



Wireless Nd1 Access Point: User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help



The USRobotics Wireless **Nd₁**[™] Access Point turns your wired network into a powerful and secure wireless network.

Featuring USRobotics' exclusive **Nd₁** wireless technology, delivering speeds up to 270 Mbps^{*} and a range up to 5 times greater than standard 802.11g, the access point is designed to provide total home/small business coverage and optimal performance. New SecureEZSetup[™] provides simple and fast installation and security configuration. A full complement of security capabilities deliver confident, high-performance wireless networking.

System Requirements

- A computer with an Ethernet adapter installed
- A router or other networking device with a DHCP server
- 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.
	SecureEasySetup	Off	SecureEasySetup mode is not ready on the access point.
		Solid	SecureEasySetup mode is ready.
		Blinking	Communicating with SecureEasySetup devices.
	LAN	Off	No LAN connection.
		Solid	LAN link is achieved.
		Flashing	Sending and receiving data.

Back

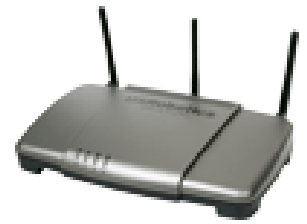


Item	Function
	Connects an antenna to the access point.
LAN	Connects the access point to a networking device.

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.
15VDC	Connects the power adapter to your access point.
 SecureEasySetup button	Enables SecureEasySetup on your access point. • To enable SecureEasySetup on your access point, press and hold the SecureEasySetup button for 1 second. • To reset your wireless security settings to the factory default (no security enabled), press and hold the SecureEasySetup button for 7 seconds.

* Actual performance may vary depending on operating environment and distance between networked devices.





USRobotics® *Wireless Nd1 Access Point:*

User Guide

- **Home**
 - **Installation**
 - **Configuration**
 - **Tutorials**
 - **Help**
-

Product Specifications

- Integrated 270 Mbps 802.11n Draft 1.0 Wireless Access Point, Bridge, and Range extender
- One RJ-45, 10/100 Mbps auto-sensing and auto-switching Ethernet LAN port
- HTML-based configuration
- Roaming capability
- Wi-Fi Multi Media (WMM): Prioritization of marked voice and video traffic
- AP firmware upgrades available through the Web User Interface
- Complies with IEEE 802.11g 54 Mbps wireless radio standard and 802.11n Draft 1.0 270 Mbps wireless radio
- Dynamic IP Address assignment via DHCP or Static IP address assignment through the Web User Interface (Access Point mode only)
- Wireless Multi-Bridging support using Wireless Distribution System (WDS) (Bridge mode only)

Security Features

- WPA and WPA2 (Wi-Fi Protected Access)
- 64/128-bit WEP (Wired Equivalent Privacy) data encryption with Open/Shared Key

- WPA/WPA2-Enterprise (WPA-WPA2 with 802.1X)
- Ability to disable SSID Broadcast
- MAC address authentication and wireless association control (Access Point and Range Extender modes only)
- 802.1x pass-through support (not supported in WDS Mode)
- WDS restrictions (Bridge mode only)



© 2005-2006 **U.S. Robotics Corporation**



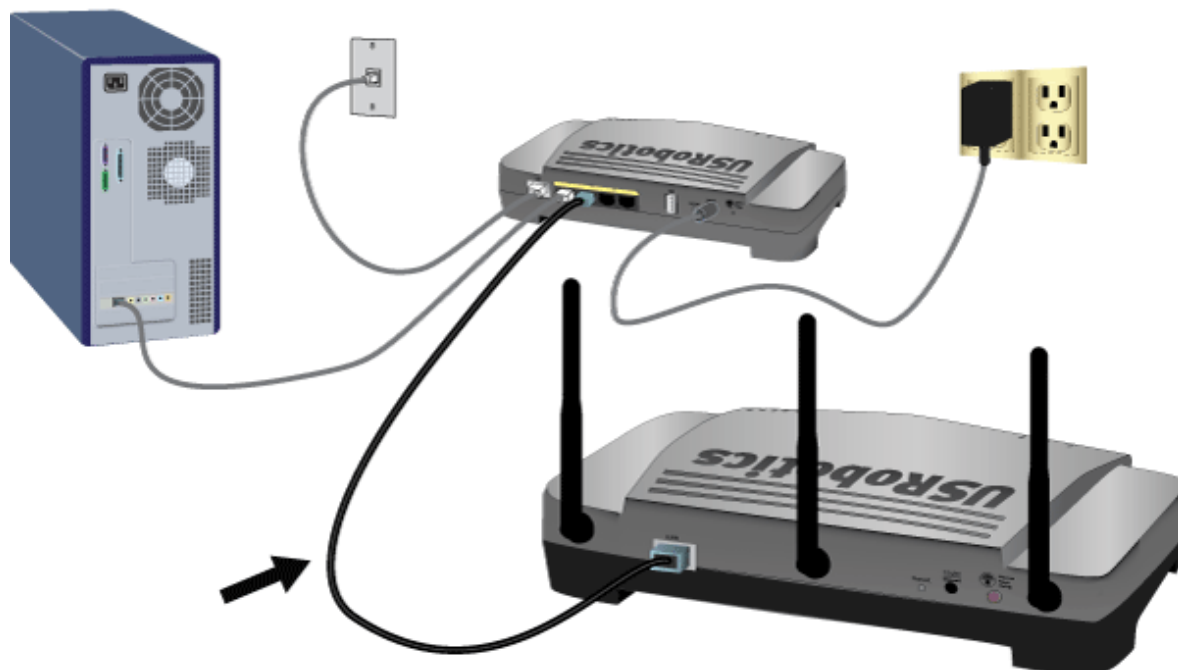
USRobotics® Wireless Nd1 Access Point: User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

Installing the Access Point

Step One: Connect the Access Point

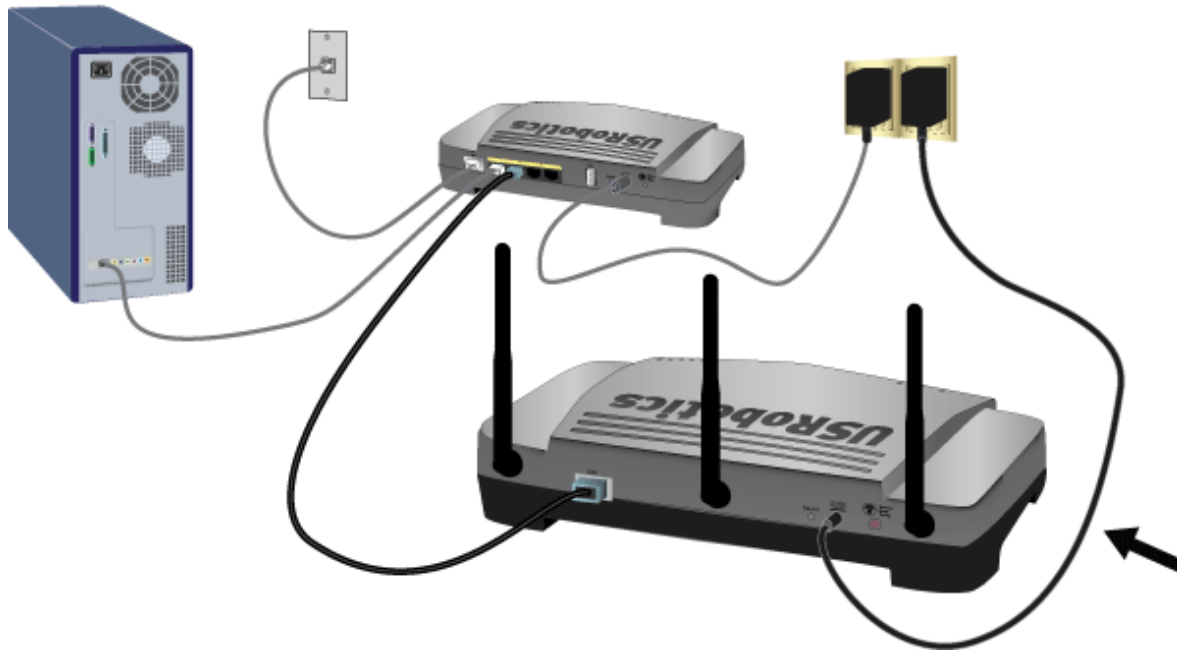
1. Look at the label on the bottom of the access point and note its LAN MAC address. You may need it to distinguish the access point from other devices on your network.
2. Connect the provided antennas to the back of the access point.
3. Use the supplied Ethernet cable to connect the LAN port on the 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 **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.

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 Network Device Locator 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:

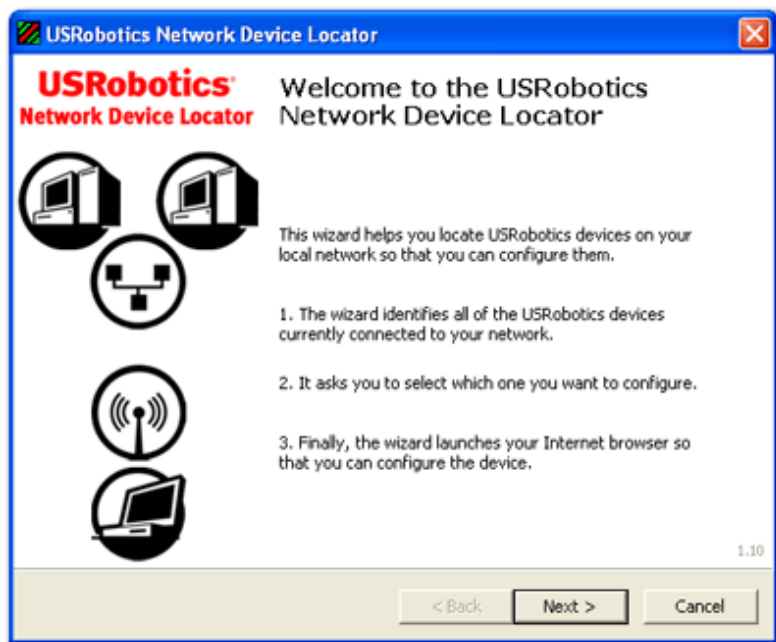
A. **Windows XP:** Click Windows **Start > My Computer**.

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

B. Double-click the CD drive.

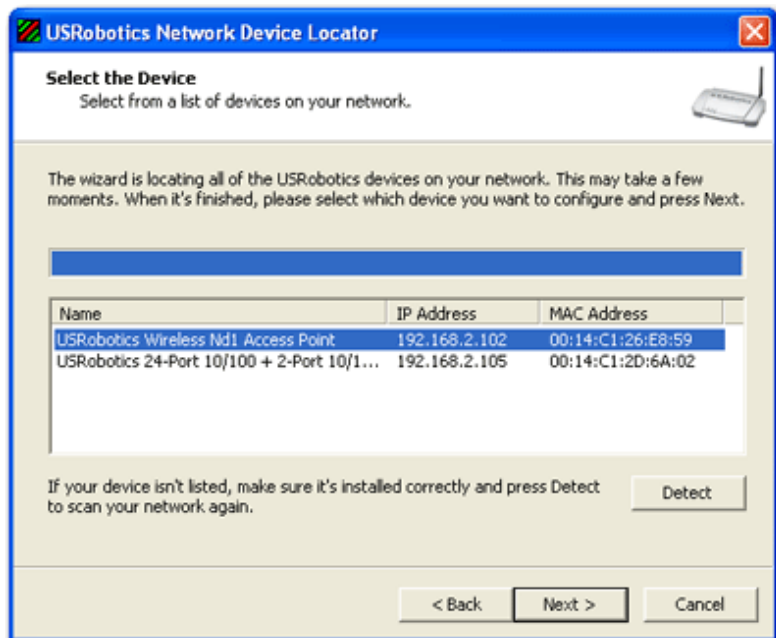
2. Follow the on-screen instructions to install the locator.

When the locator is installed, it starts automatically:



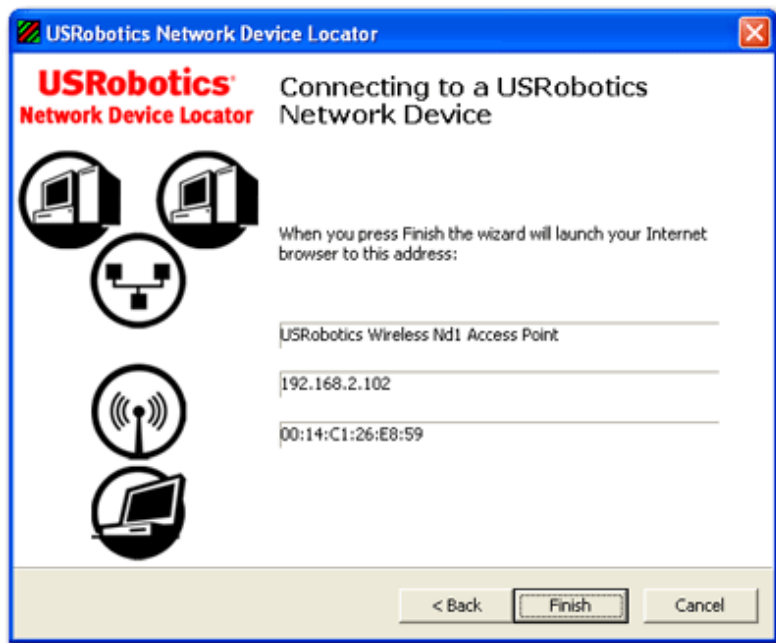
3. Click **Next**.

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



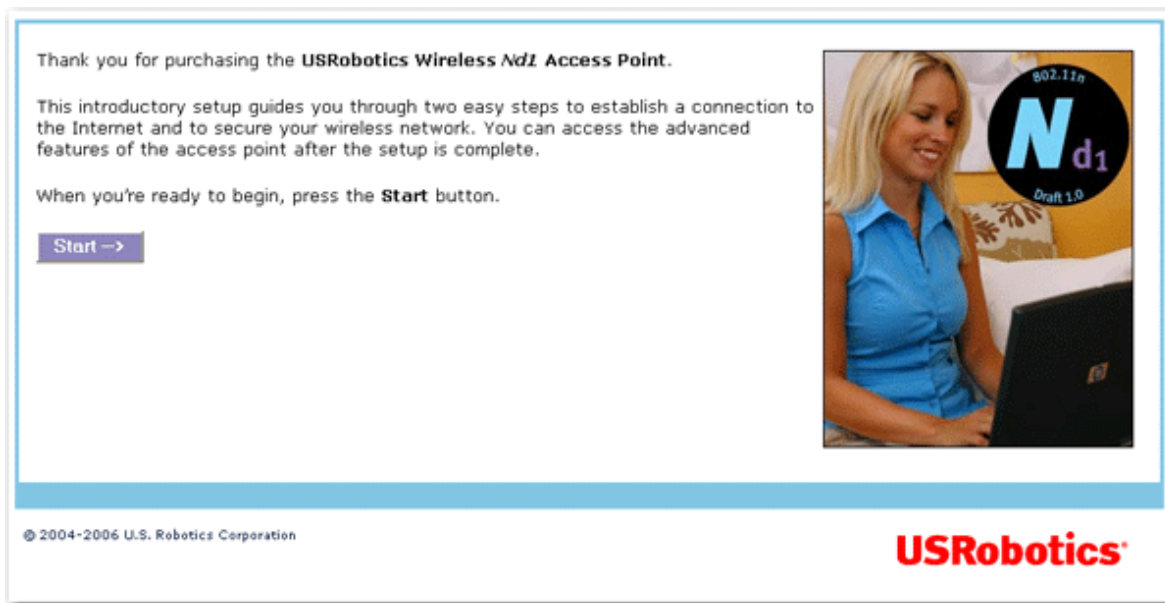
4. Select the device whose MAC address matches the LAN MAC address on the bottom of the access point, and click **Next**.

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



5. Click **Finish**.

The locator launches the setup wizard for the access point:



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

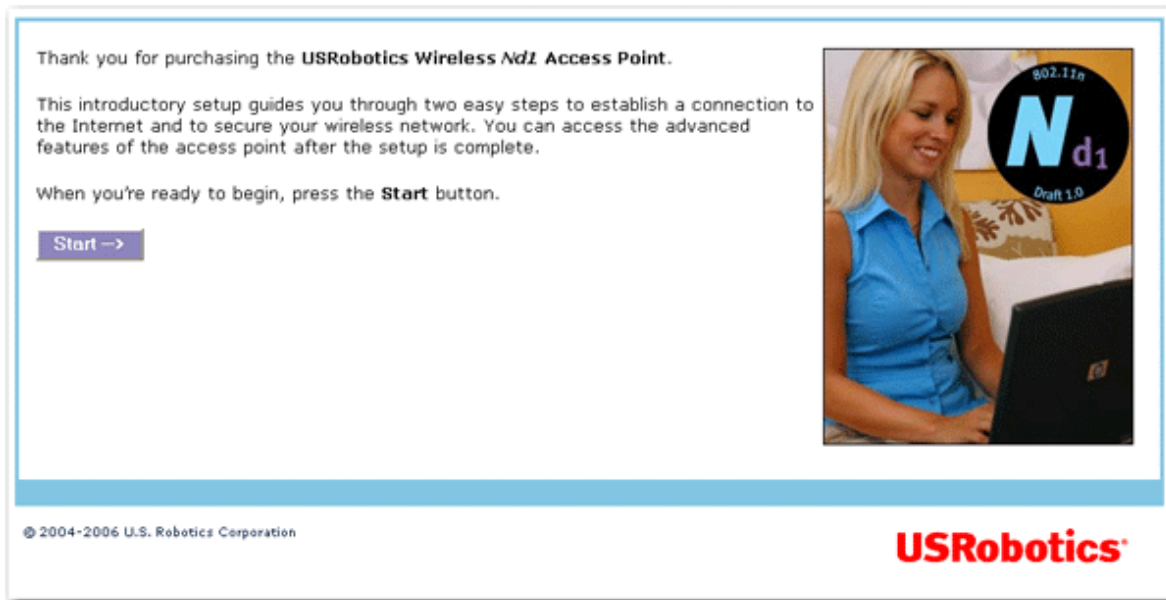
The networking device to which you connected the access point assigns IP addresses on your local network. To find the IP address of the access point:

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.
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:



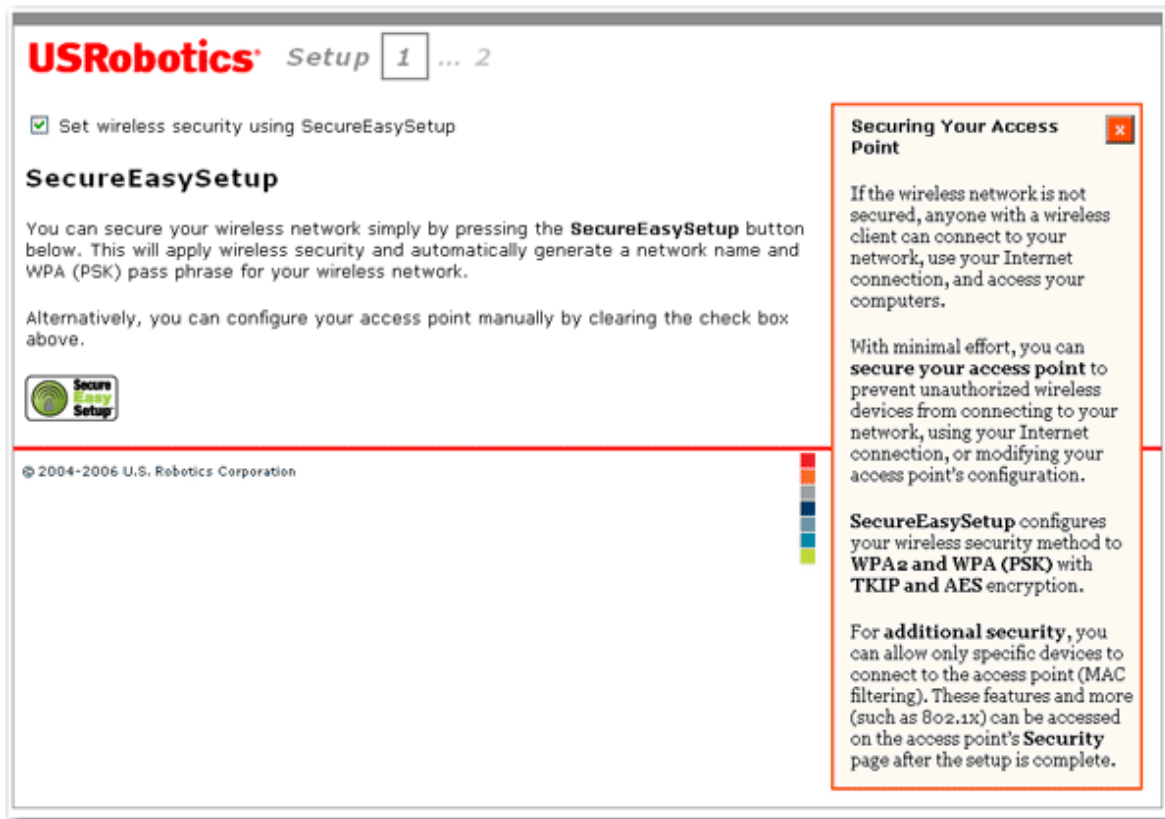
Step Three: Configure Basic Settings

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 SecureEasySetup page:



2. Do one of the following:
 - o To use SecureEasySetup to set your wireless security:

- A. Select **Set wireless security using SecureEasySetup** and click .
- B. Wait for setup to complete, then click **Continue**.

OR

- o To set your wireless security information manually:
 - A. Clear the **Set wireless security using SecureEasySetup** checkbox.

The setup page displays wireless security settings.

USRobotics Setup 1 ... 2

☐ Set wireless security using SecureEasySetup

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:

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 "USR5454APOffice" 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:

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**.

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.

SecureEasySetup configures your wireless security method to **WPA2 and WPA (PSK)** with **TKIP and AES** encryption.

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.

- B. Enter a **Network Name** (SSID), select a security **Method**, and enter your pass phrase. For more information about pass phrases, see [wireless security information](#).

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.

- C. Click **Next**.

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

USRobotics Setup 1 ... 2

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**.

Finish

© 2004-2006 U.S. Robotics Corporation

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.

3. 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 **Nd₁** 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**.

* By default, SecureEasySetup is ready to be used on your access point. If you change the wireless settings, be aware that for SecureEasySetup to be ready on your access point, it must be set with WPA2 and WPA (PSK) wireless security, with TKIP and AES encryption, and a pass phrase (which is also commonly called a Network key, WPA key, or WPA Pre-shared key). You can configure the settings manually on the Wireless configuration page of the access point or automatically by pressing the SecureEasySetup button on the back of the access point.





USRobotics® Wireless N_{d1} Access Point:

User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

Configuration Pages

The Wireless N_{d1} 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](#)
- [Using the Configuration Pages](#)

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 Device Locator (Windows Users Only)

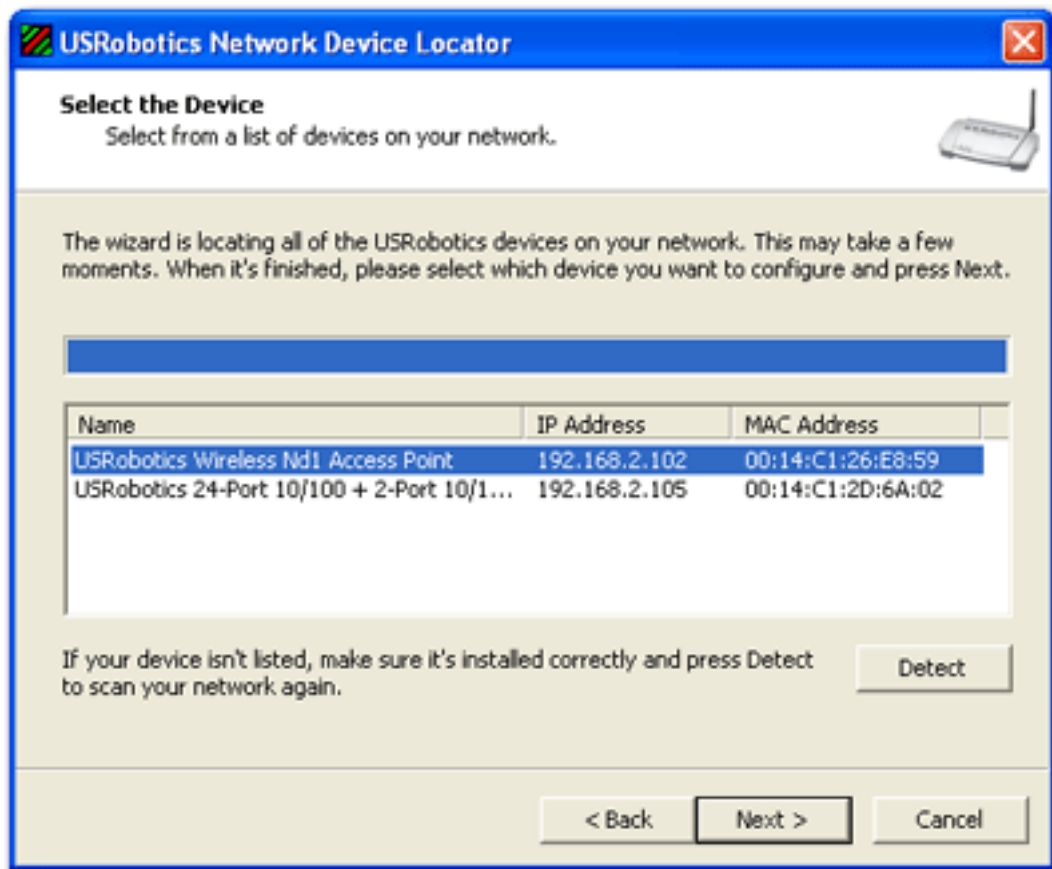
1. Click Windows **Start > Programs > USRobotics Network Device Locator**.

The locator displays its welcome screen:



2. Click **Next**.

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



- Find the Wireless **Nd₁** Access Point in the list. (If you have more than one Wireless **Nd₁** 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.

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:

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

4. Note the IP address associated with the LAN MAC address of the access point.

Using the Configuration Pages

The configuration pages are divided into the functional areas shown on its tabs and listed below:

- [Status](#)
- [Security](#)
- [Wireless](#)
- [LAN](#)
- [Device](#)





Wireless Nd1 Access Point: User Guide

- **Home**
- **Installation**
- **Configuration**
 - **Tutorials**
 - **Help**

Connecting a Wireless Client

You can use the SecureEasySetup™ button to connect installed Wireless Nd1 or other certified SecureEasySetup wireless devices to your access point.*

If your wireless client has SecureEasySetup, you should see one of the following logos on the device or within the client utility:



If your wireless client does not support SecureEasySetup, you can manually enter the wireless security settings.

Connecting a Device Using SecureEasySetup

1. Press the SecureEasySetup button on the back of the access point for 1 second. The SecureEasySetup LED on the front of the access point starts blinking after you release the button.
2. Initiate SecureEasySetup in the client utility for your wireless adapter.
3. The access point and the wireless device synchronise their wireless security settings, and the device is securely connected to the access point.

Connecting a Device Manually

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.

* BROADCOM, SecureEasySetup, and the SecureEasySetup logo are trademarks or registered trademarks of Broadcom Corporation in the United States and/or other countries.





Wireless Nd1 Access Point: User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

Using SecureEasySetup

SecureEasySetup™ makes it easy to connect wireless clients to the access point. SecureEasySetup automatically configures wireless security settings between the access point and your wireless clients.*

Access Point or Repeater Mode

If your Wireless **Nd₁** Access Point **Wireless Network Type** is set to **Access Point** or **Range Extender** mode, SecureEasySetup transmits SecureEasySetup information, so your wireless clients can execute SecureEasySetup and get the new **Network Name** (SSID), method type, encryption type, and pass phrase for your wireless network.

Note: While the access point is in SecureEasySetup configuration mode, you can only configure one SecureEasySetup device at a time. Attempting to connect multiple devices may result in errors.

When the SecureEasySetup button on the access point is pressed for 1 second:

1. One of the following occurs:

- If you do not have any wireless security settings applied to your access point, SecureEasySetup generates a **Network Name** (SSID), sets **WPA2 and WPA (PSK)** wireless security with **TKIP and AES** encryption, and generates a pass phrase.
- If you already have a **Network Name** (SSID), **WPA2 and WPA (PSK)** wireless security with **TKIP and AES** encryption, and a pass phrase set on the access point, SecureEasySetup does not change any of these settings.
- If you have another wireless security method or encryption type set on the access point, SecureEasySetup detects the **Network Name** (SSID) being used on the access point, then resets your method and encryption to **WPA2 and WPA (PSK)** wireless security with **TKIP and AES** encryption, and generates a pass phrase.

- SecureEasySetup negotiates with an installed **Nd₁** or other certified SecureEasySetup wireless device in range that is in SecureEasySetup mode to pass the wireless security settings to the device.

Pressing the SecureEasySetup button on your access point for 7 seconds resets your wireless security settings to the factory default, **None** (no security enabled).

Connect a New Wireless Client Using SecureEasySetup

- Press the **SecureEasySetup** button on the access point for 1 second. The SecureEasySetup LED will blink, indicating that it is ready to connect a SecureEasySetup device.
- Press the **SecureEasySetup** button in the utility for your networking device or physically press the **SecureEasySetup** button on the networking device.

For wireless adapters, the wireless adapter utility will display a message when the connection has been successfully completed.

For networking devices with LEDs, the SecureEasySetup LED on the access point will stop blinking when the SecureEasySetup process has completed on the access point.

Bridge or Infrastructure Mode

If your Wireless **Nd₁** Access Point **Wireless Network Type** is set to **Bridge** or **Infrastructure** mode, SecureEasySetup establishes communication and negotiates security between the router or access point.

When the SecureEasySetup button on the access point is pressed for 1 second:

- SecureEasySetup negotiates with an installed **Nd₁** or other certified SecureEasySetup networking device in range that is also in SecureEasySetup mode.
- SecureEasySetup automatically configure the access point's wireless security settings and pass phrase for a connection to the wireless network.

Pressing the SecureEasySetup button on your access point for 7 seconds resets your wireless security settings to the factory default, **None** (no security enabled).

Disable SecureEasySteup

Press the **SecureEasySetup** button on the access point for 7 seconds.

Note: This is not the same as a [restore to factory defaults](#) or a [reboot](#) of the access point. The SecureEasySetup button only affects your wireless security settings.

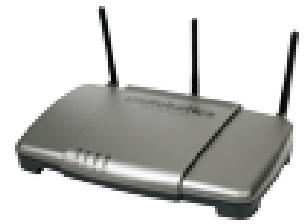
The SecureEasySetup LED will turn off. The security method and encryption type for your wireless network will be reset to **None**. No other settings on your access point will be changed.

* BROADCOM, SecureEasySetup, and the SecureEasySetup logo are trademarks or registered trademarks of Broadcom Corporation in the United States and/or other countries.





Wireless Nd1 Access Point:



User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

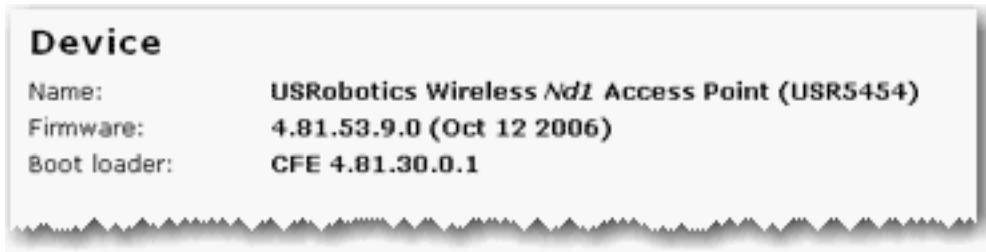
Access Point Status Information

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 the most current information.



Device



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

Wireless



This displays information on your wireless network settings, including the following:

- **Wireless mode:** Displays the mode the access point is currently functioning in, either **Access Point**, **Bridge Mode**, **Range Extender** or **Infrastructure**. This

can be configured from the [Wireless](#) page.

- **Network name:** Displays the Network name of the access point that is broadcast for wireless connections. This can be configured from the [Wireless](#) page.
- **Broadcast name:** Displays the whether the broadcasting of the network name is **Enabled** or **Disabled**. This can be configured from the [Wireless](#) page.
- **Channel:** Displays the current channel your access point is using, and any side channel information in parentheses.

Note: If the WDS channel of the networking device that the access point is connected to changes, the [Status](#) page will continue to show the old channel information for the access point. Although the **Network** list on the [Wireless](#) page will display the selected network and the correct channel, the change has not yet been applied to the access point. To update the channel information on the access point, click **Save** at the bottom of the [Wireless](#) page.

- **MAC address:** Displays the wireless (WLAN) MAC address of the access point.
- **WDS restrictions:** Displays the status of [WDS restrictions](#) on the access point, either **Enabled** or **Disabled**.
- **Access Points(s)** (Bridge and Range Extender modes only): Displays the MAC address of the networking device to which the Wireless **Nd₁** Access Point is connected.
- **Associated network** (Infrastructure mode only): Displays the network name for the network to which the Wireless **Nd₁** Access Point is connected.

Security

This section displays the current wireless security settings for your access point.



- **Method:** The security method and security settings (**Encryption, Pass phrase, Key**, etc.) for your access point. This information can be configured from the [Wireless](#) page.
- **Encryption:** The security method and security settings (**Encryption, Pass phrase, Key**, etc.) for your access point. This information can be configured from the [Wireless](#) page.
- **Pass Phrase:** The security method and security settings (**Encryption, Pass phrase, Key**, etc.) for your access point. This information can be configured from the [Wireless](#) page.
- **Wireless MAC filter:** Displays whether the wireless MAC Filter is **Enabled** or **Disabled** on your network. This information can be configured from the [Wireless](#) page.

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 timeframe before the lease will expire for the connected device.
- **Authorized:** If the client is authorized to connect to this gateway, the status will display as **Yes**. If the client is not authorised to connect to the gateway, the status will display as **No**.
- **WMM Link:** If the client supports WMM, the status will display as **Yes**. If the client does not support WMM, the status will display as **No**.
- **Power Save:** If the client is running in Power Save mode, the status will display as **Yes**. If the client is not in Power Save mode, the status will display as **No**.





USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

Security Settings

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

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:

This displays the current user name and password assigned to the access point. To change your user name and/or password, enter the new user name and password and click **Save** at the bottom of the page. You will need to log in to your access point with the new user name and password.

Password Rules:

1. The Wireless **Nd₁** access point lets you set a password up to 15 characters long. The most secure passwords are usually between 8 and 15 characters long.
2. The access point will allow you to 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.

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.)

Allow Current Clients 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 ▼

The access point configuration pages let you configure access to the access point based on MAC addresses by using the **Allow Current Clients** button or specify a level of filter to apply:

- Click **Allow Current Clients** to allow all of the wireless clients currently connected to the access point to be allowed access to the access point in the future. By default, the filter setting of **Allow only these devices** will then be applied.
- **Allow all 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: You need to click **Save** to save all your new settings and reboot the access point after you have completed all your changes.





USRobotics®

Wireless Nd1 Access Point:

User Guide

- **Home**
 - **Installation**
 - **Configuration**
 - **Tutorials**
 - **Help**
-

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**.

- **Dynamic:** Select this option if your access point will obtain an IP address from a DHCP server on the network.
- **Static:** Select this option if the access point to have a specific IP address or your network cannot assign an IP address using DHCP. Enter your new **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.



© 2005-2006 U.S. Robotics Corporation



USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

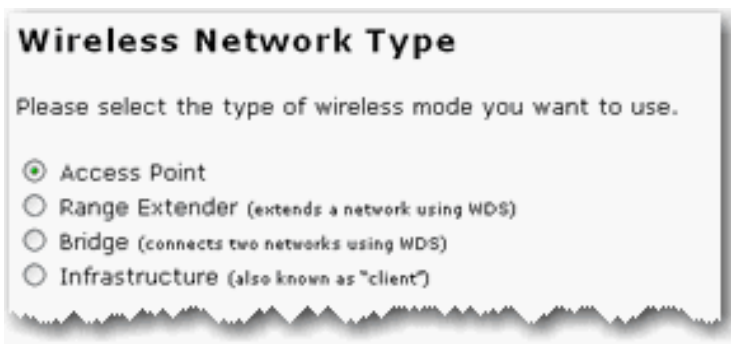
Wireless Settings

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.

Note: Depending on your settings, some items may not appear on your access point configuration pages for options that your connection does not support.

Wireless Network Type

Select the wireless network type for the access point to run.



- **Access Point:** Select this option if you will be using the access point as a traditional access point.
- **Range Extender:** Select this option if you will be using the access point to extend the range of an existing network.
- **Bridge:** Select this option if you will be using the access point to connect two WDS networks together.
- **Infrastructure:** Select this option if you will be using the access point to connect a computer or other networking device to an existing wireless network.

Broadcast Network Name



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.

Access Point Isolation

If the access point will be used in a public place where you do not want any wireless clients to be able to share files or printers between themselves, select **Access point isolation**. With this selected, all of the wireless clients will only be able to access the Internet. An example of a situation where you would want to enable this feature is in a public hotspot, such as a coffee shop or hotel. This feature is disabled by default.



Network

Select the network that the access point should connect to.

Network

Please select a wireless network (an access point or wireless router) from the list of detected networks. If the access point isn't broadcasting its network name, it won't be in the list; in that case, enter its network name in the field below.

Network Name	WDS	Strength	Wireless MAC Address	Channel
☒ USR5464_SES_23314	✓	78%	00:0C:29:00:00:00	1
☐ USR Internal	?	76%	00:0C:29:00:00:00	1
☐ USR5464	✓	66%	00:0C:29:00:00:00	1
☐ USR5453 my settings	?	70%	00:0C:29:00:00:00	6
☐ MINIVIPER01	✓	75%	00:0C:29:00:00:00	11
☐ SW735_5462	?	58%	00:0C:29:00:00:00	11
☐ USR9113_SES_51079	✓	63%	00:0C:29:00:00:00	11
☐ USR5454	?	—		1

Scan

If the network is not in the list, click **Scan** to perform a site scan and refresh your network list, or manually enter the **Network Name**, **Wireless MAC address** and select the **Channel** for the network you want to connect to, then select that network.

Network Name (SSID)

Note: If you used SecureEasySetup to configure your wireless security settings, changing the **Network Name** or other security settings for your access point will cause your connected wireless clients to lose connectivity with the access point.

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:

The default **Network name** of the access point is USR5464. If you want to use multiple Wireless **Nd₁** access points independently, you must configure a unique Network name for each access point.

Note: If you are using multiple Wireless **Nd₁** access points and you want them to use independently, each access point will need a unique Network name.

Security

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.

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

Note: For your wireless security settings, it is recommended that you select the **WPA2 and WPA (PSK)** or **WPA2 and WPA with 802.1x (RADIUS)** wireless security method using **TKIP and AES** encryption for the most secure wireless network.

Select the encryption **Method** that you want the wireless network to use. You can select from the following methods and enter the pass phrase or key:

- **WPA2 and WPA (PSK):** You need to set your **Encryption** type to **TKIP and AES, AES, or TKIP**. You will then need to 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 in length. This pass phrase must be the same on each computer that is connected to the wireless network. You can also specify a **Key rotation**, in seconds, or enter **0** in the field to disable the option.
- **WPA2 (PSK):** You need to set your **Encryption** type to **AES or TKIP**. You will then need to 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 in length. This pass phrase must be the same on each computer that is connected to the wireless network.
- **WPA (PSK):** You need to set your **Encryption** type to **TKIP and AES, AES, or TKIP**. You will then need to 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 in length. This pass phrase must be the same on each computer that is connected to the wireless network.

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 assign the access point WPA (PSK) security

with the **TKIP and AES** encryption to cover both AES and TKIP clients.

- **WEP open:** You need to set your **Key type** to **128-bit ASCII, 128-bit hex, 64-bit ASCII** or **64-bit hex**. Then, enter the **Key** (which is also commonly called a *Network key*). The 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.
- **WEP shared:** You need to set your **Key type** to **128-bit ASCII, 128-bit hex, 64-bit ASCII** or **64-bit hex**. Then, enter the **Key** (which is also commonly called a *Network key*). The 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.
- **WPA2 and WPA with 802.1x (RADIUS):** You need to set your **Encryption** type to **TKIP and AES, AES** or **TKIP**. Then you need to enter the **RADIUS server** IP address and **RADIUS Port**. You will then need to enter the **RADIUS key**.
- **WPA2 with 802.1x (RADIUS):** You need to set your **Encryption** type to **TKIP and AES, AES** or **TKIP**. Then you need to enter the **RADIUS server** IP address and **RADIUS Port**. You will then need to enter the **RADIUS key**.
- **WPA with 802.1x (RADIUS):** You need to set your **Encryption** type to **AES** or **TKIP**. Then you need to enter the **RADIUS server** IP address and **RADIUS Port**. You will then need to enter the **RADIUS key**.

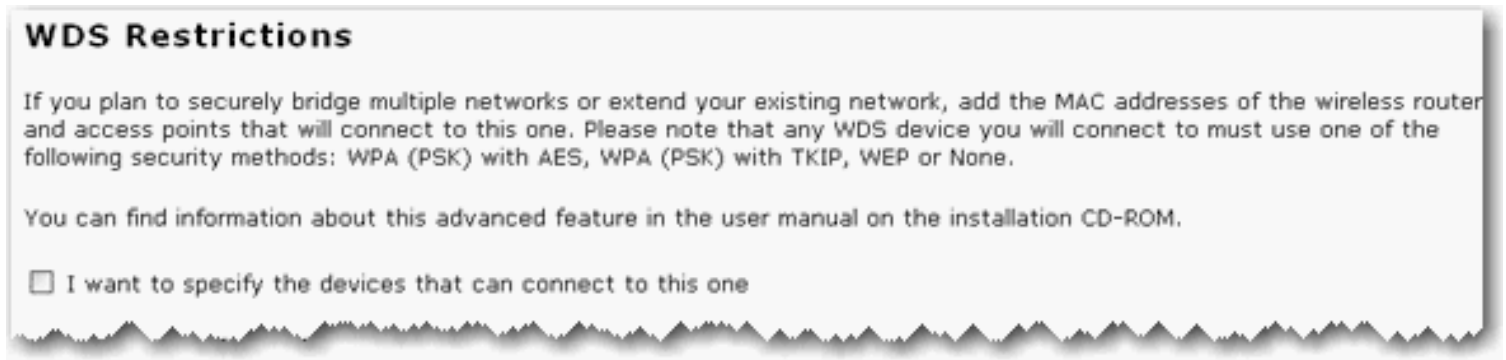
Note: Not all wireless clients support AES encryption when using WPA (PSK) security. TKIP encryption with WPA is supported by most wireless clients.

- **None:** This 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.

WDS Restrictions

USRobotics routers and access points are capable of using a feature known as WDS (Wireless Distribution System) which allows the wireless router or access point to connect directly to another wireless router or access point, while still allowing wireless clients to connect to the network.

A screenshot of a software window titled "WDS Restrictions". The window has a light gray background and a dark gray border. Inside, there is a paragraph of text explaining the WDS feature and its security requirements. Below this text is another line of text providing a reference to the user manual. At the bottom, there is a checkbox followed by the text "I want to specify the devices that can connect to this one". The bottom of the window features a decorative, jagged, mountain-like border.

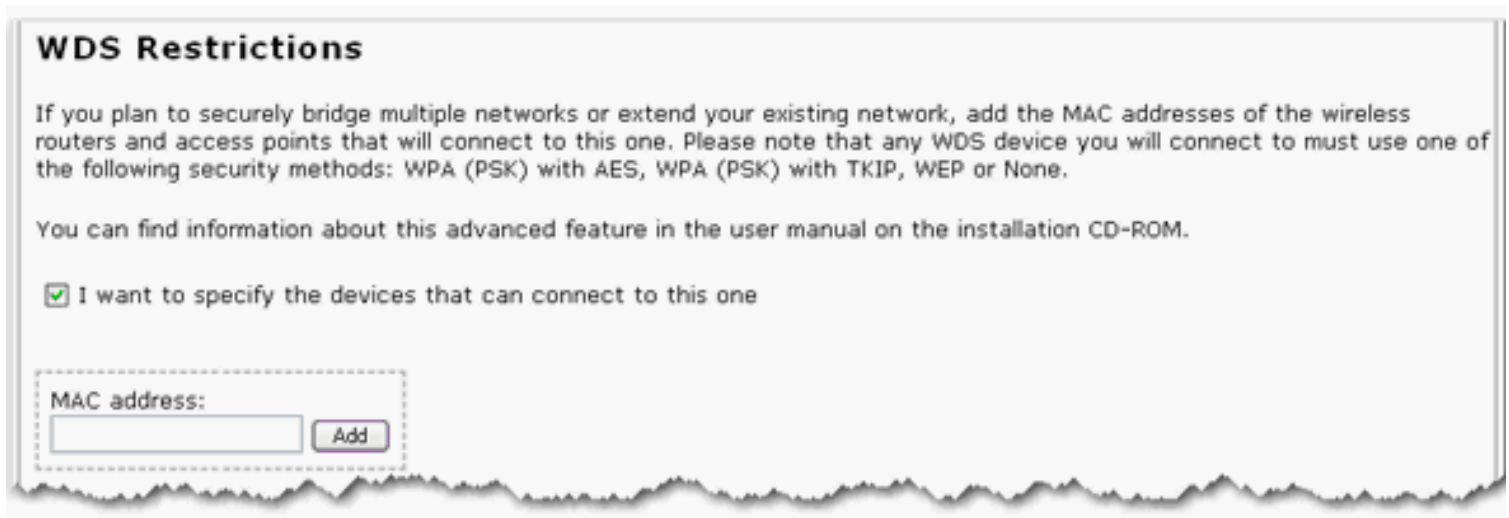
WDS Restrictions

If you plan to securely bridge multiple networks or extend your existing network, add the MAC addresses of the wireless router and access points that will connect to this one. 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.

☐ I want to specify the devices that can connect to this one

If you select **I want to specify the devices that can connect to this one**, you will need to enter the MAC addresses of the wireless routers or access points that will connect to this access point and click the **Add** button.



WDS Restrictions

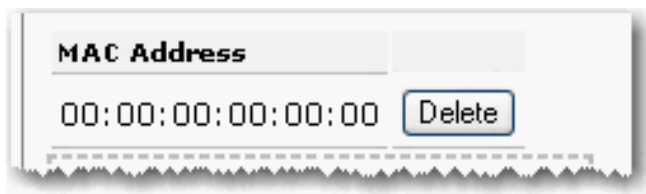
If you plan to securely bridge multiple networks or extend your existing network, add the MAC addresses of the wireless routers and access points that will connect to this one. Please note that any WDS device you will connect to must use one of the following security methods: WPA (PSK) with AES, WPA (PSK) with TKIP, WEP or None.

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

☒ I want to specify the devices that can connect to this one

MAC address:

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



MAC Address
00:00:00:00:00:00 Delete

WDS allows you to use multiple access points or wireless routers to connect several separate networks together. By connecting an access point or wireless router to each network and enabling the WDS feature, the wireless clients in the immediate area will be able to connect to the wireless network while a bridge would also be created to another access point or wireless router that is further away. The wireless access point and the wireless product that you will be creating a bridge with will need to have the same channel selected, the same **Network Name** (SSID), same wireless security settings, as well as the MAC address of the other device entered in the WDS Restrictions table. Enabling the WDS Restrictions option allows you to enter the MAC addresses of the access points or wireless routers that will be capable of connecting to each point of the wireless network that you have created. This will then limit exactly who has access to the wireless network.

One thing to note about this type of wireless network is that the throughput may be reduced for the bridging portion. Therefore, bridged routers or access points that also allow wireless clients to connect to the network should not be used for high-volume traffic. Some examples of the type of situations where you might want this type of network would be for security cameras, to provide network access to certain parts of a building that might not be able to be connected using wires, or to provide short-term network access to a conference area.

If you enable **Bridge mode** and **WDS Restrictions** in the wireless access point, a bridge will be created to another wireless router or access point and no wireless clients will be able to connect to the wireless network. This is generally used when you want to connect two networks that are in different buildings. Each wireless router or access point will have to have the MAC address of the other device entered in the WDS Restrictions table.

The access point's WDS connections do not support: **WPA2 (PSK)** or any of the **RADIUS** security methods, nor **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 **Enable 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.



If you enable WMM, you can then select **Enable 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.

Wi-Fi Multimedia (WMM)

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

- ☒ Enable WMM
- ☒ Enable no-acknowledgement
- ☒ Enable APSD (Automatic Power Save Delivery)

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: 802.11n mode does not support WMM, and the **Acceleration** option **MAXg (125 Mbps)** is incompatible with WMM. You must change the **802.11n mode** to **Off** and set the **Acceleration** option to **54g+ (Xpress™)** to enable WMM.

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.

Control and Extension Channels

Control and the secondary extension channels are only applicable if your access point is operating at 40 MHz bandwidth and the **802.11n mode** is configured as **Automatic**.

For US channels:

Control Channel	Sideband	Extension Channel
1 - 7	Lower	Channel number + 4
5 - 11	Upper	Channel number - 4

For European channels:

Control Channel	Sideband	Extension Channel
1 - 9	Lower	Channel number + 4
5 - 13	Upper	Channel number - 4

Example: If your control channel is set to 1, the extension channel will be transmitted on channel 5. The total bandwidth of the signals on channel 1 and 5 equals 40 MHz.

Example: If your control channel is set to 11, the extension channel will be transmitted on channel 6. The total bandwidth of the signals on channel 11 and 7 equals 40 MHz.

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%

Control channel: 11

802.11n mode: Automatic

Bandwidth: 20 MHz

Sideband for control channel: Lower

NPHY rate: Automatic

☒ Automatic 802.11n protection

Basic rate set: Default

Acceleration: 54g+ (XPress)

☐ Enable VLAN priority mode

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

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

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

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

Preamble: Long

- 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**.
- Power level:** Select either 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.
- Control channel:** Sets the channel on which the access point operates. If you are experiencing interference or wireless network problems, changing the channel may solve the issue. It is recommended that you keep the control channel set at "Automatic" to avoid interference with adjacent networks.

- **802.11n mode:** You can select **Automatic**, or **Off**. **Automatic** enables 802.11n support, and **Off** will disable 802.11n support.
- **Bandwidth:** Specify radio frequency bandwidth, either **20MHz** or **40MHz** (dual channel), that the access point will use if **802.11n mode** is configured as **Automatic**. If the access point detects other adjacent wireless networks, it will use 20 MHz operation so as to not interfere with the networks. If there no other adjacent networks are detected, the access point will use 40MHz operation.

In both 20 MHz and 40 MHz operation, when the **802.11n mode** is configured to **Automatic**, the router will use dynamic channel selection to determine the best channels to transmit in order for optimal operation.

- **Sideband for control channel mode:** Displays which sideband the access point is using for the control channel, either **Upper** or **Lower**. Sideband channels are only applicable if your access point is operating at 40 MHz bandwidth and the **802.11n mode** is configured as **Automatic**.
- **NPHY rate:** Set the Physical Layer (NPHY) rate. These rates are only applicable when the **802.11n mode** is configured as **Automatic**.
- **Automatic 802.11n 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 802.11 performance will be maximized under most conditions while the other 802.11 modes (802.11b, etc.) will be secondary.
- **Legacy rate:** Set the Physical Layer rate. This option is only visible when **802.11n mode** is turned **Off**.
- **Basic rate set:** Select the basic rate that wireless clients must support, either **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. Set the mode to **None** if you are experiencing difficulty with legacy 802.11b/g equipment. **MAXg (125 Mbps)** will only work with *MAXg* wireless clients.
- **Enable VLAN priority mode:** When selected, the access point will advertise packet priority using the VLAN tag.

- **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 RTS Threshold is 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 the access point will reach when sending information in packets before the packets are broken up in 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 level that the Fragmentation threshold is set to, 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:** This parameter configures 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 which 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.



© 2005-2006 U.S. Robotics Corporation

**USRobotics®****Wireless Nd1 Access Point: User**

Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

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

Reboot Access Point

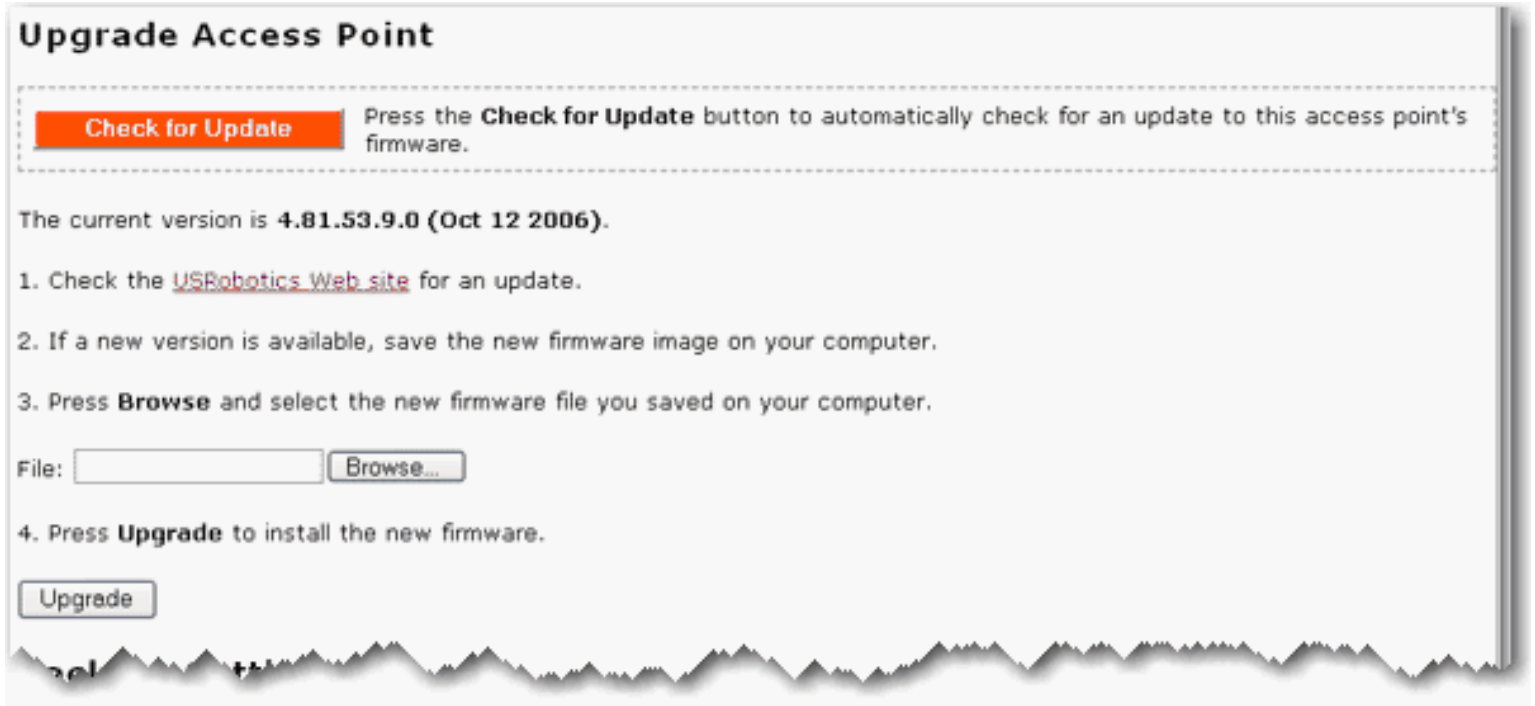
Click Reboot if you need to restart the access point. Its current settings will be retained.

Reboot

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.

The screenshot shows a web interface titled "Upgrade Access Point". At the top, there is a red button labeled "Check for Update" and a text instruction: "Press the **Check for Update** button to automatically check for an update to this access point's firmware." Below this, it states "The current version is **4.81.53.9.0 (Oct 12 2006)**." A list of instructions follows: 1. Check the [USRobotics 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. Below the instructions, there is a "File:" label, an empty text box, and a "Browse..." button. The final instruction is: 4. Press **Upgrade** to install the new firmware. At the bottom, there is an "Upgrade" button. The interface has a light gray background with a decorative wavy line at the bottom.

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.



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](#).

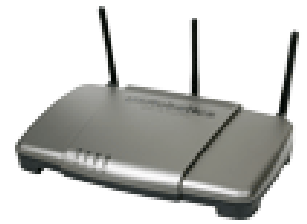
Factory Settings

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.



© 2005-2006 U.S. Robotics Corporation



USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

Configuring the Access Point as an Access Point

By default, the Wireless **Nd₁** Access Point is configured as an access point. If you are using a Windows operating system and have followed the installation instructions in this guide, your basic configuration is complete.



© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point: User Guide

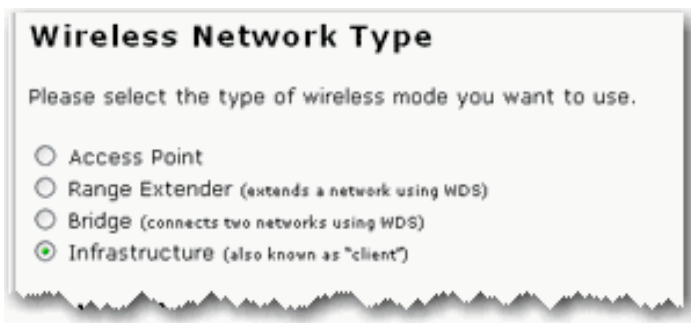


- Home
- Installation
- Configuration
 - Tutorials
 - Help

Configuring the Access Point as a Client

For Bridge mode, you must be using a wireless router or access point that supports WDS (Wireless Distribution System). If you select Infrastructure mode, you will be able to select either WPA2 PSK (AES), WPA2 PSK (TKIP), WPA PSK (AES), WPA PSK (TKIP), WEP Open, or WEP Shared for the encryption method.

1. If you have not installed your access point, complete the [installation](#) procedure.
2. Type the IP address of your access point in your Web browser's location or address line and press ENTER.
3. When prompted, enter your login and password for the access point and press ENTER.
4. Click the **Wireless** tab.
5. For the **Wireless Network Type**, select **Infrastructure**.



6. Next you will need to select the **Network Name** (SSID) of the wireless network device to

which you will be connecting the Bridge. If you do not see the **Network Name** (SSID) of the appropriate wireless network device, click **Scan** to search the area again.

Network

Please select a wireless network (an access point or wireless router) from the list of detected networks. If the access point isn't broadcasting its network name, it won't be in the list; in that case, enter its network name in the field below.

Network Name	WDS	Strength	Wireless MAC Address	Channel
☒ USR5464_SES_23314	✓	78%	08:00:27:00:00:00	1
☐ USR Internal	🔒 ?	76%	08:00:27:00:00:00	1
☐ USR5464	🔒 ✓	66%	08:00:27:00:00:00	1
☐ USR5453 my settings	?	70%	08:00:27:00:00:00	6
☐ MINIVIPER01	✓	75%	08:00:27:00:00:00	11
☐ SW735_5462	?	58%	08:00:27:00:00:00	11
☐ USR9113_SES_51079	🔒 ✓	63%	08:00:27:00:00:00	11
☐ USR5454	?	—		1

If the appropriate network device does not appear or if that device is not broadcasting its **Network Name** (SSID), manually enter the information for the network device. You will need to enter the **Network Name**, the **Wireless MAC Address**, and select the **Channel** of the existing wireless network.

- Next, you will need to select the security **Method** and enter the **Pass phrase** or the **Key** (depending on if you selected WPA PSK or WEP). These settings must match the security information of the wireless network device to which you are connecting the access point. Bridge mode only supports WPA2 in Infrastructure mode.

Security

Method:

Encryption:

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

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

- Select or enter any required **Transmission** settings that you will need to connect to the wireless network device.
- Click **Save** at the bottom of the page.



© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point: User Guide

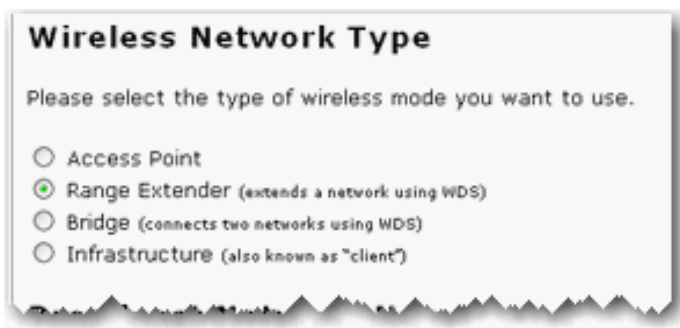


- **Home**
- **Installation**
- **Configuration**
 - **Tutorials**
 - **Help**

Configuring the Access Point as a Range Extender

You must be using a wireless router or access point that supports WDS (Wireless Distribution System). If you are using WPA as an encryption method in your wireless network, you must be using either TKIP or AES, not a combination, since the Range Extender only supports one or the other.

1. If you have not installed your access point, complete the [installation](#) procedure.
2. Type the IP address of your access point in your Web browser's location or address line and press ENTER.
3. When prompted, enter your login and password for the access point and press ENTER.
4. Click the **Wireless** tab.
5. For the **Wireless Network Type**, select **Range Extender**.



6. Select your [Broadcast Network Name](#) and [Access Point Isolation](#) options and enter any required settings.

7. Next you will need to select the **Network Name** (SSID) of the wireless network device to which you will be connecting the Bridge. If you do not see the **Network Name** (SSID) of the appropriate wireless network device, click **Scan** to search the area again.

Network

Please select a wireless network (an access point or wireless router) from the list of detected networks. If the access point isn't broadcasting its network name, it won't be in the list; in that case, enter its network name in the field below.

Network Name	WDS	Strength	Wireless MAC Address	Channel
☒ USR5464_SES_23314	✓	78%	08:00:27:00:00:00	1
☐ USR Internal	🔒 ?	76%	08:00:27:00:00:00	1
☐ USR5464	🔒 ✓	66%	08:00:27:00:00:00	1
☐ USR5453 my settings	? 70%	70%	08:00:27:00:00:00	6
☐ MINIVIPER01	✓ 75%	75%	08:00:27:00:00:00	11
☐ SW735_5462	? 58%	58%	08:00:27:00:00:00	11
☐ USR9113_SES_51079	🔒 ✓ 63%	63%	08:00:27:00:00:00	11
☐ USR5454	? —	—		1 ▾

For Range Extender mode, the list of networks is based on this access point's wireless radio scan. The channel information may be different on the peer WDS device.

If the appropriate network device does not appear or if that device is not broadcasting its **Network Name** (SSID), manually enter the information for the network device. You will need to enter the **Network Name**, the **Wireless MAC Address**, and select the **Channel** of the existing wireless network.

8. Next, you will need to select the security **Method** and enter the **Pass phrase** or the **Key** (depending on if you selected WPA PSK or WEP). These settings must match the security information of the wireless network device to which you are connecting the access point. Bridge mode only supports WPA2 in Infrastructure mode.

Security

Method:

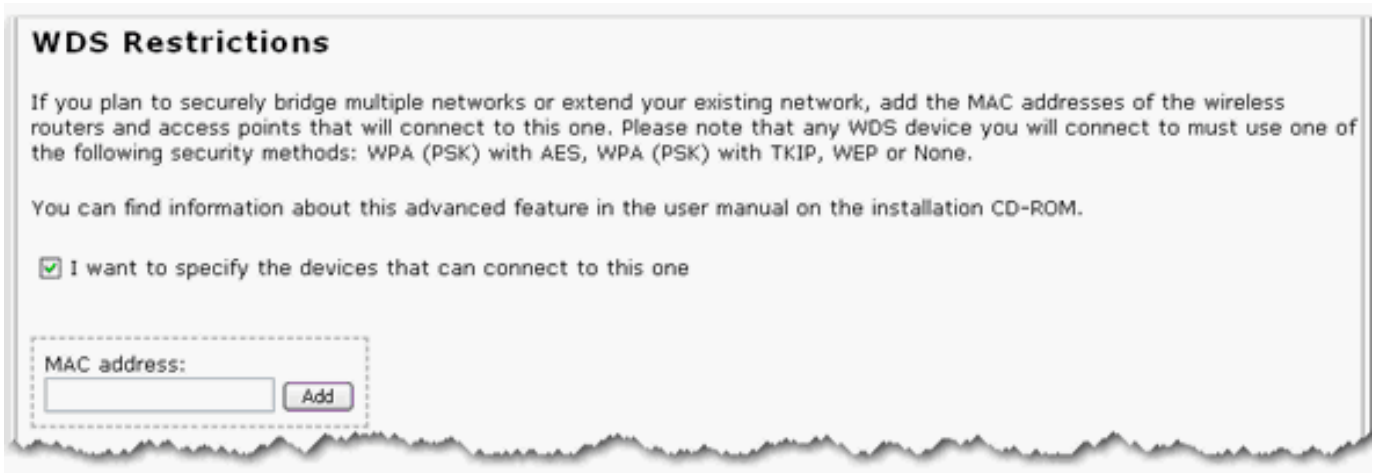
Encryption:

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

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

9. If other bridges will be connecting to this access point, select the checkbox next to **I want to specify the devices that can connect to this one** under **WDS Restrictions**. You will then need to enter the wireless **MAC address** of each new Bridge you will be connecting to this one and then click **Add**. By default, this feature is disabled. USRobotics recommends that you only

add one more Bridge in this fashion. If you add more than one Bridge in a chain, you will begin to lose network quality and speed.



WDS Restrictions

If you plan to securely bridge multiple networks or extend your existing network, add the MAC addresses of the wireless routers and access points that will connect to this one. 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.

☒ I want to specify the devices that can connect to this one

MAC address:

Note: If the WDS channel of the networking device that the access point is connected to changes, the [Status](#) page will continue to show the old channel information for the access point. Although the **Network** list on the [Wireless](#) page will display the selected network and the correct channel, the change has not yet been applied to the access point. To update the channel information on the access point, click **Save** at the bottom of the [Wireless](#) page.

10. Select or enter any required [Transmission](#) settings that you will need to connect to the wireless network device.
11. Click **Save** at the bottom of the page.





Wireless Nd1 Access Point: User Guide



- Home
- Installation
- Configuration
 - Tutorials
 - Help

Configuring the Access Point as a Bridge

For access point in Bridge mode, you must be using a wireless router or access point that supports WDS (Wireless Distribution System). If you select Bridge mode, you will be able to select either WPA PSK (AES), WPA PSK (TKIP), WEP Open, or WEP Shared for the encryption method.

Note: When you select a wireless router or access point to which you want to connect, make sure you choose one that supports WDS.

1. If you have not installed your access point, complete the [installation](#) procedure.
2. Type the IP address of your access point in your Web browser's location or address line and press ENTER.
3. When prompted, enter your login and password for the access point and press ENTER.
4. Click the **Wireless** tab.
5. For the **Wireless Network Type**, select **Bridge**.

Wireless Network Type

Please select the type of wireless mode you want to use.

- ☐ Access Point
- ☐ Range Extender (extends a network using WDS)
- ☒ Bridge (connects two networks using WDS)
- ☐ Infrastructure (also known as "client")

6. Next you will need to select the **Network Name** (SSID) of the wireless network device to which you will be connecting the Bridge. If you do not see the **Network Name** (SSID) of the appropriate wireless network device, click **Scan** to search the area again.

Network

Please select a wireless network (an access point or wireless router) from the list of detected networks. If the access point isn't broadcasting its network name, it won't be in the list; in that case, enter its network name in the field below.

Network Name	WDS	Strength	Wireless MAC Address	Channel
☒ USR5464_SES_23314	✓	78%	88:27:EB:46:54:64	1
☐ USR Internal	🔒 ?	76%	88:27:EB:46:54:64	1
☐ USR5464	🔒 ✓	66%	88:27:EB:46:54:64	1
☐ USR5453 my settings	? 70%	88:27:EB:46:54:64	6	
☐ MINIVIPER01	✓ 75%	88:27:EB:46:54:64	11	
☐ SW735_5462	? 58%	88:27:EB:46:54:64	11	
☐ USR9113_SES_51079	🔒 ✓ 63%	88:27:EB:46:54:64	11	
☐ USR5454	? —		1	

For Bridge mode, the list of networks is based on this access point's wireless radio scan. The channel information may be different on the peer WDS device.

If the appropriate network device does not appear or if that device is not broadcasting its **Network Name** (SSID), manually enter the information for the network device. You will need to enter the **Network Name**, the **Wireless MAC Address**, and select the **Channel** of the existing wireless network.

7. Next, you will need to select the security **Method** and enter the **Pass phrase** or the **Key** (depending on if you selected WPA PSK or WEP). These settings must match the security information of the wireless network device to which you are connecting the access point. Bridge mode only supports WPA2 in Infrastructure mode.

Security

Method: WPA2 and WPA (PSK) (recommended) ▼

Encryption: TKIP and AES (recommended) ▼

Pass phrase: phazhvd0skd7z9n
(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.)

8. If other Bridges will be connecting to this access point, select the checkbox next to **I want to specify the devices that can connect to this one** under **WDS Restrictions**. You will then need to enter the wireless **MAC address** of each new Bridge you will be connecting to this one and then click **Add**. By default, this feature is disabled. USRobotics recommends that you only add one more Bridge in this fashion. If you add more than one Bridge in a chain, you will begin to lose network quality and speed.

WDS Restrictions

If you plan to securely bridge multiple networks or extend your existing network, add the MAC addresses of the wireless routers and access points that will connect to this one. 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.

☒ I want to specify the devices that can connect to this one

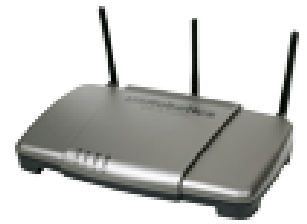
MAC address:

Note: If the WDS channel of the networking device that the access point is connected to changes, the **Status** page will continue to show the old channel information for the access point. Although the **Network** list on the **Wireless** page will display the selected network and the correct channel, the change has not yet been applied to the access point. To update the channel information on the access point, click **Save** at the bottom of the **Wireless** page.

9. Select or enter any required **Transmission** settings that you will need to connect to the wireless network device.
10. Click **Save** at the bottom of the page.



© 2005-2006 U.S. Robotics Corporation



USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

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 you are receiving power and that all 4 LEDs are lit.
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 following settings on the connected device match those of the access point.
 - Mode (must be Infrastructure mode)

- Network name or SSID
- Security type and key, psk, or passphrase.

Refer to your wireless adapter'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 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 Network Device Locator does not find the Wireless **Nd₁** Access Point.](#)

[SecureEasySetup did not configure my wireless client.](#)

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

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

I am no longer able to access the Internet.

My client does not establish a wireless connection to the Wireless **Nd₁** 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

In bridge mode, the access point will not connect to another networking device.

In range extender mode, the access point will not connect to another networking device.



© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point:



User Guide

- **Home**
 - **Installation**
 - **Configuration**
 - **Tutorials**
 - **Help**
-

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 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](#)



© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point:



User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

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 **Nd₁** 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 5 to 10 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](#)



© 2005-2006 U.S. Robotics Corporation



USRobotics® Wireless N1 Access Point:

User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

My client does not establish a wireless connection to the Wireless N₁ Access Point after I changed the settings.

In the configuration utility for your wireless adapter:

1. Ensure that you are connecting to the Wireless N1 Access Point by verifying the WLAN MAC address.
2. Ensure that the same encryption options, and their passphrase or key, are used on both the wireless adapter and the access point. If you change the setting on the access point, you must also change the settings of every wireless adapter that is intended to connect to the access point.

[Return to Troubleshooting page](#)



© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point:



User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

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](#)



© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point:



User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

The Network Device Locator does not find the Wireless Nd₁ 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 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](#)





© 2005-2006 U.S. Robotics Corporation



USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

SecureEasySetup did not configure my wireless client.

Press the SecureEasySetup button on the back of the access point for one full second and then release it. Verify that the SecureEasySetup LED on the front of the access point starts blinking before initiating SecureEasySetup in the client utility for your wireless adapter.

[Return to Troubleshooting page](#)





Wireless Nd1 Access Point:



User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

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 Nd1 Access Point:



User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

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 connectivity issue. See ["For wireless connections"](#) in the basic troubleshooting procedure.

If you cannot access the configuration pages with a wired connection, 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 5 to 10 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 Nd1 Access Point:

User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

My client cannot achieve 270 Mbps connections.

Make sure the wireless products you are using to connect to the Wireless **Nd₁** Access Point support 270 Mbps speeds and that the Wireless **Nd₁** Access Point is connected to a networking device that supports 270 Mbps speeds.

[Return to Troubleshooting page](#)





USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

In bridge mode or range extender mode, the access point will not connect to another networking device.

Solution:

If the WDS channel of the networking device that the access point is connected to changes, the **Status** page will continue to show the old channel information for the access point. Although the **Network** list on the **Wireless** page will display the selected network and the correct channel, the change has not yet been applied to the access point. To update the channel information on the access point, click **Save** at the bottom of the **Wireless** page.

Make sure the access point is using the same required **Wireless** settings as the WDS peer, including the **Control channel** and **Bandwidth** settings (under **Transmission**), and the same wireless **Security** settings as the WDS peer.

[Return to Troubleshooting page](#)





© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point:



User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

The access point is not getting an IP address from the DHCP server.

Connect the access point is connected to a networking device before you connect the access point to power.

[Return to Troubleshooting page](#)





Wireless Nd1 Access Point:



User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

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 5 to 10 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

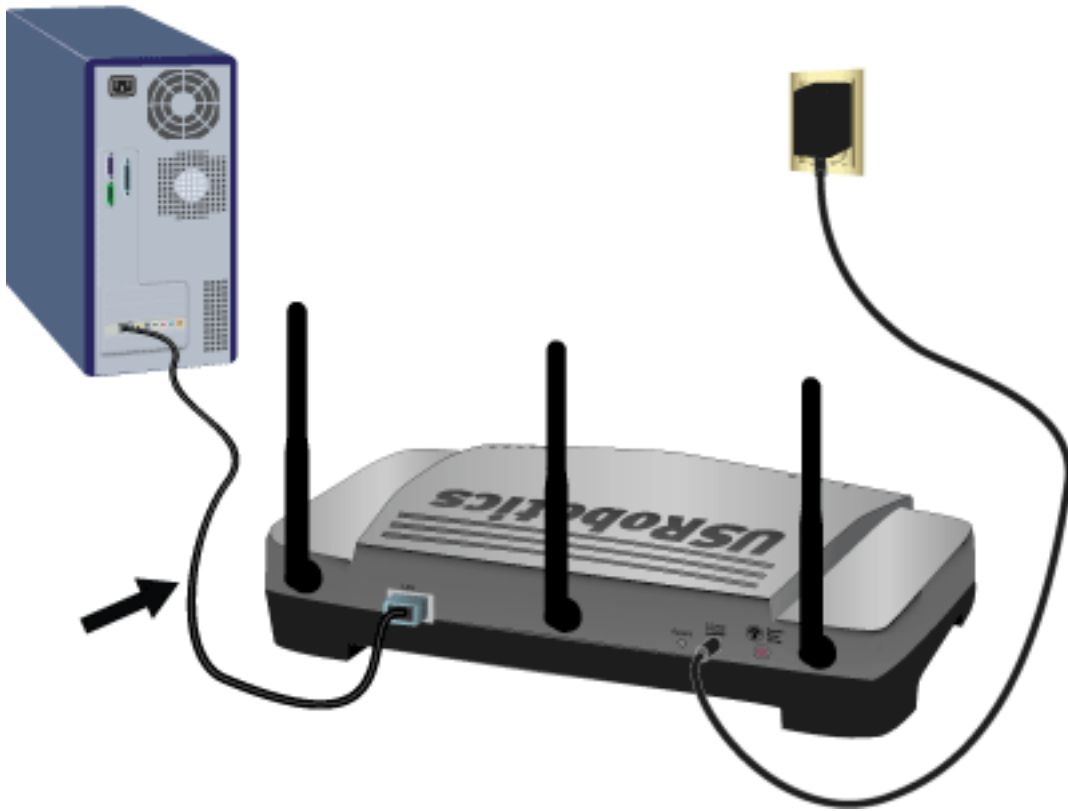
The firmware image may have been corrupted during the upgrade procedure. Try one of the following procedures to force the upgrade:

- **Windows XP, 2000, or NT users:** [perform this procedure](#).
- **Windows Me, 98, and 95 users:** [perform this procedure](#).

For Windows XP, 2000, and NT

Windows XP, 2000, and NT users can perform the following semi-automated upgrade procedure to install the firmware.

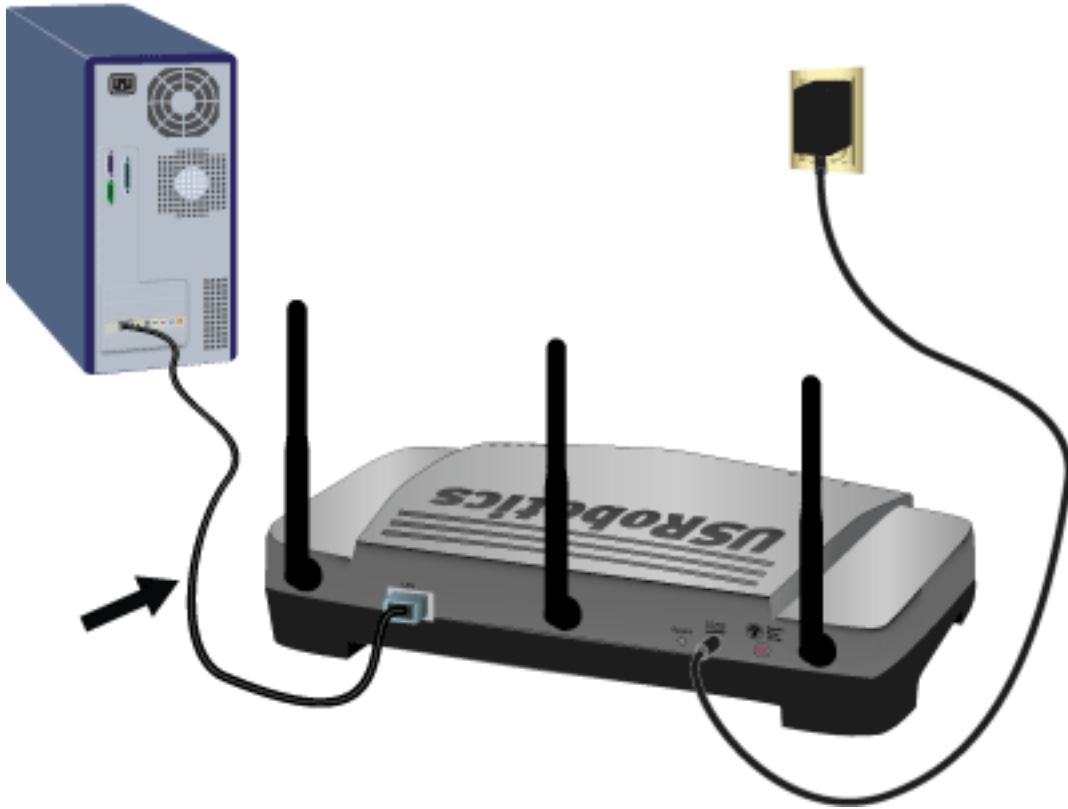
1. Use a networking cables to connect the access point directly to the computer. Do not try to use a wireless connection for this procedure.



2. Locate the folder that contains the firmware file that you downloaded.
3. On the USRobotics Installation CD-ROM, locate the Manual_Upgrade.cmd utility.
4. Drag the firmware file onto the Manual_Upgrade.cmd utility icon and follow the on-screen instructions.
5. Set IP addressing for the network adapter on the computer back to "Obtain an IP address automatically" as follows:
 - A. Open the **Control Panel** and double-click **Network Connections**.
 - B. Right-click the **Local Area Connection** of the network adapter that connects the computer to the networking device and select **Properties**.
 - C. On the **General** tab, select **Internet Protocol (TCP / IP)** and click **Properties**.
 - D. Select **Obtain an IP Address Automatically** and click **OK**.
 - E. Click **OK** again.

Windows XP, 2000, and NT users can also perform the following manual upgrade procedure:

1. Use a networking cables to connect the access point directly to the computer. Do not try to use a wireless connection for this procedure.



2. Determine the IP address to use for the access point:
 - A. If the most recent IP address of the access point was acquired dynamically, use **192.168.1.64**
 - B. If you assigned a static IP address to the access point, use the address that you assigned. If you cannot remember the IP address that you assigned, run the [Network Device Locator](#). As long as the access point is in the same subnet as the computer, the locator will find the access point.
3. On the Windows **Start** menu, select **Run**.
4. In the Run dialog box, type **cmd** and click **OK**.
5. Locate the folder that contains that firmware file that you downloaded.
6. 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\usr5454"
```

and then press ENTER.

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

tftp -i xxx.xxx.x.x put 5454.usr where xxx.xxx.x.x is the IP address of the access point.

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

9. Press ENTER.

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

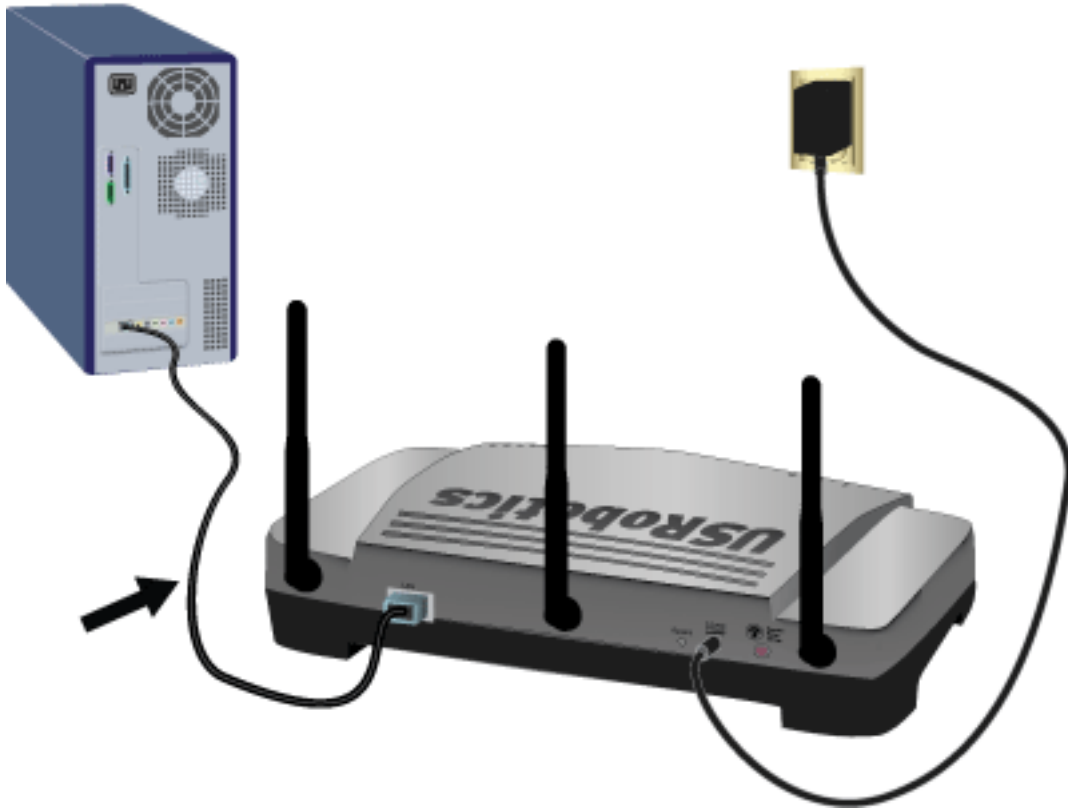
10. Wait for the upgrade to finish. When the wireless LED  turns on, the upgrade is done.
11. Set IP addressing for the wired network adapter to "Obtain an IP address automatically" as follows:
- A. Open the **Control Panel** and double-click **Network Connections**.
 - B. Right-click the **Local Area Connection** of the network adapter that connects the computer to the router and select **Properties**.
 - C. On the **General** tab, select **Internet Protocol (TCP / IP)** and click **Properties**.
 - D. Select **Obtain an IP Address Automatically** and click **OK**.
 - E. Click **OK** again.

[Return to Troubleshooting page](#)

For Windows Me, 98, and 95

Perform the following steps to manually install the access point's firmware:

1. Use a networking cables to connect the access point directly to the computer. Do not try to use a wireless connection for this procedure.



2. Determine the IP address to use for the access point:
 - A. If the most recent IP address of the access point was acquired dynamically, use **192.168.1.64**
 - B. If you assigned a static IP address to the access point, use the address that you assigned. If you cannot remember the IP address that you assigned, run the [Network Device Locator](#). As long as the access point is in the same subnet as the computer, the locator will find the access point.
3. On the desktop, right-click **Network Places** or **Network Neighborhood** and select **Properties**.
4. On the **Configuration** tab, select the network adapter that connects the computer to the router and click **Properties**.
5. Select **Use the following IP address**:

6. Specify a temporary static IP address for the computer's network adapter.

The IP address must be in the same subnet as the access point:

- If the access point was acquiring its address dynamically, set the IP address of your computer to 192.168.1.100.
- If you assigned a static IP address to the access point, match the first three parts of the IP address to the static address of the access point. For example, if the static address of the access point is 192.168.3.1, set the IP address of the computer to 192.168.3.100.

7. Click **OK**.

8. Click **OK** again.

9. Run the **Device Locator** to obtain the IP addresses of devices on your local network. Match the MAC address printed on the bottom of the access point to the addresses shown by the utility to find the access point's IP address.

10. On the Windows **Start** menu, click **Run**.

11. In the Run dialog box, type **command** and click **OK**.

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

13. 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\usr5454"
```

and then press ENTER.

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

```
tftp -i xxx.xxx.x.x put 5454.usr where xxx.xxx.x.x is the IP address of the access point.
```

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

16. Press ENTER.

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

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

[Return to Troubleshooting page](#)





Wireless Nd1 Access Point:



User Guide

- **Home**
 - **Installation**
 - **Configuration**
 - **Tutorials**
 - **Help**
-

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 all networking devices between the computer and 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.

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.](#)

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 computer 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](#)



© 2005-2006 U.S. Robotics Corporation



USRobotics® Wireless Nd1 Access Point: User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

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. Click Windows **Start > Run**.
2. In the **Run** dialog box:
 - **Windows XP, 2000, and NT users:** Type **cmd** and click **OK**.
 - **Windows Me, 98, and 95 users:** Type **command** and click **OK**.
3. 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.
4. Obtain IP information for your computer as follows:
 - **Windows 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

```

5. Type **Ping** followed by the IP address displayed in step 4 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 **Nd₁** Access Point, plug it back in, and reboot your computer.

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

If you can establish communication with the Wireless **Nd₁** 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.

7. Type **Ping** followed by the LAN IP address, which is the Default Gateway address displayed in step 4, and press ENTER.

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

8. 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.

9. Type **Ping** followed by the DNS server address displayed in step 4 and press ENTER.

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

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

Windows XP, 2000, or NT:

- A. Open the **Control Panel** and double-click **Network Connections**.

- B. Right-click the **Local Area Connection** of the network adapter that connects the computer to the networking device, select **Status**, and click **Details**.
- C. Note the IP addresses of the DNS servers.
- D. In the Network Connections window, right-click the **Local Area Connection** of the network adapter that connects the computer to the networking device and select **Properties**.
- E. On the **General** tab, select **Use the following DNS server addresses**, enter the IP addresses that you noted in step C, and click **OK**.
- F. Click **OK** again.

Windows Me, 98, or 95:

- A. Click Windows **Start > Run**.
- B. Type **command** and press ENTER.
- C. In the MS-DOS Prompt window, type **winipcfg /all** and press ENTER.
- D. Note the IP addresses of the primary and secondary DNS servers.
- E. On the desktop, right-click **Network Places** or **Network Neighborhood** and select **Properties**.
- F. On the **Configuration** tab, select the network adapter that connects the computer to the router and click **Properties**.
- G. On the **DNS Configuration** tab, click **Enable** and enter a **Host** name.
- H. In **DNS Server Search Order**, enter the IP address of the primary DNS server and click **Add**.
- I. In **DNS Server Search Order**, enter the IP address of the secondary DNS server and click **Add**.
- J. Click **OK**.
- K. Click **OK** again.

[Return to Troubleshooting page](#)





USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
- Installation
- Configuration
 - Tutorials
 - Help

Support

1. Know your model and serial number.

Your model number is 5454. 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.

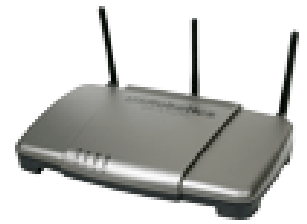
Country	Webmail	Voice
United States & Canada	http://www.usr.com/emailsupport	(888) 216-2850

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	800 979 266
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



© 2005-2006 U.S. Robotics Corporation



USRobotics® Wireless Nd1 Access Point:

User Guide

- Home
 - Installation
 - Configuration
 - Tutorials
 - Help
-

Frequently Asked Questions

Can I use SecureEasySetup to configure wireless security for the access point?

Yes. For the initial setup of the access point, refer to the [installation instructions](#).

1. Click the **SecureEasySetup** button on the back of the access point.
 2. Press the **SecureEasySetup** button in the utility for the client adapter. Your client adapter will display a message when the connection has been successfully completed.
-

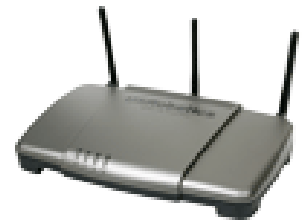
How do I restore the access point to its factory default settings?

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 5 to 10 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.





USRobotics® *Wireless Nd1 Access Point:*

User Guide

- **Home**
 - **Installation**
 - **Configuration**
 - **Tutorials**
 - **Help**
-

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

5454 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.

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 5454 is limited in CH1~11 from 2412 to 2462 MHz by specified firmware controlled in USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

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.

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 **Nd₁** Access Point, Model 5454, 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 **0.838** W/Kg.

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.





© 2005-2006 U.S. Robotics Corporation



Wireless Nd1 Access Point:



User Guide

- **Home**
 - **Installation**
 - **Configuration**
 - **Tutorials**
 - **Help**
-

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 User Guide.

Copyright © 2006 U.S. Robotics Corporation. All rights reserved. U.S. Robotics and the U.S. Robotics logo are registered trademarks of U.S. Robotics Corporation. Other product names are for identification purposes only and may be trademarks of their respective companies. Product specifications subject to change without notice.





Wireless Nd1 Access Point:



User Guide

- **Home**
 - **Installation**
 - **Configuration**
 - **Tutorials**
 - **Help**
-

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 caused 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

