Release Notes for SA 500 Series Security Appliances Firmware Version SA500-K9-1.1.65

August 13, 2010

These release notes describe the known and resolved issues in firmware version SA500-K9-1.1.65.

Contents

This document includes these topics:

Recommended Practices

Recommended Upgrade Steps

When upgrading from version 1.0.15, 1.0.17, or 1.0.39 the firmware will reset the router to its factory default and you will need to back up the configuration described in this section. When upgrading from 1.1.21, 1.1.42, 1.1.56, or 1.1.62, these steps are not required.

CAUTION Do not try swap images if a secondary firmware image is not present. Doing so can cause the to router to NOT boot up.

To upgrade the SA 500 follow these steps.

STEP 1 Back up the existing configuration using the SA 500 Configuration Utility.

If you need to revert to the previous firmware version, this allows you to restore the configuration associated with the prior version.

To access the configuration back-up options, click **Administration** on the menu bar, then click **Firmware & Configuration > Network** in the navigation tree.

Follow the instructions in the *Cisco SA 500 Series Security Appliances Administration Guide* to back up the configuration.

STEP 2 Write down or take screenshots of your existing configuration settings. After upgrading to firmware version SA500-K9-1.1.65, you must manually re-enter these settings by using the SA 500 Configuration Utility.

This is necessary because the SA 500 is reset to factory defaults as part of the upgrade process and the previous configuration back-up file format is incompatible with the format required for firmware version SA500-K9-1.1.65.

STEP 3 Perform the upgrade by using the Configuration Utility. To access the upgrade options, see the **Upgrade Firmware** section of the Getting Started (Basic) page of the Configuration Utility.

STEP 4 Manually re-enter the configuration settings you recorded in Step 2.

STEP 5 Verify that the installation is working properly.

If the upgrade is not successful, you can revert to the previous firmware version and restore the configuration from the backup that you created in Step 1.

Limitations and Restrictions

These are the limitations and restrictions for the SA 500. These are known limitations that will not be fixed and there is not always a workaround.

- When performing a factory default reset, the updated IPS signatures (newer than the image's built-in signatures) are erased and fall back to the built-in signature in the image.

  The workaround is to reinstall the latest signatures.

Important Notes

These are important notes related to firmware version SA500-K9-1.1.65.

- If the LAN LEDs remain down for more than 10 minutes, or if the Diagnostic LED is up, press the reset button (with the router powered on) for 10 seconds and release. During that time, do not power off the device.
- Upgrading the firmware over wireless or over slow internet connections is not recommended. When upgrading, always connect to the LAN. Do not exit the browser window or interrupt the process in anyway until the operation is complete.

Known Issues

The following table lists the known issues in firmware version SA500-K9-1.1.65.

Ref Number	Description
CSCtc15599	The router's optional port cannot be configured in VLAN trunk mode (Only applies to the SA 540). **Symptom** Changing the optional port from Access mode to Trunk mode does not allow traffic to pass though. **Workaround** Use other LAN ports for VLAN trunking.
CSCtd83237	Firewall rules and positions in the Available Firewall Rules table are not the same number. **Symptom** Index numbers begin counting with 0 (zero), and positions begin counting with 1 (one). This can cause confusion when using the "Move to *<index number>*" button. **Workaround** Use the **Move Up** button to move the rule up the list.
CSCte60926	Unable to access IPv6 internet addressing when using 6 to 4 automatic IPv6 tunneling. **Workaround** None.
CSCtf07567	Sometimes there is no audio for a voice call, when a UC 500 is behind the router. **Symptom** The UC 500 sends out two C lines (media and session level addresses) in the SIP header, but the router only translates the media level address. **Workaround** Configure the UC 500 to send only the media level addresses in the SIP header by entering these commands from the CLI: voice class sip-profiles 1 request ANY sdp-header Connection-Info remove response ANY sdp-header Connection-Info remove ! voice service voip sip sip-profile 1

Ref Number	Description
CSCtf37764	Bandwidth profiles do not restrict the following: ▪ HTTP traffic when content filtering is enabled ▪ Passive FTP sessions **Workaround** For HTTP traffic, disable content filtering. For passive FTP sessions, there is no workaround.
CSCtf40495	After modifying the default VLAN IP and DHCP pool addresses, sometimes the PC cannot obtain a DCHP address. **Symptom** The PC connected to the LAN port can no longer obtain a DHCP address, even after release/renew or by plugging and then unplugging the power cable. **Workaround** Configure a static IP address in the newly configured network to regain access to the router. For example, if you changed your default VLAN to 192.168.10.x, you will then need to configure a static IP address for your PC to 192.168.10.5.
CSCtg60881	The QuickVPN client can access the default VLAN on the router, but cannot access other configured VLANs. **Workaround** None.

Ref Number	Description
CSCtf62341	An SSL VPN tunnel cannot be established. **Workaround** This might indicate that the previous VPN client did not uninstall correctly from your PC. Clean up the previous client installation by following these steps: a. In Internet Explorer, on the **Tools** menu, click **Internet Options**. b. On the **General** tab, click **Settings**. c. Click **View Objects**. d. Delete all object files then relaunch the browser. If this workaround does not resolve the problem, do the following: a. Click **Start** and then click **Control Panel**. Double-click **System**. b. On the **Hardware** tab, click **Device Manager.** c. Double-click Network Adapters**.** Right-click the **Vpn Tunnel ssldrv** adapter and click **Uninstall.** d. Restart your system.
CSCtf63339	Interface statistics for Tx Pkts (send) and Rx Pkts (receive) are not accurate between LAN and WAN. **Workaround** None.
CSCtf72391	Voice is not supported on the DMZ interface. **Workaround** None.
CSCtg04762	Protocol bindings do not work when content filtering and/or ProtectLink services are enabled on the router. **Workaround** None.
CSCtg06961	WAN connectivity takes two to three minutes to be established after the router reboots. **Workaround** None.

Ref Number	Description
CSCtf07090	A “server is down” error message sometimes appears when ProtectLink Web threat protection is set to high. **Workaround** None.
CSCtg64332	When adding or deleting firewall rules, sometimes the changes don’t appear on the Firewall Rules page. **Workaround** None.
CSCtg75025	Site-to-Site IPSec VPN between the SA 500 and a ASA security device is not established when the ASA WAN is disconnected. **Workaround** Disable and then re-enable the IPSec VPN policies on the SA 500.
CSCth19415	SIP option request is being blocked by router. **Workaround** None.
CSCth37110	SSL VPN Tunnel installation fails sometimes on certain Windows 7 64-bit PCs. **Symptom** An error message occurs during an SSL VPN tunnel adapter installation. **Workaround** None.
CSCth39492	When Inter-VLAN routing is enabled on the router and heavy traffic occurs, unicast and multicast packets are seen between VLANs. **Workaround** None.
CSCth40743	Failover takes two to three minutes to complete. **Workaround** Reduce the retry interval for the WAN Failure Detection Method on the WAN Mode page.
CSCth49243	Slow Web browsing occurs when the router is configured with load balancing. **Workaround** None.
CSCti11224	When two or more SA 500’s are connected together on the LAN and share the same subnet, a memory leak might occur. This can cause the router to reboot under certain network environments. **Workaround** None.

Resolved Issues

These issues were resolved in firmware version SA500-K9-1.1.65.

Ref Number	Description
CSCtb42723	The router does not display connected UPnP devices.
CSCtc52591	NAT hairpinning is not supported.
CSCte99463	Source and destination columns in the IPS logs are blank.
CSCtf26376	When a Certificate Authority (CA) requests a 2048-bit signature, the router generates a 1024-bit signature instead.
CSCtf33065	VPN remote subnet starting IP address automatically resets the last octet to 0.
CSCtf37097	When the router is configured with DDNS and Dual WAN with auto-rollover, the SSL VPN port displays the IP address instead of the FQDN.
CSCtf40495	After modifying the default VLAN IP and DCHP pool addresses, the PC connected to the LAN port cannot obtain a DHCP address.
CSCtf41808	The country name “Bulgaria” is not spelled correctly on the Wireless > Radio Settings page.
CSCtf47059	After restoring the SA 520 configuration (.cfg) file to the SA 520, the router goes down.
CSCtf97022	Periodic firmware checks occur, even when this option is disabled on the Firmware and Configuration page.
CSCtg04778	Performing RDP sessions (outside the IPSec tunnel) to other IPSec sites, causes the router to reboot every few hours.
CSCtg31890	The SA 500 default configuration allows a user with default user credentials, to log in from the WAN interface when Remote Management is enabled.
CSCtg31898	The Protocol Bindings page displays "Optional WAN" as "Configurable Wan".
CSCtg31914	When the router is configured as Dual WAN in Load Balancing mode, port forwarding, RDP, and WebEx problems occur.
CSCtg33833	Static route cannot be added when the router is using PPPoE.
CSCtg36916	The description for the URL Keyword option in the online help is incorrect.

Ref Number	Description
CSCtg36922	The word" UNSECURE" is spelled incorrectly (shows as INSECURE) on the IPv4 and IPv6 Firewall Rule pages.
CSCth37427	SSL tunnel installation intermittently fails on Windows Vista PCs.
CSCth40717	Changes made on the WAN mode page causes the WAN subsystem to restart.
CSCth41960	The router only supports two QuickVPN client connections for port 60443.
CSCth41961	The QuickVPN client drops tunnels during an FTP session.
CSCth41957	When three or more QuickVPN tunnels are configured on the router, it does not respond to ping.
CSCth60950	The Protectlink Gateway license cannot be activated from the License Management page.
CSCth65046	The User Login Policy is enabled but is not enforced after a reboot.
CSCth97632	When configuring firewall rules on the router, only the first 45 firewall rules work.
CSCti23707	SSL VPN does not support 3-DES encryption.
CSCti16492	Firewall rule does not appear in the Available Firewall Rules table when moving it from an index position greater than 10, to an index position 9 or below.

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/sa500software Click the product name to download the firmware and Open Source offer letter (login is required)
Quick VPN Software	www.cisco.com/go/qvpnsoftware
Product Documentation	
SA 500 Technical Documentation	www.cisco.com/go/sa500resources
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-23405-01