Release Notes for RV220W Firmware Version 1.0.3.5

November 2011

These Release Notes describe the changes and known issues in RV220W firmware version 1.0.3.5.

CAUTION As with any firmware release, read these release notes before upgrading the firmware.

Contents

This document includes the following topics:

Issues Resolved Since RV220W Firmware Version 1.0.2.4

- Fixed an issue in which NTP stopped working after a firmware upgrade.
- Fixed a critical error that prevented the configuration of remote logging to a syslog server. (CSCtr83453)

- Fixed an issue that prevented clients from connecting via SSL VPN when using MacOs+Java 1.6.0.24 or later. (CSCtr88429)
- Fixed an issue that restricted Cisco QuickVPN Client connections to only 10 users. Now up to 25 connections are supported. (CSCts40693)

Known Issues in Version 1.0.3.5

The following issues are known to occur in this version of the firmware. Read this information before upgrading.

- VLANs created in version 1.0.1.0 or earlier may fail when upgrading to version 1.0.2.4 or later. The router may be inaccessible. (CSCtt22105)
  Work Around:
  a. To prevent this issue before upgrading, open the *Networking > LAN (Local Network) > VLAN Membership* page and set all the access/trunk ports to General mode. Assign all ports to all VLANs, and then proceed to upgrade.
  b. If "Option a" above was not implemented and this issue occurs after upgrading, factory reset the router.
- WAN QoS profile binding based on a particular services, such as FTP, may not work properly. (CSCtu07893)
  Work Around: Select ANY as the service type when creating QoS profiles. This work around limits QoS bindings to the traffic selector match type (IP address Range, MAC address, VLAN, DSCP, and SSID) rather than service type. Due to this limitation you cannot overlap a particular traffic selector match type among the different QoS bindings.
- If the router is configured with multiple independent subnets for multiple VLANs, Cisco QuickVPN Client can access only the original subnet. If the router's LAN IP address is in another subnet, the QuickVPN client cannot connect. (CSCtr23433)
  Work Around: If you configured the router with multiple subnets for multiple VLANs, assign the router a LAN IP address in the first subnet range to ensure that a QuickVPN connection can be made. Be aware that the users can access only the resources in the first subnet range.
- When Shrewsoft or TheGreenBow client-to-gateway software is used, file transfers greater than 500MB cause the VPN connection to fail. (CSCts38114)
  Work Around: Use Cisco QuickVPN.

- Disabling the radio settings on the *Wireless > Basic Settings* page does not disable the active access points. (CSCts38848, CSCts41444)
  Work Around: When disabling the radio, also disable all SSIDs in the *Wireless Basic Setting Table* by unchecking the Enable SSID box.
- Port forwarding does not function as designed for a default service (such as HTTP or FTP) if the default value of the source port (Forward From Port field) is changed. (CSCtt08533)
  Work Around: Instead of editing the port for a default service, create a custom service as described here. In the *Firewall > Advanced Settings > Custom Services* page, create a new service. Select TCP or UDP as the type. To enter a single port as the source, enter the same value in both fields of the range. After saving this record, return to the *Firewall > Port Forwarding* page and either add or edit a rule. Select the service that you added. Specify the internal destination in the Forward to Port field.
- Daylight Savings Time does not take effect upon saving the setting on the *Administration > Time Settings* page. (CSCtt70054)
  Work Around: After enabling Daylight Savings Time, reboot the router.
- When a Gateway To Gateway tunnel is configured in aggressive mode, the router cannot establish a connection to a Cisco RVS4000 or Cisco WRVS4400N router with a dynamic WAN IP address. (CSCtt61631)
  Work Around: Configure a Gateway To Gateway tunnel in Main mode instead. On the *VPN > IPsec > Advanced VPN Setup* page, select the tunnel and then click **Edit**. Change the Exchange Mode to Main. When the VPN tunnel is configured in Main mode, the router can establish a connection. However, be aware that you will need to update the tunnel configuration whenever there is a change in the RVS4000's dynamic IP address.
- When Internet Explorer version 9 is used, the *Status > View Logs* page does not include line breaks between system log entries. (CSCtr24294)
  Work Around: Use Firefox or Chrome to launch the Configuration Utility.
- SSL VPN is not working for users whose computers are running Windows 7 64-bit. (CSCtq79042)
  Work Around: Use Windows XP 64-bit or Windows 7 32-bit.
- If a client has its IP address bound to a MAC address in the IP/MAC Binding table, firewall rules/filters enabled for the client no longer work. All traffic is allowed to pass through this client even though IP blocking/filtering for the client is enabled on the RV220W. (CSCtl09244)
  Work Around: Do not use IP/MAC Binding for a client that has firewall rules/filters assigned to it.

- WLAN clients fail to connect to the router using WPA Enterprise or WPA2 Enterprise. (CSCtj76452)
  Work Around: To work around this issue, disable the Block Fragmentation option in the Firewall page.
- The router fails to apply trusted or self-signed SSL certificates to HTTPS sessions. Although on-screen messages indicate that the certificate was successfully added, the router uses the original default certificate for subsequent HTTPS connections. (CSCtr39253)
  Work Around: The router will use a certificate that is signed by the root CA. You can generate a Self Certificate Request from the router and have it signed by the root CA. Upload the root CA certificate in the Trusted CA Certificate table. Finally, upload the signed certificate in the Active Self Certificate table. See the *Security > SSL Certificate* page of the Configuration Utility.
- Internet NAT redirection does not work using firewall port-forwarding rules. A LAN client cannot access a service by using the WAN IP address of the LAN device (such as an IP camera or an FTP server). (CSCts00209)
  Work Around: Do not use the *Firewall > Port Forwarding* page, but instead create the forwarding rule by using the *Firewall > Access Rules* page. The working port forwarding entry is created along with the firewall access rule.
- A client cannot connect via SSL VPN with a corporate proxy setting. (CSCto14499)
  Work Around: Disable the proxy setting or set the proxy by using the IP address instead of the domain name. For example, in Internet Explorer, adjust the proxy settings by going to **Tools > Internet Options**. Click the **Connections** tab, and then click the **LAN settings** button. Proceed as needed:
  - To disable the proxy, uncheck the **Use a proxy server** box and then check the **Automatically detect settings** box. Click **OK** to save the changes, and then click **OK** to close the *Internet Options* window.

    OR
  - **To identify the proxy by IP address:** Check the **Use a proxy server** box, delete the domain name if in use, and enter the IP address of the proxy server in the **Address** box.
- VPN connectivity can be lost when using SSL VPN port forwarding and later versions of Firefox. (CSCtj59663)
  Work Around: Use Internet Explorer or Firefox version 3.6.17.

- There are issues with the SSL VPN client installer on Internet Explorer 8. (CSCtq79042)
  Work Around: Adjust the settings in Internet Explorer as described below.
  1. In Internet Explorer, go to **Tools > Internet Options**.
  2. Click the **Security** tab, and then click the **Custom Level** button.
  3. Scroll down to *ActiveX controls and plug-ins*.
  4. For **Automatic prompting for ActiveX controls**, click **Enable**.
  5. For **Download signed ActiveX controls**, click **Enable**.
  6. Click **OK** to save the changes, and then click **OK** to close the *Internet Options* window.
- The GUI configurations listed below require restarting the RV220W. (CSCtu33997)
  - Changing the time zone to use an NTP server.
  - Manually setting the time.
  - Enabling and configuring remote management.
- The traffic blocking setting on the *Administration > WAN Traffic Meter* page does not function properly. Traffic is allowed even after the specific limit is reached. (CSCts95836)
- A 6to4 tunnel may encounter packet loss depending on the type of NIC used. (CSCtr08162)
- On the *Administration > Firmware Upgrade* page, the Firmware Last Updated field is blank. (CSCtr00764)
- The online help file for Wi-Fi Multimedia (WMM) should read “WMM: Opens the **QoS Configuration** page to edit the QoS configuration parameters for this profile.” (CSCtk66482)
- SNMP MIBs only support read access. (CSCtj48019)
- The DHCP Client Table does not show all clients. (CSCtq44404)
- Certain syslogs such as IKE and Kernel logs will appear with the time stamp of 2000-01-01 and not the current time. (CSCtu34004)
- The syslog does not always list the timestamps in sequential order. (CSCtu34011)

Firmware Upgrades and Downgrades

Refer to the following instructions:

- **Upgrading the Firmware**
- **Downgrading the Firmware**

Upgrading the Firmware

STEP 1 As a best practice before upgrading, back up the current configuration by performing the following tasks:

a. Open the *Administration > Backup / Restore Settings* page.

b. Click the **Backup Startup Configuration** button, and choose a file location. Later, if needed, you can restore the configuration.

STEP 2 On the *Administration > Firmware Upgrade* page, click **Browse** and then select the new firmware.

STEP 3 Click **Upload**.

STEP 4 When the confirmation message appears, click **OK** to continue, or click **Cancel** to close the message without upgrading the firmware.

Downgrading the Firmware

If you wish to re-install an earlier version of the firmware after upgrading, use this procedure.

STEP 1 As a best practice before downgrading, back up the current configuration by performing the following tasks:

a. Open the *Administration > Backup / Restore Settings* page.

b. Click the **Backup Startup Configuration** button, and choose a file location. Later, if you upgrade the firmware, you can restore the configuration.

STEP 2 Check the **Reset all configuration / settings to factory defaults** box.

IMPORTANT: It is necessary to factory reset the router when downgrading the firmware. Checking this box eliminates the need to do a manual reset.

STEP 3 On the *Administration > Firmware Upgrade* page, click **Browse** and then select the firmware that you want to install.

STEP 4 Click **Upload**.

STEP 5 When the confirmation message appears, click **OK** to continue with the downgrade, or click **Cancel** to close the message without modifying the firmware.

STEP 6 To restore the configuration that you saved with the earlier version of the firmware, perform these tasks:

a. Open the *Administration > Backup / Restore Settings* page.

b. Click **Browse** and then select the configuration file.
IMPORTANT: Ensure that the restored configuration file is from the same firmware version that you installed in this procedure.

c. Click **Restore** to restore the saved settings.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Cisco Small Business Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Small Business Products. No login is required. Downloads for all other Cisco Small Business products, including Network Storage Systems, are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
Product Documentation	
Cisco RV220W	http://www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

OL-26166-01