

Release Notes for Cisco RV120W Firmware Version 1.0.4.10

September 2012

These Release Notes describe the changes and known issues in Cisco RV120W firmware version 1.0.4.10.

IMPORTANT:

As with any firmware release, please read these release notes before upgrading the firmware. Cisco also recommends backing up your configuration before any firmware upgrade.

Contents

This document includes the following topics:

- [Changes Since Firmware Release 1.0.3.10](#)
- [Known Issues in Release 1.0.4.10](#)
- [Related Information](#)

Changes Since Firmware Release 1.0.3.10

Table 1 Resolved Issues in Firmware Version 1.0.4.10

Ref Number	Description
CSCtk66428	Adding a 1-to-1 NAT service to a subnet only works when adding the service to a subnet of VLAN1.
CSCtt08533 CSCts27240	Port forwarding does not work when the port is specified.
CSCtr83966	The external syslog server receives only kernel messages from the RV120W.
CSCts00209	Internet NAT redirection does not work when services are forwarded using port forwarding.
CSCtn43366	Microsoft Internet Explorer version 8 accessibility upon reboot issue. NOTE: To prevent problems, clear the web browser cache after the router is upgraded.
CSCto46996	PPTP connected/configured users are not shown on the VPN Client Connection Status page.
CSCts21176	Enable inter-VLAN option does not work when setting up multiple VLANs at one time.
CSCtw85203	The QuickVPN client cannot access the computers in the LAN of the RV120W when the LAN subnet is smaller than a /24 subnet. NOTE: The lower limit for subnets is /24.
CSCtx84235	If a manually-configured NTP server is used, the RV120W does not synchronize with the NTP server after a reboot.
CSCtc50330	The IPSec Connection Status takes too long to recognize that the VPN tunnel has been disconnected. NOTE: Dead Peer Detection must be enabled for the IPSec Connection Status to reflect the current tunnel connection status.
CSCtr91709	PPTP connection remains active after a PPTP user is disabled or deleted in the RV120W.
CSCub88212	6to4 Tunneling will not work when SLA ID is set to zero.
CSCub88224	6to4 tunneling requires a static route to work.
CSCub88282	Windows native FTP File transfer fails when using QuickVPN behind NAT on Windows 7.

Known Issues in Release 1.0.4.10

Table 2 Known Issues in Firmware Version 1.0.4.10

Ref Number	Description
CSCub51099	<p>Issue—Configuration and logging policies are lost after an upgrade. The RV120W loses the PPTP users and any specific logging options after the upgrade.</p> <p>Workaround—None. You must reconfigure PPTP users after the upgrade.</p>
CSCub59425	<p>Issue—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 from this client even though IP blocking/filtering for the client is enabled on the RV120W.</p> <p>Workaround—None.</p>
CSCtl79849	<p>Issue—Firewall is not supported for IPv6.</p> <p>Workaround—None.</p>
CSCtj73922	<p>Issue—Time is off by 7 hours when Daylight Saving Time (DST) is enabled on Central European Time.</p> <p>Workaround—Do not use the DST setting; manually set the clock if the time needs to be changed to conform to DST.</p>
CSCtr76264	<p>Issue—PPTP users can access the configuration utility even if remote management is disabled.</p> <p>Workaround—None.</p>
CSCtu34004	<p>Issue—Certain syslogs such as IKE and Kernel logs will appear with the timestamp of 2000-01-01 and not the current time.</p> <p>Workaround—None.</p>
CSCty01349	<p>Issue—When clicking to reorder access rules—especially after a reboot—some rules may not be available for reordering while others may be duplicated.</p> <p>Workaround—Delete and re-add the access rules in order of the desired priority.</p>
CSCub64446	<p>Issue—DHCP option 150 does not work.</p> <p>Workaround—Use option 66 and enter a hostname (without a domain name).</p>

Release Notes

Table 2 Known Issues in Firmware Version 1.0.4.10

Ref Number	Description
CSCua43141	<p>Issue—Current implementation of DHCP Option 66 does not support an IP address.</p> <p>Workaround—Enter a hostname (without a domain name) instead of an IP address when entering the settings on the Networking > LAN (Local Network) > Advanced DHCP Configuration page.</p>
CSCua43159	<p>Issue—The router does not allow you to append the domain to a hostname when configuring DHCP Option 66. For example, the router will accept “MyHost” as a host name, but not “MyHost.example.com.”</p> <p>Workaround—None.</p>
CSCua43166	<p>Issue—When specifying the configuration file for Option 67, the Networking > LAN (Local Network) > Advanced DHCP Configuration page allows only files with a .cfg extension.</p> <p>Workaround—None.</p>
CSCtj42903	<p>Issue—When blocked keywords are configured in the Firewall page, users attempting to reach sites that use blocked keywords are redirected to the router login page instead of the appropriate warning page.</p> <p>Workaround—None.</p>
CSCts24763	<p>Issue—Changing the MTU value from the default value in the WAN window prevents clients from connecting to the Internet.</p> <p>Workaround—None. Use the default MTU value (1500 bytes) to ensure that clients can connect to the Internet.</p>
CSCtu24324	<p>Issue—QoS Profile Binding does not work properly for a selected service.</p> <p>Workaround—Select the service type Any instead of selecting a particular service when configuring a QoS profile. QoS profile binding is then based on an IP address or a group of IP addresses.</p>
CSCts32168	<p>Issue—When the DMZ is enabled, access to a device through the WAN is not allowed.</p> <p>Workaround—Use port forwarding instead of DMZ to access LAN devices.</p>
CSCtj31483	<p>Issue—When remote management is enabled and a non-standard QVPN port (standard QVPN ports are 443 or 60443) is configured, the QuickVPN client cannot successfully establish a connection.</p> <p>Workaround—None; use port 443 (the default management port) or 60443 QVPN port when defining the remote management.</p>

Table 2 Known Issues in Firmware Version 1.0.4.10

Ref Number	Description
CSCtc98644	<p>Issue—Configuring Wi-Fi Protected Setup using the push-button configuration method does not work properly.</p> <p>Workaround—Configure WPS using the PIN method.</p>

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/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/go/software Select a link to download firmware for Cisco Small Business Products. No login is required.
Product Documentation	
Cisco Small Business RV Series Routers	www.cisco.com/go/smallbizrouters
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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2012 Cisco Systems, Inc. All rights reserved. 78-20884-01