Release Notes for SA500 Series Security Appliances Firmware Version SA500-K9-2.1.19

July 2011

These release notes describe the known and resolved issues in firmware version SA500-K9-2.1.19.

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.

NOTE These steps only apply if you are upgrading from firmware version 1.0.15, 1.0.17, or 1.0.39. Otherwise, upgrading 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-K9-2.1.19 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-K9-2.1.19 .

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.

Important Notes

These are important notes related to version SA500-K9-2.1.19.

- 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.l

Known Issues

The following table lists the known issues in version SA500-K9-2.1.19.

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.
CSCtf07567	Sometimes there is no audio for a voice call, when a UC500 is behind the router. **Symptom** The UC500 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 UC500 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
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.
CSCth19415	The SIP option request is being blocked by router. **Workaround** None.
CSCti53414	Ping drops intermittently when a wireless client is connected in 802.11n mode. **Workaround** Change the wireless mode to “g and b” mode.

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, follow these steps: a. Login to MAC OS X 10.1.4 with user privileges. b. Enter the following command on the terminal window to launch the Safari browser (use the exact syntax). **sudo/Applications/Safai.app/Contents/MacOS/Safari** c. Enter the user's admin password (not the root password) to connect to the tunnel.
CSCtj09710	When the POP3 and IMAP protocols for "detect and prevent" are enabled on the IPS Protocol Inspection Settings page, all inbound POP3 and IMAP services are blocked. **Workaround** Check the IPS logs and disable the particular signature that is causing the problem.
CSCtj54878	Multicast IPTV playback is experiencing delays in audio and video streams. **Workaround** None.
CSCtj85631	When upgrading from firmware v1.42 to v1.65 and later, some Domain parameters (under Administration > Domains) are erased. **Workaround** To re-establish authentication to the Radius Active Directory/ LDAP server, follow these steps: a. Delete all users and groups associated with the corrupted/erased Domain. b. Delete the corrupted/erased Domain. c. Create the Radius Active Directory Domain as before. d. Re-create the groups and accounts.

Resolved Issues

These issues were resolved in version SA500-K9-2.1.19.

Ref Number	Description
CSCtd83237	Firewall rules and positions in the Available Firewall Rules table are not the same number.
CSCtd92747	Web filtering does not work consistently.
CSCte60923	After enabling content filtering, Active-X is not blocked.
CSCte91638	SSL VPN does not work with Windows 7 32-bit or 64-bit operating systems.
CSCtf07090	A “server is down” error message appears when the ProtectLink security level is set to High.
CSCtf37764	In the Bandwidth Profile, the maximum bandwidth rate is not taking effect.
CSCtj57633	When no IPS signature upgrade is available, the View All Logs window in the GUI shows the Log Severity as ERROR.
CSCtf57964	The router does not connect to QuickVPN Client 14.0.5 running the Windows 7 Ultimate 64-bit operating system.
CSCtf82549	Enabling content filtering breaks the HTTP firewall rules.
CSCtg02230	Content filtering does not block web access if a proxy server is being used.
CSCtg04762	Protocol Binding is not working when content filtering and/or ProtectLink services are enabled.
CSCtg27736	The router drops all VPN connections when the Optional Port is disabled.
CSCtg31902	The VPN Wizard default settings for IKE authentication is 3DES instead of AES which is more secure.
CSCtg36906	Cannot edit a Bandwidth Profile name under certain conditions.
CSCtg36916	The description for the URL Keyword option in the online help is incorrect.
CSCtg60881	The QuickVPN client can only access the default VLAN.
CSCtg63955	User cannot identify which IPS category is blocking a stream from a signature URL.

Release Notes

Ref Number	Description
CSCtg64332	When adding or deleting firewall rules, sometimes the changes do not appear on the Firewall Rules page.
CSCtg93337	When installing a program, the URL “www.cisco.com” is shown as an unverified publisher for SSL VPN.
CSCth40721	When a cable modem is connected to the router, the modem uses a private IP address (instead of the public IP address) when its ISP is down.
CSCth51755	Webpage not being rendered properly when URL Filtering is enabled.
CSCth51789	Cannot access the Web interface though a VPN site-to-site tunnel.
CSCti11224	Memory leak occurs when using certain topologies.
CSCti33347	Clients cannot authenticate to a wireless network through RADIUS authentication.
CSCti60157	For some countries, the Radio Settings page only shows 802.11b (or g mode). The n modes are not available.
CSCti65780	SSL certificates signed by Thawte will not work on the router as a 1024-bit certificate.
CSCti79855	The IPS Automatic Signature upgrade process fails to upgrade the signature.
CSCti82318	Multicast IPTV playback is not working properly.
CSCti91709	In WAN Failure Detection, the default value for the retry interval does not change.
CSCti43660	Web Content Filtering does not work on a DMZ.
CSCtj73858	CDP neighbors are not showing up in the CDP neighbor table.
CSCtk13773	When performing an RDP session over an IPSec tunnel, sessions disconnect and then reconnect every few minutes.
CSCtq65669 CSCtq65681	Cisco SA500 Series Security Appliances are affected by two vulnerabilities on their web-based management interface. An attacker must have valid credentials for an affected device to exploit one vulnerability; exploitation of the other does not require authentication. Both vulnerabilities can be exploited over the network. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available. This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20110720-sa500.shtml

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-25492-01