Release Notes for SPA100 Series Analog Telephone Adapters Firmware Version 1.2.1

August 2012

These Release Notes provide information about SPA100 Series Analog Telephone Adapters firmware version 1.2.1.

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.

NOTE Because of a change to the bootloader in firmware version 1.2.1(004), downgrading to earlier versions is not possible.

Contents

Enhancements

- Added the ability to enable or disable the Reset button. Use the *Administration > Management > Reset Button* page. When it is enabled, press this button for 1-2 seconds to reboot the ATA and for 5-6 seconds to reset it to the factory default configuration.
- Added these parameters for audio configuration:
  - Use Remote Pref Codec—Use the remote peer's preferred codec.
  - Codec Negotiation—Methods for choosing a codec.
- Updated the T.38 library.
- Fax to Voice Feature
- DHCP option 15 feature
- Support for Bell 202 FSK Caller ID
- Support for resync via HTTP with xuser/xpassword parameters. For more information, see **xuser/xpassword Parameters**, below.
- SPA1x2 ATA Resync_At Parameter v1.2.1(004) For more information, see **Using the Resync_At Parameter, page 3**.
- The default setting for the CWT1 Cadence was changed from 30 seconds to infinite. The value in the phone will be changed from "30" to "*" where * = infinity. After completing the upgrade, the user can adjust this setting as needed.

xuser/xpassword Parameters

NOTE Before you use these parameters, be aware that the credentials will be sent as clear text. *This procedure is recommended for lab use only.*

Use a command with the following structure:

```
http://192.168.15.1/admin/resync?tftp://192.168.15.244/pathToFile/
ConfigFile.xml&xuser=admin&xpassword=1234
```

Where:

`192.168.15.1`—IP address of ATA

`tftp`—The scheme, which can be tftp, http, or https

`192.168.15.244`—The IP address or name of the server hosting the configuration file.

`pathToFile`—The location of configuration file.

`ConfigFile.xml`—The name of configuration file.

`&xuser=admin`—The required administrator username, *admin*.

`&xpassword==1234`—The password that you want to assign to the administrator.

Using the Resync_At Parameter

The introduction of this new parameter can affect three settings after a firmware upgrade on the SPA1x2 ATA, unless you explicitly configure these parameters. The changes made to these setting do not affect device stability or security in any way.

NOTE If you factory reset the SPA1x2 ATA after upgrading to 1.2.1(004), then the parameters are correctly set and the above can be ignored.

The affected parameters are:

- Resync_At__HHmm
- Resync_At_Random_Delay
- Resync_Fails_On_FNF

To eliminate unintended settings, configure the following settings through a provisioning file or the web-based configuration utility. You can use the factory defaults or your own values.

Using a Provisioning File

```
<flat-profile>
<Resync_At__HHmm_ ua="na"></Resync_At__HHmm_>
<Resync_At_Random_Delay ua="na">600</Resync_At_Random_Delay>
<Resync_Fails_On_FNF ua="na">Yes</Resync_Fails_On_FNF>
…
…
<router-configuration>
…
…
</router-configuration>
</flat-profile>
```

Using the Web-Based Configuration Utility

STEP 1 Choose **Voice > Provisioning**.

STEP 2 Enter the desired values in these fields:

- **Resync At (HHmm)—**The time of day when the device tries to resync. The resync is performed each day. Used in conjunction with the Resync At Random Delay.
  Default setting: blank
- **Resync At Random Delay—**Used in conjunction with the Resync At (HHmm) setting, this parameter sets a range of possible values for the resync delay. The system randomly chooses a value from this range and waits the specified number of seconds before attempting to resync. This feature is intended to prevent the network jam that would occur if all resynchronizing devices began the resync at the exact same time of day.
  Default setting: 600
- **Resync Fails On FNF—**Determines whether a file-not-found response from the provisioning server constitutes a successful or a failed resync. A failed resync activates the error resync timer.
  Default setting: yes

STEP 3 Save the settings.

Resolved Issues

Tracking Number	Description
CSCtn94221	Fixed issues with certain DTMF settings.
CSCtr20000	Fixed issues with DTMF detection.
CSCtr76788	Fixed an issue in which the ATA could not connect to the secondary DNS server when SIP Transport was set to TLS.

Tracking Number	Description
CSCtr94454	Fixed an issue in which auto-recovery fails when the ATA was connected to a switch port with spanning-tree enabled in normal mode.
CSCtu12329	Fixed an issue in which calls could not be made if the primary DNS server was unreachable.
CSCtw76382	Fixed an issue in which the ATA rebooted repeatedly after loading an encrypted configuration file.
CSCtx11685	Fixed an issue in which the caller ID was not sent to the phones.
CSCtx35811	Fixed an issue in which a phone displayed a message waiting indication although there were no new messages.
CSCtx45666	Fixed an issue in which the ATA did not request files if the profile rule specified HTTP.
CSCtx49628	Fixed an issue in which a username and password could not be passed to the ATA for a resync operation.
CSCtx53264	Fixed an issue with the use of an encrypted configuration file and a -key parameter.
CSCtx89777	Fixed an issue in which changes in the DTMF Playback Length value did not take effect.
CSCty14865	Fixed an issue in which a reboot loop occurred after the settings for VMWI Ring Policy and VMWI Ring Splash Len were changed.
CSCty30504	Fixed an issue in which the ATA did not honor DHCP OPTION 15.
CSCty62166	Fixed an issue in which a valid time server address was not accepted by the web-based configuration utility.
CSCty84042	Fixed an issue with extra lines in the SPC output for this ATA.
CSCty85573	Fixed an issue in which the ATA could not resolve CNAME for the provisioning server.

Tracking Number	Description
CSCtz07186	Fixed an issue in which an ATA no longer operated in bridge mode after receiving a configuration update through TFTP.
CSCtz07729	Fixed an issue with missing SNMP parameters in the SPC template.
CSCtz15420	Fixed an issue in which the ATA did not attempt registration if the proxy was identified by a domain name.
CSCtz26143	Fixed an issue in which an ATA could not be configured in bridge model from a configuration file.
CSCtz26162	Fixed an issue in which an error in a configuration file caused the ATA to become unresponsive.
CSCtz26618	Fixed an issue in which the ATA sent an invalid NONCE, resulting in a 401 Unauthorized response.
CSCtz38321	Added new DTMF transmit methods: InBand + INFO and AVT + INFO) to allow the configuration of multiple DTMF transmission methods on the ATA.
CSCtz53215	Fixed an issue in which modem tones were heard upon answering and during Call Waiting.
CSCtz76693	Fixed an issue in which the ATA could be reset from the IVR even though the Protect IVR Factory Reset parameter was set to Yes.
CSCua00242	Fixed an issue in which the ATA became unresponsive or rebooted itself after receiving a SIP invite containing a display name with more than 26 characters.
CSCua08194	Fixed an issue in which DNS SRV lookup failed.
CSCua09987	Fixed an issue in which a static IP address could not be set from a configuration file.
CSCua36631	Fixed an issue in which the administrator password could not be set from a configuration file.

Tracking Number	Description
CSCua61320	Fixed an issue in which the ATA did not send a SIP reINVITE after detecting a CNG tone.
CSCua61325	Fixed an issue in which the ATA changed the session ID after detecting a CNG tone, violating RFC3624 and resulting in a 408 Not Allowed Here response.
CSCub02239, CSCub16975	Fixed issue in which an ATA rebooted frequently after retrieving files from the server.
CSCub22461	Fixed an issue in which the ATA did not resync after a reboot.

Known Issues

- The static IP address, network mask, and gateway IP address are not successfully changed by using the IVR after disabling DHCP. (CSCtx26394)
  Work Around: Retry or use the web-based configuration utility to change the settings.
- On Cisco SPA112, when HTTPS is selected on the *Administration > Management > Web Access Management* page, the Remote Management Port field does not show the correct default value, 443.
  Work Around: Enter the value 443 in the field before submitting the changes.

Upgrading the Firmware

Follow these instructions to upgrade the phone adapter.

STEP 1 Download the latest firmware by using the Firmware link on the following web page: www.cisco.com/go/smallbizvoicegateways

STEP 2 Launch a web browser, and enter the LAN IP addresses of the phone adapter.

STEP 3 Log in to the Configuration Utility.

STEP 4 Click **Administration** in the menu bar, and then click **Firmware Upgrade** in the navigation tree.

STEP 5 Click **Browse** and select the location of the upgrade file that you downloaded.

STEP 6 Click the **Upgrade** button to upgrade the firmware.

NOTE Upgrading the firmware may take several minutes. Until the process is complete, DO NOT turn off the power, press the hardware reset button, or click the Back button in your current browser.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Downloads and Documentation	
Firmware	www.cisco.com/go/software
Cisco Small Business Voice Gateways Documentation	www.cisco.com/go/smallbizvoicegateways
Open Source Documentation	Follow the Release Notes link at www.cisco.com/go/smallbizvoicegateways
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

78-20713-02