Release Notes for SA500 Series Security Appliances Firmware Version SA500-K9-2.1.51

July 2011

These release notes describe the known and resolved issues in firmware version SA500-K9-2.1.51.

Contents

This document includes these topics:

- Recommended Practices
- Limitations and Restrictions
- Important Notes
- Known Issues
- Resolved Issues
- Related Information

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.

NOTE These steps only apply if you are upgrading from firmware version 1.0.15, 1.0.17, or 1.0.39. Resetting to factory defaults is not required.

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

To upgrade the SA500 follow these steps.

STEP 1 Back up the existing configuration using the SA500 Configuration Utility.

If you need to revert to the previous 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 SA500 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 version SA500-K9-2.1.51 you must manually re-enter these settings by using the SA500 Configuration Utility.

This is necessary because the SA500 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 version SA500-K9-2.1.51.

STEP 3 Perform the upgrade by using the Configuration Utility. To access the upgrade options, see the **Upgrade** 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 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 SA500. 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.

- When VPN users connect to the SA500, they can access internal networks and the Internet, but not DMZ networks.

Important Notes

These are important notes related to version SA500-K9-2.1.51.

- 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 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 version SA500-K9-2.1.51:

Ref Number	Description
CSCtc15599	The router's optional port cannot be configured in VLAN trunk mode (Only applies to the SA540). **Symptom** Changing the optional port from Access mode to Trunk mode does not allow traffic to pass through. **Workaround** Use other LAN ports for VLAN trunking.
CSCte60926	Unable to access IPv6 internet addressing when using 6 to 4 automatic IPv6 tunneling. **Workaround** None.
CSCtf62341	An SSL VPN tunnel cannot be established. **Workaround** This can 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.
CSCtf72391	Voice is not supported on the DMZ interface. **Workaround** None.

Ref Number	Description
CSCtj02357	Unable to connect to an SSL VPN tunnel when running Mac OS X Snow Leopard. **Workaround** To connect to the tunnel, the root user must add the following line in the /etc/sudoers file: **test ALL=NOPASSWD: /usr/sbin/chown,/bin/chmod,/bin/rm** where *test* is the admin username. **Note**: This line only needs to be added "once" for each Mac and corresponding line for every admin user.
CSCtj54878	Multicast IPTV playback is experiencing delays in audio and video streams. **Workaround** None.
CSCto11653	Remote SSL VPN user cannot connect on MAC and Linux platforms after upgrading to Java Version 6 Update 24. **Workaround** Revert back to the older working version of Java.
CSCto35003	In certain configurations when URL Filtering is enabled, a web page takes longer than usual to download completely. **Workaround** None.
CSCtq95726	With 1-to-1 NAT and content filtering enabled, the HTTP traffic (port 80) uses the WAN address instead of the IP Alias address. Disable content filtering from the **Firewall > Content Filtering > Content Filtering** page.
CSCtr58108:	When content filtering or ProtectLink is enabled, the remote VPN client cannot access the Internet when configured for a full tunnel. **Workaround** Configure split tunneling on the remote VPN client policy.

Resolved Issues

These issues were resolved in firmware version SA500-K9-2.1.51.

Ref Number	Description
CSCtg61468	With 1-to-1 NAT, packets going from LAN to WAN has the source address as the primary WAN IP address instead of the WAN IP alias IP address.
CSCth19415	SIP option request being blocked by the SA500.
CSCth40743	WAN failover takes up to 2 to 3 minutes.
CSCth49243	Slow Internet browsing occurs when the SA500 is configured with load balancing.
CSCti53414	Ping drops intermittently when a wireless client is connected in 802.11n mode.
CSCtj85631	Firmware upgrade erases the parameters on the Administration > Domain Configuration page.
CSCtk31271	HTML links broken in log entries.
CSCtk59442	Approved URL List is limited to 100 entries; needs to increase to 250.
CSCtk61856	Time stamp not appearing in email logs.
CSCtk63483	When the SA500 if configured with load balancing and the primary IPSec tunnel goes down (such as a WAN failure), the backup IPSec VPN tunnel fails.
CSCtk63514	IPSec VPN rollover takes too long for WAN failover using Dynamic DNS.
CSCtk66300	When 50 or more DHCP bindings are configured on the SA500, the Device Status > Dashboard page displays high Memory Utilization.
CSCtn14541	When using the Cisco VPN client, the SA500 only supports split tunneling.
CSCtn14550	VPN user information is not being logged in system logs.
CSCtn14576	High memory usage occurs when auto-refresh is active on the Configuration Utility.
CSCtn15512	Critical kernel errors display in system logs.
CSCtn17625	Cisco VPN client cannot resolve resource name through the VPN tunnel.
CSCtn18394	1-to-1 NAT not working properly.

Ref Number	Description
CSCtn87362	When a site-to-site tunnel is established between a SA500 and UC560, calls drop intermittently and at random.
CSCto15189	When a UC560 is behind an SA500 with port forwarding enabled, all inbound calls are rejected by the UC560 and a SIP 400 error occurs.
CSCto15767	SSL VPN SA520 security levels issues (Win 7 32-bit SSL connections with Firefox/ Chrome browser and 3DES displaying incorrectly in system logs).
CSCto15776	After a firmware upgrade, site-to-site VPN does not pass HTTP or email traffic.
CSCto15801	Cannot ping the main site from the remote site with SA500 and iPad with built-in Cisco VPN connection.
CSCto15792	Site-to-site VPN problem with remote Internet access.
CSCto34912	The Configuration Utility allows a user to configure overlapping address space between a VPN server on a SA500 and the Cisco VPN client, which is not a supported configuration.
CSCto34964	URL Request not passing through the SA500.
CSCto35007	Signature information not available on the IPS Policy page. Each signature is now a hyperlink that links to another page that includes the signature description.
CSCto35015	SA500 reboots under certain traffic conditions.
CSCto79345	High memory utilization causes the SA500 to reboot.
CSCtf07567	Sometimes there is no audio for a voice call, when a UC500 is behind the router.
CSCtf58513	A VPN tunnel between a SA520 and ASA5500 cannot be terminated when DPD is configured.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation	www.cisco.com/support (Log in required)
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Software	
Quick VPN Software	www.cisco.com/go/qvpn
Cisco VPN Client	www.cisco.com/go/ciscovpnclient
SA500 Firmware Downloads	www.cisco.com/go/sa500software
Product Documentation	
SA500 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-25415-01