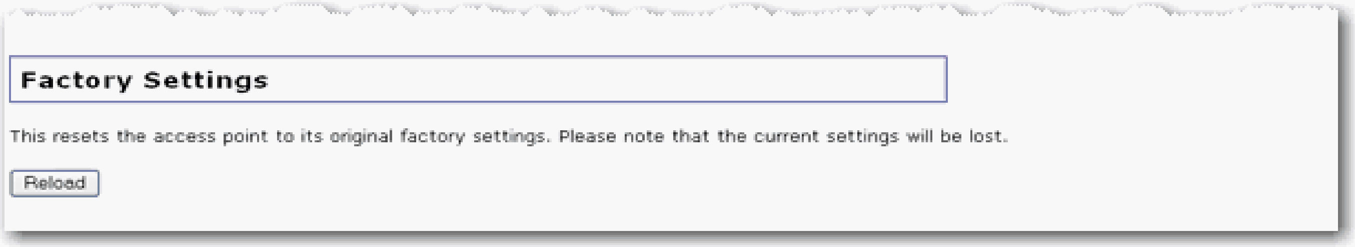
File:

2. Press **Restore** to load the settings file into the access point.

1. Browse to the location where your backup file is saved and click **Open.**
2. In the access point configuration page, click **Restore**.

Factory Settings

Click **Reload** to restore the factory default settings of your access point. When you restore the factory default, all your current settings will be lost. If you have forgotten the password to your access point, you will need to restore to the factory default using the **Reset** button on the access point, and then reinstall your access point.



Factory Settings

This resets the access point to its original factory settings. Please note that the current settings will be lost.

You can also restore the factory default settings using the **Reset** button on the access point. Press in and hold the **Reset** button on the access point for 7 seconds.

Basic Troubleshooting Procedure

This basic procedure addresses a number of symptoms that you might experience with your access point:

1. Verify that the power cord and the Ethernet cable are connected securely at both ends.
2. Ensure that the power outlet to which the access point is connected is a live outlet.
3. Make sure that the access point is receiving power and that following LEDs are on: ⏻ 📡 🖧 (power, WLAN, and LAN).
4. For connectivity issues, try rebooting the access point by disconnecting and then reconnecting its power supply.
5. For wireless connections:
   - Low link quality or range can be caused by environmental interference, such as lead-based paint and concrete walls, or some electronic items, such as 2.4GHz phones. Try moving the antennas of the access point or repositioning the wireless client to improve the link quality.
   - Verify that the device is set to infrastructure mode.
   - Verify that the following settings on the connected device match those of the access point.
     - Network name or SSID

- Security type and key, psk, or passphrase.

Refer to your device's documentation to determine how to change these settings.

If you still have trouble using the access point, follow the procedure below that best describes your symptom.

Installation and Configuration

The networking device I am using does not have a DHCP server.

The access point is connected to a live power source, but the power LED is off.

The installation procedure did not start when I inserted the USRobotics Installation CD-ROM.

The detection utility does not find the Wireless ***MAXg*** Access Point.

I cannot access the configuration pages.

After I performed a firmware upgrade, the access point did not display its status page.

Wireless Connections

The Wireless ***MAXg*** Access Point does not appear when I scan for it with a wireless client.

My client is not communicating with the Wireless ***MAXg*** Access Point.

I am no longer able to access the Internet.

My client does not establish a wireless connection to the Wireless ***MAXg*** Access Point after I changed the settings.

My wireless unicast connection is very slow while another client is using the access point for a multicast stream, such as videoconferencing or Internet radio.

Troubleshooting ping procedure

The networking device I am using does not have a DHCP server.

The Wireless ***MAX*g** Access Point can be connected to a networking device that does not have a DHCP server. By default, the access point is configured to obtain an IP address from a DHCP server, but you can manually set the IP address of the access point from the configuration pages.

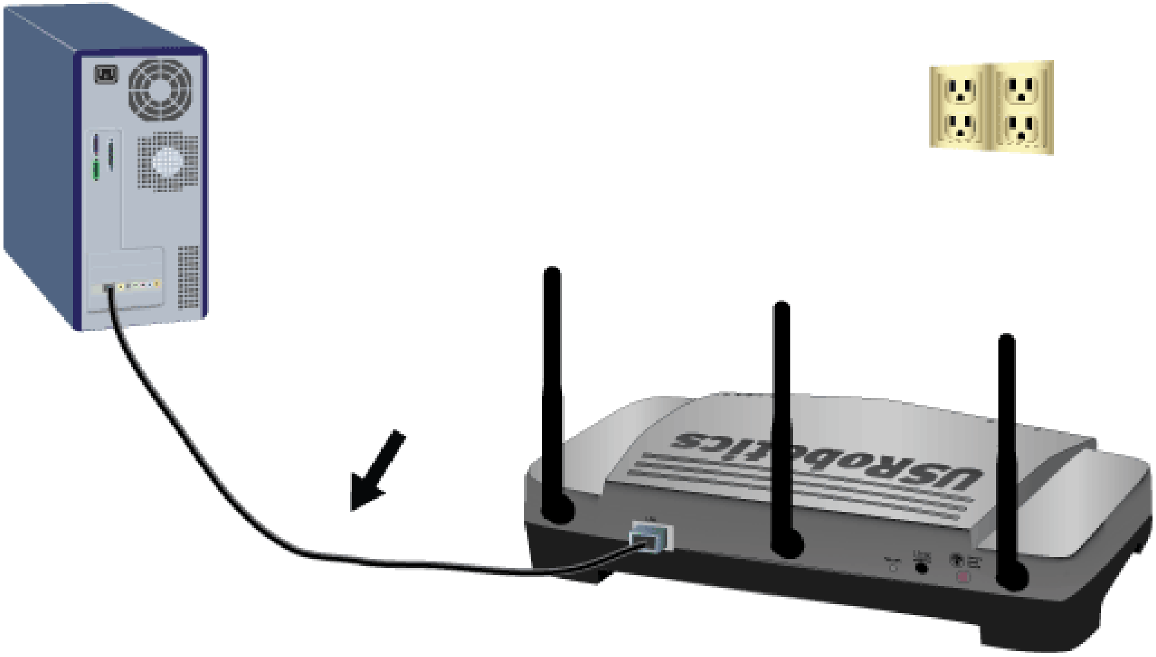
If you have not set up the access point or it is in its factory default state, see I have not installed my access point.

If you have your access point already installed and connected to a networking device but need to connect it to a different device that does not have a DHCP server, see I have installed my access point but need to connect it to a different networking device.

I have not installed my access point.

If your networking device does not have DHCP and cannot assign an IP address to the access point, you can install the access point using a static IP address by connecting the access point directly to a computer.

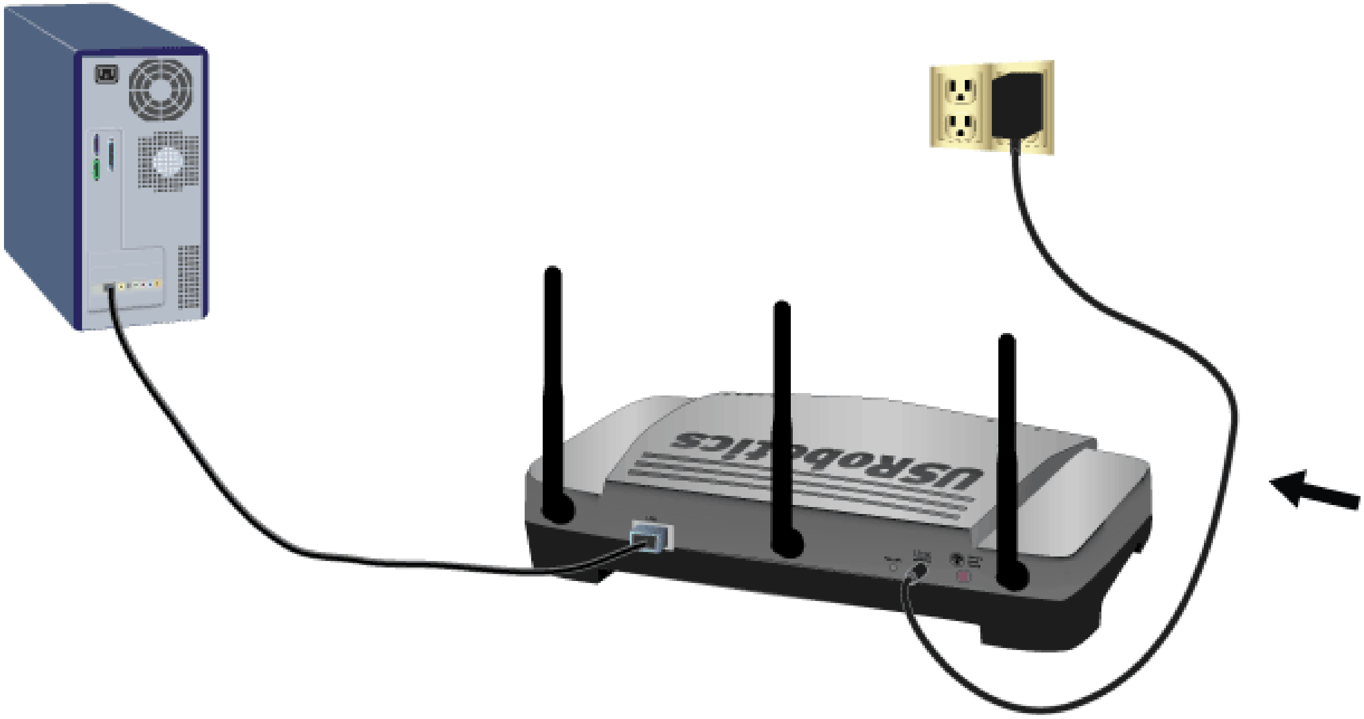
1. Connect the provided antennas to the back of the access point.
2. Use the supplied Ethernet cable to connect the LAN port on the access point to a LAN port on your computer.



3. Supply power to the access point as follows:

> **Note to UK Users**: With the power adapter unplugged, connect the appropriate power plug for your country on to the power adapter. Apply enough pressure to cause a click and firmly seat the plug.

A. Connect the supplied power adapter to the **15VDC** port on the access point.



B. Plug the power adapter into a standard power outlet.

Note: This product is intended to be supplied by a Listed Direct Plug-in Power Unit marked Class 2 and rated 15VDC, 1200 mA.

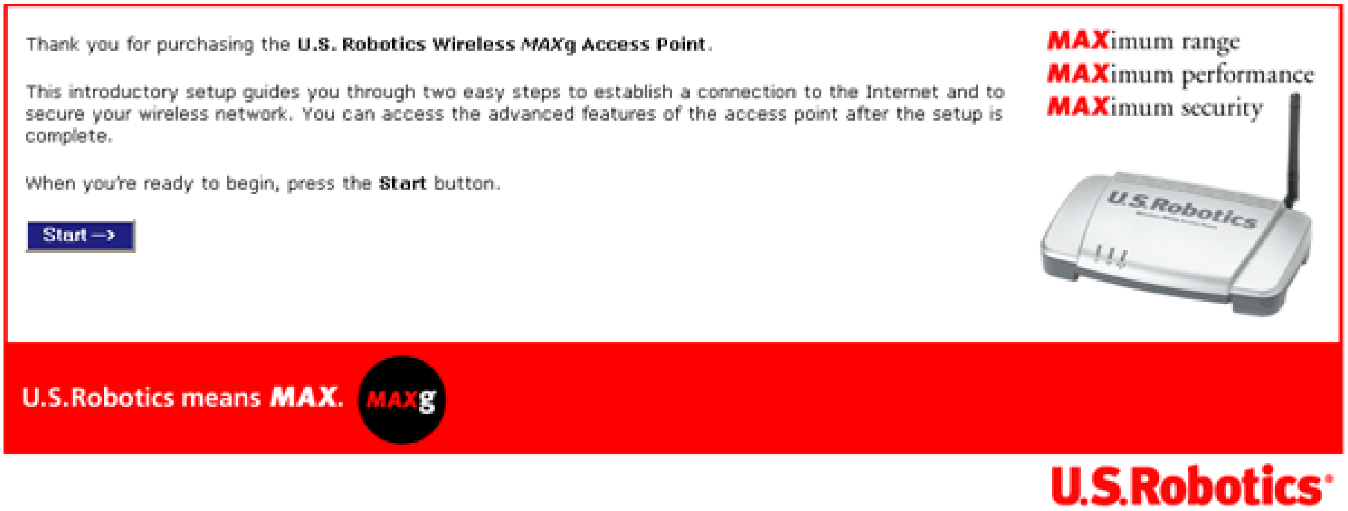
4. Power up your computer.

5. Assign a static IP address within the **192.168.1.*x*** range (example: 192.168.1.100) to your computer. For information on assigning a static IP address to your computer, see the documentation for your operating system.

6. Start your Web browser.

7. In the location or address line, type **http://192.168.1.64** and press ENTER.

8. The wizard displays its welcome page:



Thank you for purchasing the **U.S. Robotics Wireless *MAXg* Access Point**.

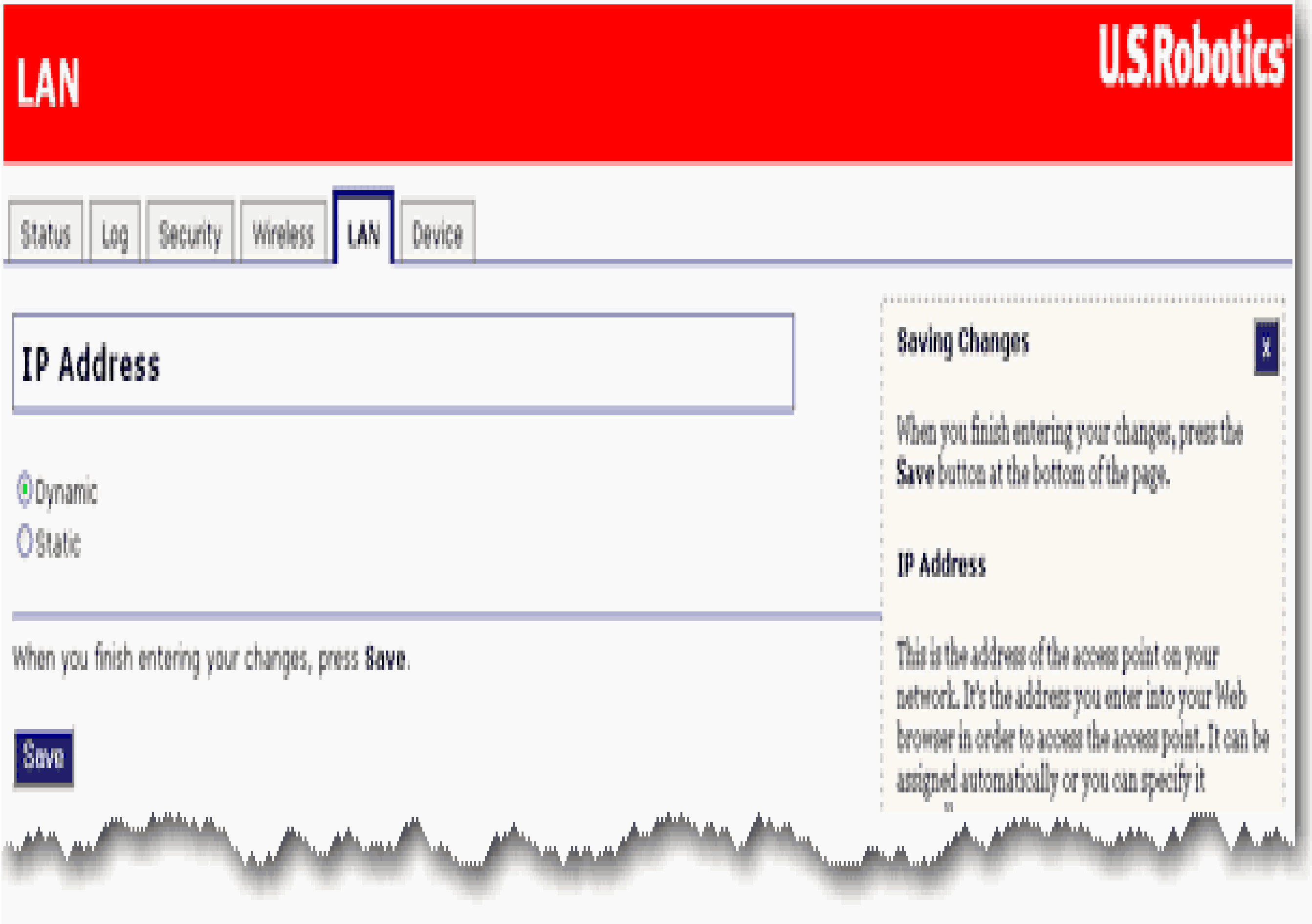
This introductory setup guides you through two easy steps to establish a connection to the Internet and to secure your wireless network. You can access the advanced features of the access point after the setup is complete.

When you're ready to begin, press the **Start** button.

9. Continue the installation procedure starting with Step Three: Configure Basic Settings.

10. After you have configured the basic settings, click the **LAN** tab on the configuration pages.

11. Select **Static** and enter the **IP address** for the access point, then enter the **Gateway**, **DNS server**, and **Subnet mask** of the networking device.



IP Address

● Dynamic
○ Static

When you finish entering your changes, press **Save**.

Saving Changes

When you finish entering your changes, press the **Save** button at the bottom of the page.

IP Address

This is the address of the access point on your network. It's the address you enter into your Web browser in order to access the access point. It can be assigned automatically or you can specify it

12. Click **Save** at the bottom of the page.

13. When you have finished the installation of the access point, you can disconnect the Ethernet cable from the computer and connect your access point to your networking device. You do not need to perform the configuration steps of the installation procedure again.

I have installed my access point but need to connect it to a different networking device.

If you've already installed your access point and then need to connect the access point to a networking device that does not have a DHCP server, you can log in to the access point's configuration pages and assign a static IP address within the range of the new networking device before you move the access point.

1. Start your Web browser.

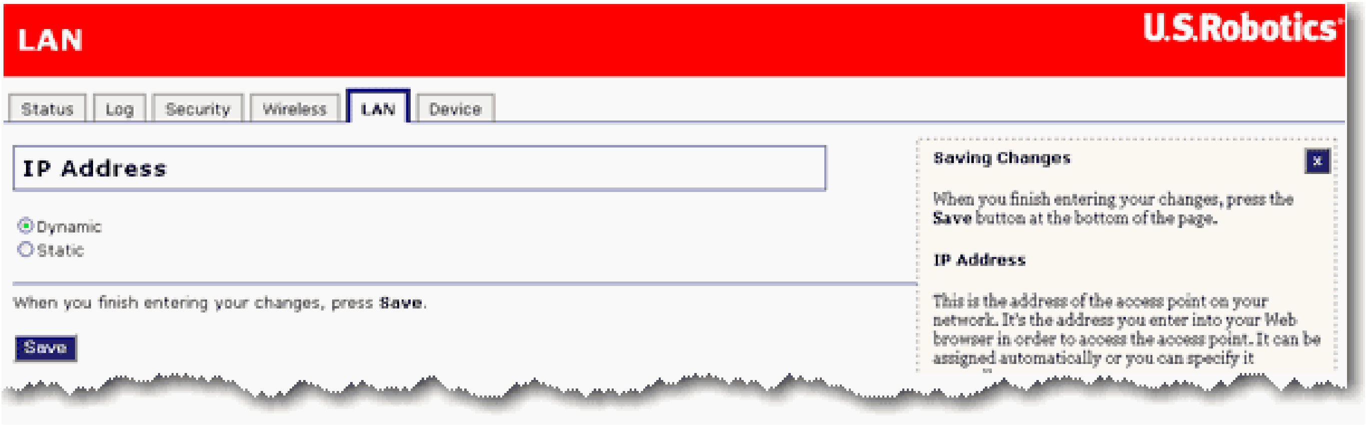
2. In the location or address line, type the IP address of the access point, and press ENTER.

3. Enter your password and login and click **OK**.

4. Click the **LAN** tab on the configuration pages.

5. Select **Static** and enter the **IP address** for the access point, then enter the **Gateway**, **DNS server**,

and **Subnet mask** of the new networking device.



IP Address

● Dynamic
○ Static

When you finish entering your changes, press **Save**.

Saving Changes

When you finish entering your changes, press the **Save** button at the bottom of the page.

IP Address

This is the address of the access point on your network. It's the address you enter into your Web browser in order to access the access point. It can be assigned automatically or you can specify it

6. Click **Save** at the bottom of the page.

7. You can disconnect the Ethernet cable from the networking device and reconnect your access point to another networking device. You do not need to perform the configuration steps of the installation procedure.

Return to Troubleshooting page

USRobotics® Wireless MAXg Access Point: User Guide

The access point is connected to a live power source, but the power LED is off.

Make sure that the access point is connected to a networking device before connecting the access point to power.

Return to Troubleshooting page

The installation procedure did not start when I inserted the USRobotics Installation CD-ROM.

Solution

Some programs may keep the autoplay feature of the installation CD-ROM from starting. Close any open applications and reinsert the CD-ROM.

Solution

Start the CD-ROM manually as follows:

1. **Windows Vista:** Click Windows **Start > Computer**.

   Windows XP: Click Windows **Start > My Computer**.

   Windows 2000: On the desktop, double-click **My Computer**.

2. Double-click the CD drive.

Return to Troubleshooting page

The detection utility does not find the Wireless *MAX*g Access Point.

1. Click **Detect** to rescan the network.

2. If the locator still does not find the access point, look at the client list for the networking device that is connected to the access point. Refer to the device's documentation to find out how to view the client list.

3. In the client list, find the LAN MAC address shown on the bottom of the access point and note the IP address associated with that MAC address. This is the IP address of the access point.

4. Start a web browser, type the IP address of the access point, and press ENTER.

5. Verify that the connection information is correct for the network to which the access point is connected.

Return to Troubleshooting page

USRobotics *Wireless MAXg Access Point: User Guide*

I cannot access the configuration pages.

1. In your Web browser, make sure that you are entering the correct IP address for the access point. To find the IP address, see Logging in to the Configuration Pages.

2. Configure your Web browser so that the HTTP Proxy feature of your Web browser.

3. If you are trying to access the configuration pages wirelessly, try to access them with a wired connection as follows:

   A. Using a computer connected by Ethernet cable to the same networking device as the access point, start a Web browser.

   B. Enter the IP address of the access point and press ENTER.

      - If you can access the configuration pages with a wired connection, you are experiencing a wireless connectivity issue. See "For wireless connections" in the basic troubleshooting procedure.
      - If you cannot access the configuration pages with a wired connection, reboot the access point by disconnecting and then reconnecting its power supply.

      If you have rebooted the access point but still cannot access the configuration pages, restore the factory default settings of the access point to reactivate it.

> **Note:** When you restore the factory default settings, the access point will lose all custom settings.

To restore the factory default settings, use a small object such as a paper clip to press in and hold the reset button on the back of the access point for 7 seconds.

After you restore the access point to its factory default settings, reconfigure the basic settings of the access point, or, if you made a backup of your settings, restore the settings by using the backup.

Return to Troubleshooting page

USRobotics *Wireless MAXg Access Point: User Guide*

After I performed a firmware upgrade, the access point did not display its status page.

Solution

The upgrade may still be in progress. Wait for at least two minutes.

Solution

If you received the upgrade completion message, reboot the access point by disconnecting and then reconnecting its power supply.

Solution

1. Restore the factory default settings of the access point to reactivate it.

   > **Note:** When you restore the factory default settings, the access point will lose all custom settings.

   To restore the factory default settings, use a small object such as a paper clip to press in and hold the reset button on the back of the access point for 7 seconds.

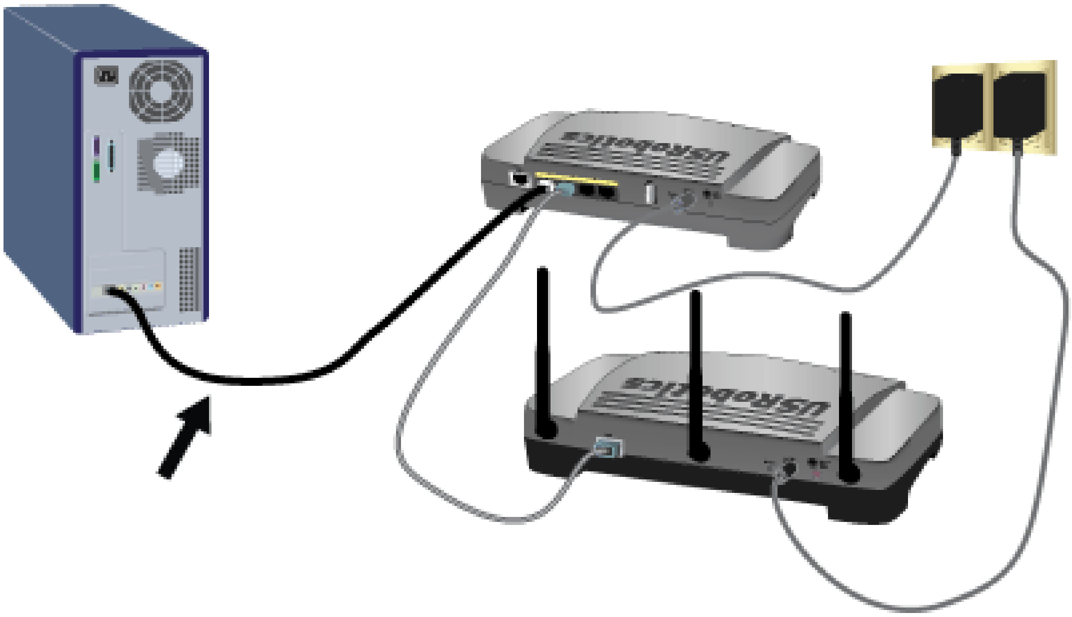
After you restore the access point to its factory default settings, reconfigure the basic settings of the access point, or, if you made a backup of your settings, restore the settings by using the backup.

2. Reapply the firmware upgrade.

Solution

The firmware image may have been corrupted during the upgrade procedure. Perform the following procedure to force the upgrade:

1. Using a networking cable and the same computer that you were using when the upgrade failed, connect the computer directly to the same networking device as the access point. Do not try to use a wireless connection for this procedure.



2. **Windows users**:

   A. If you do not know the IP address of the access point, run the Network Device Locator to find the IP address.

   B. Locate the folder that contains that firmware file that you downloaded.

   C. Open a command prompt as follows:

Windows Vista:

1. Click Windows **Start**.
2. In the **Search** box, type **Command Prompt** and press ENTER.
3. In the result list, double-click Command Prompt.

All other Windows operating systems:

1. Click Windows **Start > Run**.
2. In the **Run** dialog box:

   Windows XP, 2000, and NT: Type **cmd** and click **OK**.

   Windows Me, 98, and 95: Type **command** and click **OK**.

Macintosh and Linux users:

A. If you do not know the IP address of the access point, find the IP address manually.

B. Open a terminal.

3. Type **cd** followed by the path to the firmware file. Use quotation marks around the pathname as shown in the following example:

   cd "C:\networking\usr5455"

   and then press ENTER.

4. Type the following command (but do not press ENTER):

   tftp -i *xxx.xxx.x.x* put 5455.usr where *xxx.xxx.x.x* is the IP address of the access point.

5. Disconnect and then reconnect the power supply of the access point.

6. Press ENTER.

   You should see a message in the command window stating that the image was transferred.

7. Wait for the upgrade to finish. When the wireless LED 📶 turns on, the upgrade is done.

Return to Troubleshooting page

USRobotics® Wireless MAXg Access Point: User Guide

The Wireless Nd1 Access Point does not appear when I scan for it with a wireless client.

Solution:

The access point may not be broadcasting its network name.

1. Using a computer connected to the same networking device as the access point, start a Web browser.
2. Type the IP address of the access point, and press ENTER to display the configuration pages of the access point. You can get the IP address from the Network Device Locator.
3. Click the Wireless tab and verify that Broadcast network name is selected. If it is not selected, select it, scroll to the bottom of the Wireless page, and click **Save**.

Solution:

Disconnect the network cable from the client device before scanning for the access point.

Return to Troubleshooting page

USRobotics® *Wireless MAXg Access Point: User Guide*

My client is not communicating with the Wireless Nd1 Access Point.

Solution:

See "For wireless connections" in the basic troubleshooting procedure.

Solution:

In the configuration utility for your wireless card or adapter, ensure that you are connecting to the correct Wireless ***MAX*g** Access Point by verifying the WLAN MAC address. You can find the WLAN MAC address on the label on the bottom of the access point.

Solution:

The access point may not have received a valid IP address for your network. Check the LAN configuration page of the access point.

- If the IP address is set to Dynamic, make sure that the access point is connected to a DHCP server.
- If you use a static IP address verify that it is in the same subnet as your client's IP address.

Solution:

The access point may not be responding. Try the following:

1. Reconnect by following the steps in Connecting a Wireless Client.
2. If you still are not communicating with the access point, restore the factory default settings of the access point to reactivate it.

   Note: When you restore the factory default settings, the access point will lose all custom settings.

   To restore the factory default settings, use a small object such as a paper clip to press in and hold the reset button on the back of the access point for 7 seconds.
3. After you restore the access point, reconfigure the basic settings of the access point, or, if you made a backup of your settings, restore the settings by using the backup.

Return to Troubleshooting page

USRobotics **Wireless MAXg Access Point: User Guide**

I am no longer able to access the Internet.

When your computer uses an access point to connect to the Internet, a number of devices have to work together:

- Your computer connects to the access point via a wireless connection.
- Your access point connects to your router or other networking device via an Ethernet cable.
- Your router connects to your cable or DSL modem via an Ethernet cable (your router and modem may be contained within a single device).
- Your cable or DSL modem connects to your Internet Service Provider (ISP) via your cable or phone network.

Your Internet access might be failing within any of these devices or in any of the connections between them. To solve the problem, you need to identify the device or connection that is causing the failure and then correct the failing condition. Perform the following procedures to locate and correct the problem:

1. Check the indicator lights.

2. Verify the connection between your computer and the access point.

3. Verify the connection between the access point and your other networking device.

Check the Indicator Lights

Check the indicator lights of all networking devices between the computer and the point where Internet service enters the building. If one or more of these devices indicates a problem, see the documentation for that device to return it to normal operations. On the access point, the following LEDs should be on: ⏻ 📶 🖧 (power, WLAN, and LAN).

Verify the Connection between Your Computer and the Access Point

Run your wireless adapter utility. Does it report a successful connection to your access point?

If You Have a Wireless Connection

If your wireless utility reports a successful wireless connection, your computer may be connected to a neighbour’s access point instead of yours. Use your wireless utility to check the Network name (SSID) of the access point you’re connected to. If the wireless adapter is connected to the wrong access point, use the utility to force your computer to connect to your access point (see the documentation for your wireless adapter).

If you are connected to the access point and still do not have access to the Internet, verify that the access point is responding by logging in to the configuration pages.

If You Do Not Have a Wireless Connection

1. See "For wireless connections" in the basic troubleshooting procedure.

2. If you have enabled MAC filtering on the access point, make sure that your wireless adapter is permitted to connect to the access point. Note that MAC filtering refers to specific wireless adapters. If you use MAC filtering and have changed wireless adapters, you must add the MAC address of the new wireless adapter to the MAC filtering list on the access point.

Verify the Connection between the Access Point and Your Other Networking Device

1. On the device to which the access point is connected by ethernet cable, check the

power and status LEDs. Verify that the device is powered on and connected to the Internet. Refer to the device's documentation for information on its status indicators.

2. If the access point is configured to get an IP address dynamically, make sure that the networking device has a DHCP server running.

3. If the access point is connected directly to your modem, check the modem documentation to determine whether the access point needs to have a static IP, gateway, and DNS entries or will get the network address using DHCP; then make sure that the access point is configured accordingly.

4. Ping the router or other networking device. If the ping returns a reply, the access point is reaching the networking device. Refer to the device's documentation for debugging the connection between the device and your Internet Service Provider.

Return to Troubleshooting page

USRobotics® Wireless MAXg Access Point:

User Guide

My client does not establish a wireless connection to the Wireless *MAX*g Access Point after I changed the settings.

In the configuration utility for your wireless adapter:

1. Ensure that you are connecting to the Wireless Nd1 Access Point by verifying the WLAN MAC address.
2. Ensure that the access point and your wireless adapter are using the same network name, channel, and encryption options, including the passphrase or key. If you change one of these settings on the access point, you must also change the setting on every wireless adapter that is to connect to the access point.

Return to Troubleshooting page

USRobotics *Wireless MAXg Access Point: User Guide*

My wireless unicast connection is very slow while another client is using the access point for a multicast stream, such as videoconferencing or Internet radio.

Set the multicast rate to 2 and try your unicast connection. If your connection improves, continue increasing the multicast rate until you find the speed that provides the best combination of connections for unicast and multicast clients. In a wireless network with both 802.11b and 802.11g clients connected to the access point, you can increase the multicast rate up to 9. In a wireless network with only 802.11g clients connected to the access point, you can increase the multicast rate up to 54.

Return to Troubleshooting page

USRobotics Wireless MAXg Access Point: User Guide

My client cannot achieve 270 Mbps connections.

Make sure the wireless products you are using to connect to the Wireless ***MAXg*** Access Point support 270 Mbps speeds and that the Wireless ***MAXg*** Access Point is connected to a networking device that supports 270 Mbps speeds.

Return to Troubleshooting page

USRobotics *Wireless MAXg Access Point: User Guide*

Troubleshooting ping procedure

If at any time during the ping procedure you do not receive a return message for a successful ping, the address that you are pinging has been changed and is causing a conflict or is no longer available.

> **Note:** Linux users can perform steps 3 through 7 after opening a terminal.

1. Open a command prompt as follows:

   Windows Vista:

   A. Click Windows **Start**.

   B. In the **Search** box, type **`Command Prompt`** and press ENTER.

   C. In the result list, double-click **`Command Prompt`**.

   All other Windows operating systems:

   A. Click Windows **Start > Run**.

   B. In the **Run** dialog box:

      Windows XP, 2000, and NT: Type **cmd** and click **OK**.

      Windows Me, 98, and 95: Type **command** and click **OK**.

2. Type **`Ping 127.0.0.1`**. This is your local host address and this will ensure that the TCP/IP

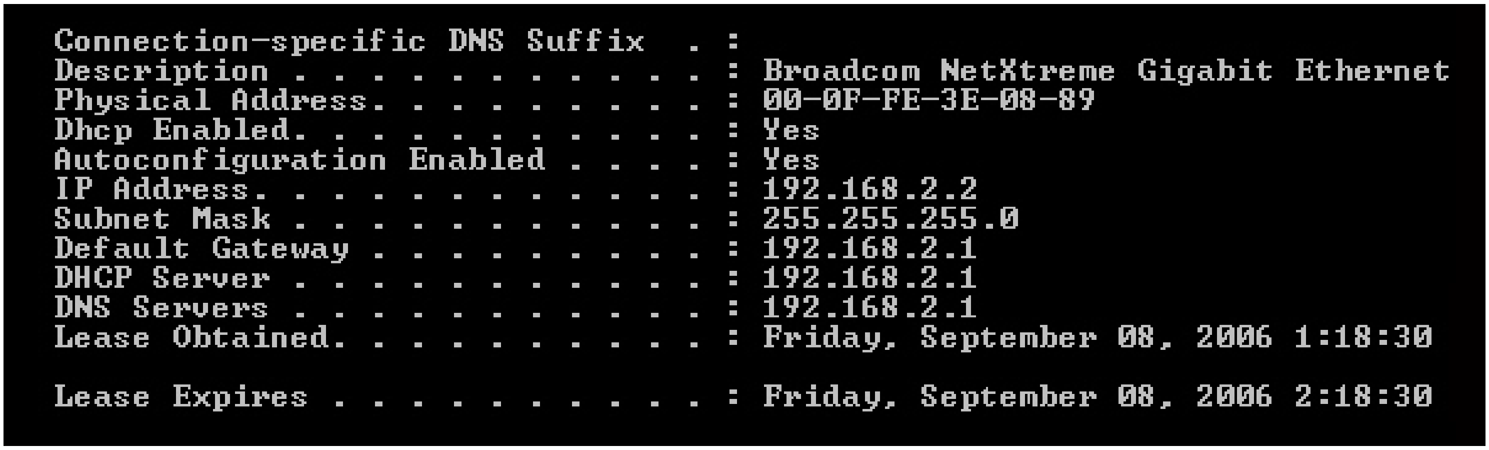
protocol is installed and functioning properly. If you cannot complete this ping, refer to your Windows operating system documentation for instructions on installing TCP/IP.

3. Obtain IP information for your computer as follows:

   Windows Vista, XP, 2000, and NT users: **Type** **`ipconfig /all`** and press ENTER.

   Windows Me, 98, and 95 users: Type **`winipcfg`** and press ENTER.

   This displays IP configuration similar to the following:



```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
   Physical Address. . . . . . . . . : 00-0F-FE-3E-08-89
   Dhcp Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . . . . . . . . : 192.168.2.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DNS Servers . . . . . . . . . . . : 192.168.2.1
   Lease Obtained. . . . . . . . . . : Friday, September 08, 2006 1:18:30

   Lease Expires . . . . . . . . . . : Friday, September 08, 2006 2:18:30
```

4. Type **`Ping`** followed by the IP address displayed in step 3 and press ENTER.

   This verifies whether your computer is responding to requests. If your computer's IP address is 169.254.xxx.xxx or if you cannot complete this ping, make sure all the cables are properly connected, unplug the Wireless ***MAX*g** Access Point, plug it back in, and reboot your computer.

5. Type **`Ping`** followed by the IP address of the access point and press ENTER.

   If you can establish communication with the Wireless ***MAX*g** Access Point, you can access the configuration pages. If you cannot establish communication with the access point, make sure all the cables are properly connected, unplug it, plug it back in, and reboot your computer. If you still cannot complete this ping, refer to My client is not communicating with the Wireless Nd1 Access Point and skip the solutions dealing with wireless connections.

6. Type **`Ping`** followed by the LAN IP address, which is the Default Gateway address displayed in step 3, and press ENTER.

   This verifies whether you can get past the access point to your gateway. An example of a gateway is a router.

7. Type **Ping** followed by the WAN IP address of your gateway.

   This is the address that is provided either by your ISP or by the outside LAN. \ This procedure will ensure that you have access to the Internet.

8. Type **Ping** followed by the DNS server address displayed in step 3 and press ENTER.

   This lets you resolve valid Internet host names to IP addresses and to verify that you can browse the Internet.

9. If you can successfully ping the DNS server but still cannot reach the Internet, assign your DNS servers statically as follows:

   Windows Vista:

   A. Access the configuration program or configuration pages of the networking device connected to the access point, and find the WAN status information. From that information you need the IP addresses of the WAN DNS servers. For detailed instructions, consult the documentation for the networking device.

   B. Click Windows **Start > Control Panel**.

   C. Double-click **Network and Internet > Network and Sharing Center > Manage network connections**.

   D. Right-click the **Local Area Connection** of the network adapter that connects the computer to the networking device, select **Properties**.

   E. Under **This connection uses the following items**, select **Internet Protocol (TCP/IP)** and click **Properties**.

   F. Select **Use the following IP address**, enter the IP addresses that you noted in step A, and click **OK**.

   G. Click **OK** again.

   Windows XP, 2000, or NT:

   A. Access the configuration program or configuration pages of the networking device connected to the access point, and find the WAN status information. From that information you need the IP addresses of the WAN DNS servers. For detailed instructions, consult the documentation for the networking device.

B. Click Windows **Start > Control Panel**, and double-click **Network Connections**.

C. In the **Network Connections** window, right-click the **Local Area Connection** of the network adapter that connects the computer to the networking device, select **Properties**.

D. Under **This connection uses the following items**, select **Internet Protocol (TCP/IP)** and click **Properties**.

E. Select **Use the following DNS server addresses**, enter the IP addresses that you noted in step A, and click **OK**.

F. Click **OK** again.

Windows Me, 98, or 95:

A. Access the configuration program or configuration pages of the networking device connected to the access point, and find the WAN status information. From that information you need the IP addresses of the WAN DNS servers. For detailed instructions, consult the documentation for the networking device..

B. On the desktop, right-click **Network Places** or **Network Neighborhood** and select **Properties**.

C. On the **Configuration** tab, select the network adapter that connects the computer to the router and click **Properties**.

D. On the **DNS Configuration** tab, click **Enable** and enter a **Host** name.

E. In **DNS Server Search Order**, enter the IP address of the primary DNS server and click **Add**.

F. In **DNS Server Search Order**, enter the IP address of the secondary DNS server and click **Add**.

G. Click **OK**.

H. Click **OK** again.

Return to Troubleshooting page

USRobotics® *Wireless MAXg Access Point: User Guide*

Frequently Asked Questions

How do I restore the access point to its factory default settings?

First, be aware that restoring the factory default settings loses all configuration changes that you made.

If you are certain that you need to restore the factory default settings, use a small object such as a paper clip to press in and hold the reset button on the back of the access point for 7 seconds.

After you restore the access point, reconfigure the basic settings of the access point, or, if you made a backup of your settings, restore the settings by using the backup.

Can I use the access point if my networking device does not have DHCP?

Yes. By default, the access point is configured to obtain an IP address from a DHCP server, but you can manually set the IP address of the access point from the configuration pages. For information on assigning a static IP address to the access point, see The networking device I am using does not have a DHCP server.

USRobotics Wireless MAXg Access Point: User Guide

Support

1. Know your model and serial number.

   Your model number is 5455. You can find your serial number on the side of the package and on the bottom of the access point.

2. Go to the Support section of the USRobotics Web site at www.usr.com/support

   Many of the most common difficulties that users experience have been addressed in the FAQ and Troubleshooting Web pages for your access point. The Support Web pages also contain information on the latest firmware and documentation updates.

3. Submit your technical support question using an online form, or contact the USRobotics Technical Support Department.

Country	Webmail	Voice
United States & Canada	http://www.usr.com/emailsupport	(888) 216-2850

Country	Webmail	Voice
Austria	www.usr.com/emailsupport/de	07110 900 116
Belgium (Flemish)	www.usr.com/emailsupport/nl	070 23 35 45
Belgium (French)	www.usr.com/emailsupport/be	070 23 35 46
Czech Republic	www.usr.com/emailsupport/cz	

Denmark	www.usr.com/emailsupport/ea	38323011
Finland	www.usr.com/emailsupport/ea	08 0091 3100
France	www.usr.com/emailsupport/fr	0825 070 693
Germany	www.usr.com/emailsupport/de	0180 567 1548
Greece	www.usr.com/emailsupport/gr	
Hungary	www.usr.com/emailsupport/hu	0180 567 1548
Ireland	www.usr.com/emailsupport/uk	1890 252 130
Italy	www.usr.com/emailsupport/it	39 02 69 43 03 39
Luxembourg	www.usr.com/emailsupport/be	342 080 8318
Middle East/Africa	www.usr.com/emailsupport/me	+44 870 844 4546
Netherlands	www.usr.com/emailsupport/nl	0900 202 5857
Norway	www.usr.com/emailsupport/ea	23 16 22 37
Poland	www.usr.com/emailsupport/pl	
Portugal	www.usr.com/emailsupport/pt	0 21 415 4034
Russia	www.usr.com/emailsupport/ru	8 800 200 20 01
Spain	www.usr.com/emailsupport/es	902 117964
Sweden	www.usr.com/emailsupport/se	08 5016 3205
Switzerland	www.usr.com/emailsupport/de	0848 840 200
Turkey	www.usr.com/emailsupport/tk	0212 444 4 877
United Arab Emirates	www.usr.com/emailsupport/me	0800 877 63
United Kingdom	www.usr.com/emailsupport/uk	0870 844 4546

For current support contact information, go to: www.usr.com/emailsupport