

WRVS4400N FAQs

Document ID: 109207

Questions

- Introduction
- LEDs
- Security Supported
- Special Features
- Cisco ProtectLink
- Compatibility Concerns
- Related Information

Introduction

This article is one in a series to assist in the setup, troubleshooting, and maintenance of Cisco Small Business products.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Front Panel



Back Panel



Q. Where can I find the Admin Guide and Quick Start Guide for the WRVS4400N?

A. Visit the Cisco Small Business Routers Technical Documentation page.

Q. What is the WRVS4400N and what are some the features included?

A. The Cisco WRVS4400N is a Wireless-N Gigabit Security Router with VPN support. It comes equipped with a powerful Stateful Packet Inspection (SPI) firewall and, Intrusion Prevention System (IPS) technology to protect your Small Business PCs against intruders and most known Internet attacks. It can provide secure wireless network connectivity for your office with the latest wireless encryption methods. Its Virtual Private Network (VPN) function creates encrypted "tunnels" through the Internet so up to 5 remote users can securely connect to your office network from off-site using the QuickVPN software client, or allow users in your branch office to connect to the corporate network as if they are in the main office by creating up to 5 Gateway-to-Gateway tunnels between 2 or more WRVS4400N routers.

Q. What is the default IP address, username and password to log into the WRVS4400N?

A. The default IP address is **192.168.1.1**. The username is **admin**, and the password is **admin**. Simply open your web browser and enter **http://192.168.1.1** to access the web based graphical user interface inside the router.



Q. How can I reset the WRVS4400N to factory default settings?

A. Press and hold the **Reset** button on the back of the WRVS4400N for 10 seconds in order to reset the entire configuration back to the original default settings. You can also choose **Administration > Factory Defaults** from the web based user interface to perform this same action.

Q. What is the Warranty period length of the WRVS4400N?

A. The WRVS4400N comes with a 3 (three) year limited warranty. More information on the warranty can be found at http://www.cisco.com/en/US/docs/general/warranty/3year_SmallBusiness.html.

Q. Can I modify the default username and password on the WRVS4400N?

A. Yes*, by upgrading your WRVS4400N to the latest firmware you can modify the default username. You can also add additional user accounts to the WRVS4400N configuration.
*(This applies to the v1.0 and v1.1 hardware versions running firmware version 1.1.13. v2.0 hardware version running firmware 1.00.09).

Q. Does the built-in switch on the WRVS4400N support Power over Ethernet (PoE)?

A. No, the built-in switch on the WRVS4400N does not support PoE.

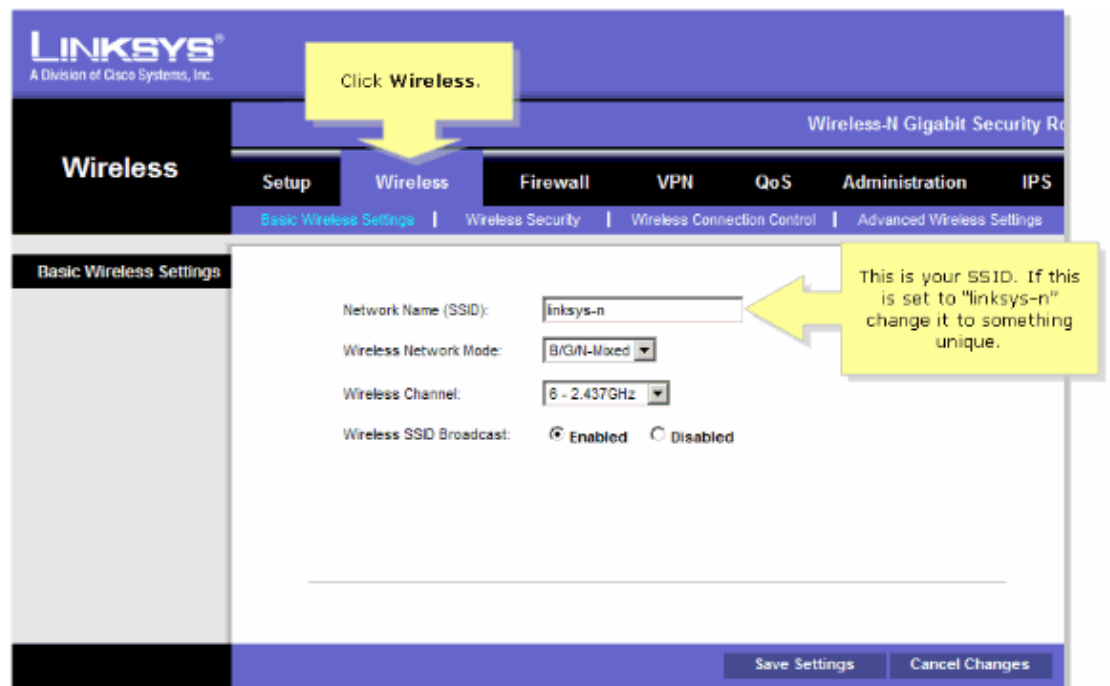
Q. Does the WRVS4400N support Quality over Service (QoS)? How many types of QoS does it support?

A. Yes. The WRVS4400N supports two types of QoS: Application-based QoS and Port-based QoS. The Application QoS setting and the Port-based QoS setting can be found under Menu > Submenu.

Q. How do I set up my wireless network SSID channel for a WRVS4400N that runs slow bandwidth?

A. In order to set up and improve your wireless network's signal, you can change your Wireless Network Name (SSID) and/or try using a different channel. Complete these steps:

1. Access the router's web-based setup page, such as Internet Explorer or Firefox.
2. Go to the Address bar and enter your router's IP Address **http://192.168.1.1**. Then, click **Enter**.
3. A new window prompts you for a username and password. Enter **admin** (this is the default username and password), then click **OK**.
4. When the router's web-based setup page appears, click **Wireless**.
5. Look for Wireless Network Name (SSID). If it is still set to linksys-n, change it to something unique. Then, click **Save Settings**.



6. After changing your SSID, try changing channels to get around interferences. Preferred channels to use are 1, 6 and 11 because these are considered non-overlapping channels.

LINKSYS
A Division of Cisco Systems, Inc.

Wireless N Gigabit Security Router

Wireless | Setup | Wireless | Firewall | VPN | QoS | Administration | IPS

Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings

Basic Wireless Settings

Network Name (SSID): linksys-n

Wireless Network Mode: B/G/N-Mixed

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ☒ Enabled ☐ Disabled

Select 1, 6 or 11 then click **Save Settings**.

Save Settings | Cancel Changes

7. Click **Save Settings**.

LEDs

Q. What LEDs does the WRVS4400N have?

A. The WRVS4400N has six LEDs located on the front panel: Power, DIAG, IPS, Wireless, Ethernet (1–4), and Internet.

Q. What are the LEDs, and what do they mean?

- ◆ **Power LED (green)** The Power LED lights when the Router is powered on.
- ◆ **DIAG LED (red)** The DIAG LED lights when the system is not ready. The LED light goes off when the system is ready. The Diag LED blinks during Firmware upgrades.
- ◆ **IPS LED (green/red)** The IPS LED lights when the IPS function is enabled. The LED light is off when the IPS functions are disabled. The IPS LED flashes green when an external attack is detected. The IPS LED flashes red when an internal attack is detected.
- ◆ **WIRELESS LED (green)** The Wireless LED lights when the wireless radio is enabled. If the LED flashes, the Router is actively sending or receiving data over the wireless network.
- ◆ **ETHERNET (1–4) LED (green)** The LAN LED serves two purposes. If the LED is solidly lit, the Router is connected to a device through the related port (LAN 1, 2, 3, or 4). If the LED flashes, the Router is sending or receiving data over the port.

Security Supported

Q. What levels and types of wireless security does the WRVS4400N support?

A. The WRVS4400N supports 64 and 128Bit WEP, WPA–Personal, WPA2–Personal, WPA2–Personal Mixed, WPA–Enterprise, WPA2–Enterprise, WPA2–Enterprise Mixed, and Wireless MAC address filtering.

Q. How many numbers of VLANs does WRVS4400N support?

A. The WRVS4400N supports no more than four VLANs. You can choose between 802.1q VLAN mode or Port Based VLAN mode.

Q. How many VPN clients does WRVS4400N support at most?

A. WRVS4400N supports no more than five VPN clients.

Q. Which kind of Encryption is supported in WEP security mode?

A. 64 bits and 128 bits.

Q. How many wireless clients are prevented/permitted access to the wireless network when using the wireless mac filtering feature?

A. Twenty wireless client MAC address can be entered into the MAC address filtering list.

Q. How do I set up wireless client filtering on the WRVS4400N?

A. Complete these steps in order to enable the wireless filtering feature:

1. Open the WRVS4400N web setup page.
2. Click the **Wireless** tab.
3. Click the **Wireless Network Access** sub tab.
4. Select the **Prevent from accessing** and **Permit to access** buttons.
5. Fill in the wireless MAC address that is filtered so you can control which wireless client can connect due to route.

Q. What is the AP Isolation feature and how does it work?

A. The AP Isolation feature isolates all wireless clients and wireless devices on your network from each other. The isolation is done at the MAC address level so all wireless devices are able to communicate with the Router but not with each other. In order to use this function, click the **Enable** radio button and save the settings. AP Isolation is disabled by default.

Q. Can I allow a Quick VPN user to change their password?

A. Yes, you can enable the **Allow User to Change Password** feature on the VPN Client Accounts page within the WebGUI by clicking the **Yes** radio button and clicking the **Save** button.

Q. How many URL Filtering Policies are established at most?

A. The WRVS4400N supports URL Filtering for up to twenty URLs. This type of filtering is based on the actual URL or on key words. You can block more URL s by category using the Cisco ProtectLink service. For more information on ProtectLink, refer to <http://www.cisco.com/go/protectlink> (registered customers only) .

Q. Can I delete URL Filtering Policies?

A. Yes, you can delete any of the URL filters that you have created.

Q. What is Port Forwarding?

A. Port forwarding allows you to run a publicly accessible server behind the router. Port Forwarding opens a specific TCP or UDP port to a computer's LAN IP address behind the router, allowing all Incoming Traffic on that port to be sent directly to that server. The Port Forwarding screen allows you to setup public services on your network. For example, port 80 (HTTP) is used for web, port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server or other specialized Internet applications. You will need to add a port forwarding rule for each service.

Q. What is Port Range Triggering?

A. Port Range Triggering forwards specified TCP or UDP port ranges based on the incoming port specified. Check with your software application to find out what is necessary to enter in these fields.

Note: You can set ten rules at most.

Q. How many Port Forwarding rules are supported by the WRVS4400N?

A. The WRVS4400N supports a total of 15 Single Port Forwarding rules. You can also configure 10 Port Range Forwarding rules.

Special Features

Q. What internet connection types does the WRVS4400N support?

- ◆ Automatic IP Configuration – DHCP
- ◆ PPPoE
- ◆ Static IP
- ◆ L2TP
- ◆ PPTP
- ◆ Heart Beat Signal

Q. Can the IP address number assigned by the DHCP server be more than 253?

A. No, it cannot. The default number of DHCP users is 50. This can be changed to a maximum of 252 users. The built-in DHCP server will issue IP address leases starting at 192.168.1.100. This will also allow you to configure other devices with static IP addresses from 3–99. For example your Servers, Printers, APs, etc. If you would still like to change the default behavior of the DHCP server, you can do so.

Q. What is the "Operating Mode" on the Advanced Routing and what is it used for?

A. If this Router hosts your network's connection to the Internet, select **Gateway**. If another Router exists on your network or between any other Router's connection, select **Route** mode.

Q. What is "MAC address clone" and what is it used for?

A. Some ISPs require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you can assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature. If you want to clone the MAC address of the PC you currently use in order to configure the Router, click the **Clone My MAC Address** button. The Router automatically detects your PC's MAC address, so you do **not** have to call your ISP in order to change the registered MAC address to the MAC address of the Router. It is recommended that you use the PC registered with the ISP to open the **MAC Address Clone** tab.

Q. Which dynamic route protocol is supported on WRVS4400N?

A. The WRVS4400N supports RIPv1/RIPv2 dynamic route protocol and up to twenty static routes.

Q. How many Wireless Network Names (SSID) are supported by the WRVS4400N?

A. The WRVS4400N supports a total of four Wireless Network Names (SSIDs).

Q. How can I isolate the PCs within the multiple SSIDs?

A. The WRVS4400N supports wireless isolation between each configured SSID. In order to enable this feature choose **Wireless > Security Settings**, then enable the AP isolation option from within the WebGUI and click the **Save** button.

Q. How can I isolate PCs within the same SSID?

A. Choose **Wireless > Wireless Security**, and then disable the **Allow PCs on the same wireless network name (SSID)** to see each other's options.

Q. What is Wireless Distribution System (WDS), and what is it used for?

A. The WDS feature only works with the first SSID that is setup in the WRVS4400N. Make sure that the channel and security settings are the same for all WDS enabled devices. WDS allows a wireless signal to be repeated by a repeater. This mode allows a wireless client to connect to the Router through a repeater, such as WAP4400N, WAP54GP, WAP54GPE, when it operates in Repeater Mode. This mode allows you to extend the coverage of the Router with up to three repeaters. Select **Auto** in order to enable the remote access point when in Repeater Mode or select **Manual** and enter the MAC address of the repeater.

Q. Does WDS work with any other SSID except SSID1?

A. No, it only works with wireless SSID1.

Q. How many repeaters allow repeating the wireless signal of the Router?

A. A maximum of three repeaters are allowed to repeat the wireless signal from the WRVS4400N.

Q. What is the web block feature and how does it work?

A. Web block prevents the local LAN computers from using Java, ActiveX, Cookies, and access to HTTP Proxy Servers. You can enable this feature on the Firewall > Basic Settings page in the Web interface.

Q. How many PCs MAC addresses can you specify in the Wireless Network Access List of each SSID?

A. In the earlier firmware versions the maximum was 16 MAC addresses. The updated firmware version 1.1.13 for the version 1.0 and 1.1 hardware now supports up to 20. The v2.0 hardware supports 20 as well.

Q. How can I block all of the TCP or UDP services?

A. You can select port 0 to block all these services.

Q. How many URL Filtering Policies can I establish?

A. The URL Filtering feature supports up to twenty websites to be blocked by the router.

Q. How many Internet Access Policies can I establish?

A. You can establish up to ten Internet Access Policies with the WRVS4400N.

Q. What is VPN Passthrough?

A. If a VPN client is in a private network and achieves connection to a remote VPN device, the VPN client local gateway must support VPN Passthrough. More specifically the router must permit IPSEC, L2TP, and PPTP VPN encryption data to passthrough the router from LAN to WAN without being blocked or changed. The WRVS4400N supports all 3 types of VPN passthrough.

Q. What is the Global NAT – Traversal used for?

A. When one of the VPN End Points (routers) is behind another NAT enabled router or gateway, you must enable the Global NAT–Traversal feature. You can only enable this feature by selecting the Any option in the Remote Gateway IP pulldown menu when setting up a VPN Tunnel.

Q. How is IPS/IDS feature implemented in WRVS4400N?

A. IPS is an advanced technology to protect your network from malicious attacks. IPS works together with your SPI Firewall, IP Based Access Control List (ACL), Network Address Port Translation (NAPT), and Virtual Private Network (VPN) to achieve the highest level of

security. The WRVS4400N wireless router has hardware-based acceleration for real-time pattern matching to detect malicious attacks. It actively filters and drops malicious TCP/UDP/ICMP/IGMP packets and can reset TCP connections. Refer to WRVS4400N Wireless-N Gigabit Security Router with VPN – Administration Guide for more information on this feature.

IDS is not yet supported on WRVS4400N.

Q. What is the WI-FI Multimedia (WMM) feature?

A. WMM is a component of the IEEE 802.11e wireless LAN standard for Quality of Service (QoS). It specifically supports priority tagging and queuing. The priority is given to downstream traffic (AP to Client) based on the 802.1p tagged value. There are four queues supported: Voice, Video, Best Effort, and Background. This feature should be enabled for wireless networks that will have a lot of voice traffic and/or video traffic.

Q. What is the Priority Queue?

A. Depending on the settings of the Priority Queue, this feature assigns information a high or low priority for the five preset applications and three additional applications that you specify. For each application, select High Priority or Low Priority. The packets are put into High or Low Queue for the egress port of WAN based on your settings. Specify Port number. Enter the respective application port numbers in the Specific Port in order to add three additional applications.

Q. What is Diagnostics, and what is it used for?

A. The Diagnostics page provides the customer with a set of tools that can be used to check your Internet connectivity, LAN device connection validation, and website connectivity. The applications included on this page are ping and traceroute.

Q. What is the Universal Plug and Play (UPnP) feature?

A. Universal Plug and Play (UPnP) allows Windows XP and Windows Vista to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. UPnP will also allow for other network devices to be configured and visible, for example a DVR with an Ethernet port, or other devices such as NAS. UPnP is disabled by default.

Q. Does the WRVS4400N support simple network management protocol (SNMP)?

A. Yes, the WRVS4400N supports SNMPv1/v2c. You can enable the WRVS4400N to send SNMP trap messages to an SNMP server on your local network or over the internet for monitoring and troubleshooting purposes.

Q. Does the product support VoIP?

A. Yes, you can connect any IP phone to any of the Ethernet ports of the router.

Q. Is the product compatible with Wireless–N draft 2.0?

A. Yes, the WRVS4400N supports Wireless–N draft 2.0 of the IEEE 802.11n.

Cisco ProtectLink

Q. Can I buy the Cisco ProtectLink Service for my WRVS4400N from retail stores?

A. No, currently the service is only available at selected Cisco distributors. For more information, refer to this link: <http://www.cisco.com/en/US/products/ps9952/index.html>.

Q. What is Cisco Protectlink Web Protection used for?

A. The Cisco ProtectLink Gateway Security Service delivers cost–effective email and Web filtering. Because it is a hosted service with no additional hardware requirements, deployment across your network is a quick and easy process. The service allows you to create and enforce your business's Web–usage policies by restricting access to offensive or non–work–related sites. This helps you improve company productivity, reduces Web–based threats, and conserves bandwidth.

Q. What is Trend Micro InterScan Messaging Hosted Security (IMHS)?

A. Trend Micro InterScan Messaging Hosted Security is a hosted email security service that can benefit any size organization. We provide the hardware, software, and messaging expertise to cleanse your email of spam, viruses, worms, Trojans, and phishing (identity theft) attacks. The cleaned mail stream is sent directly to your mail server for final delivery to your end users. To use this service you must manage and have administrative access to your own SMTP server. Have the domain/IP information ready during the registration process.

Q. Where do I get the ProtectLink Service?

A. You can find the ordering information on the Cisco website here: <http://www.cisco.com/go/protectlink>. Check the Cisco website for firmware updates if you have a router not currently included on the list. Then purchase a Registration key from a Cisco approved retailer. After you have a Registration key you can log into the interface of your Router, click the **Security Protection** or **ProtectLink** tab, and you have a link from there to sign up for the service.

Q. How much does the ProtectLink service cost?

A. The ProtectLink services are sold as one year licenses in 5 seat and 25 seat increments. Contact Sales or a Local/Online Retailer for exact prices.

Q. How long does the initial setup of the ProtectLink service take?

A. If you just registered for the Web Protection service, it can take up to 24 hours to activate your account through Trend Micro. You receive an email that contains your account information and instructions on how to manage your account.

Once this portion is active, if you chose to sign up for the IMHS Service during Registration,

it can take up to another 24–48 hours to receive your account information and instructions on how to manage this service. Once your IMHS account is active, it can take an additional 24 hours to update your MX record.

Q. My Router is listed, but I do not see the ProtectLink tab within the Web UI. What should I do?

A. If your router is listed, but you do not see the **ProtectLink** tab, complete these steps:

1. Go to Cisco Small Business Routers.
2. Click the **Resources** tab
3. Upgrade to the latest WRVS4400N firmware.

Note: Be sure to look at the product label on the back of your router to verify the version of hardware you have. Then download the firmware for your specific hardware version.

Q. I already signed up for the ProtectLink Web Protection service but now I want to use the ProtectLink email security service as well. How do I add this service to my router?

A. In order to activate the ProtectLink email security service after initial registration, contact Trend Micro Support at imhs_support@trendmicro.com with your SMTP server domain/IP information.

Q. How do I begin to use the ProtectLink email security service? Do I need to install, configure, or maintain anything?

A. A simple redirection of your Mail exchange (MX) record is all that is needed to start the service. Your email is processed by the Trend Micro InterScan Messaging Hosted Security to remove spam, viruses, worms, Trojans, and Phishing attacks. The clean messages are then sent directly to your mail server. This process can be activated either through the Initial Trend Micro Registration or through mailto:imhs_support@trendmicro.com if you have already activated the Web Protection Portion of the service.

Q. What level of ProtectLink Web Reputation should I choose?

A. The higher the security level, the more URLs that are blocked based on known or suspect Web threats.

- ◆ **High** Blocks a greater number of Web threats but increases the risk of false positives.
- ◆ **Medium** Blocks most Web threats and does not create too many false positives. This is the recommended setting.
- ◆ **Low** Blocks fewer Web threats but reduces the risk of false positives.

Compatibility Concerns

Q. With what browsers can the WRVS4400N be used?

A. Netscape 4.7 or higher, Mozilla Firefox 2.0 or higher, and Microsoft Internet Explorer 5.0 or higher.

Q. What Dynamic DNS (DDNS) providers does the WRVS4400N support?

A. The WRVS4400N supports **TZO.com** and **DynDNS.org DDNS** providers. All you have to do is create an account with one of these providers and enter your account information into the appropriate fields, then save the settings. For more information, refer to <http://www.tzo.com> in order to learn how to set up DDNS for your WRVS4400N.

Related Information

- **Technical Support & Documentation – Cisco Systems**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 30, 2009

Document ID: 109207
