Release Notes for Cisco Unified Communications 300 Series UC320W Firmware Version 2.2.2

March 2012

These Release Notes describe the changes, known issues, system requirements, and firmware upgrade procedures for Cisco Unified Communications 300 Series UC320W 2.2.2.

Contents

This document includes the following topics:

Enhancements in Firmware Version 2.2.x

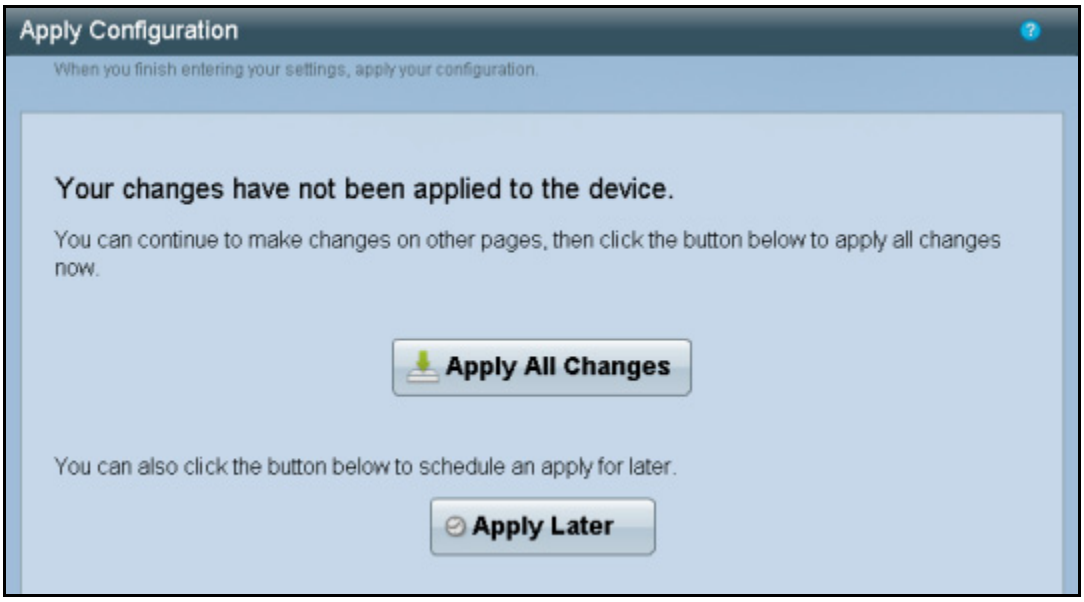
The following enhancements are included in firmware version 2.2.x:

Faster Configuration Changes

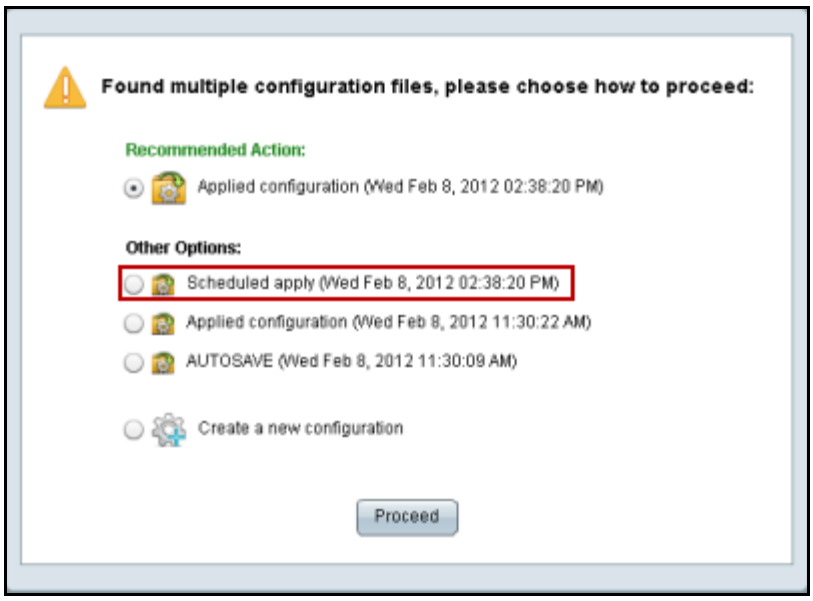
Most configuration changes are completed more quickly than in earlier versions of the firmware. When you apply a configuration change, the Cisco UC320W and connected devices are rebooted only for certain types of changes.

Apply Later Option for Configuration Changes

When applying a configuration change, you have the option to use the *Apply Later* button to schedule the update at a convenient time.

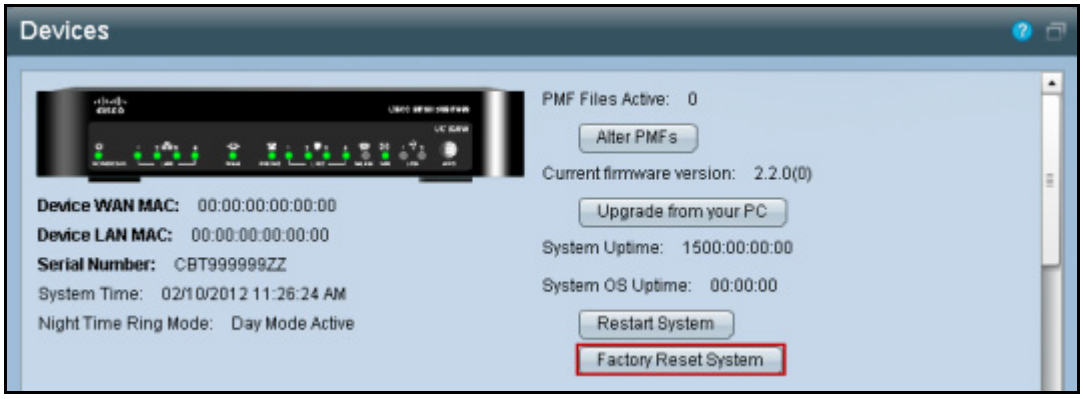


NOTE If you launch the configuration utility before the scheduled time for the configuration update, the "Scheduled apply" will be listed among the possible configuration files that you can load. To continue where you left off in the previous session, choose the "Scheduled apply." Make any changes, as needed, and then either apply the configuration or use the *Apply Later* button to schedule it.



Factory Reset from the Configuration Utility

You can perform a factory reset from the Configuration Utility. From the *Status* > *Devices* page, click the *Factory Reset* button to return the Cisco UC320W to the default factory settings.



NOTE Be aware that the system will restart, phone calls will be interrupted, network traffic will stop, and custom settings will be abandoned. The username/password will be reset to cisco/cisco. If you selected a network topology other than the *Cisco*

UC320W Routes Voice and Data option, you should disconnect the Cisco UC320W from the LAN to prevent DHCP server conflicts while you reconfigure the Cisco UC320W.

Classes of Restriction and Dialing Privileges

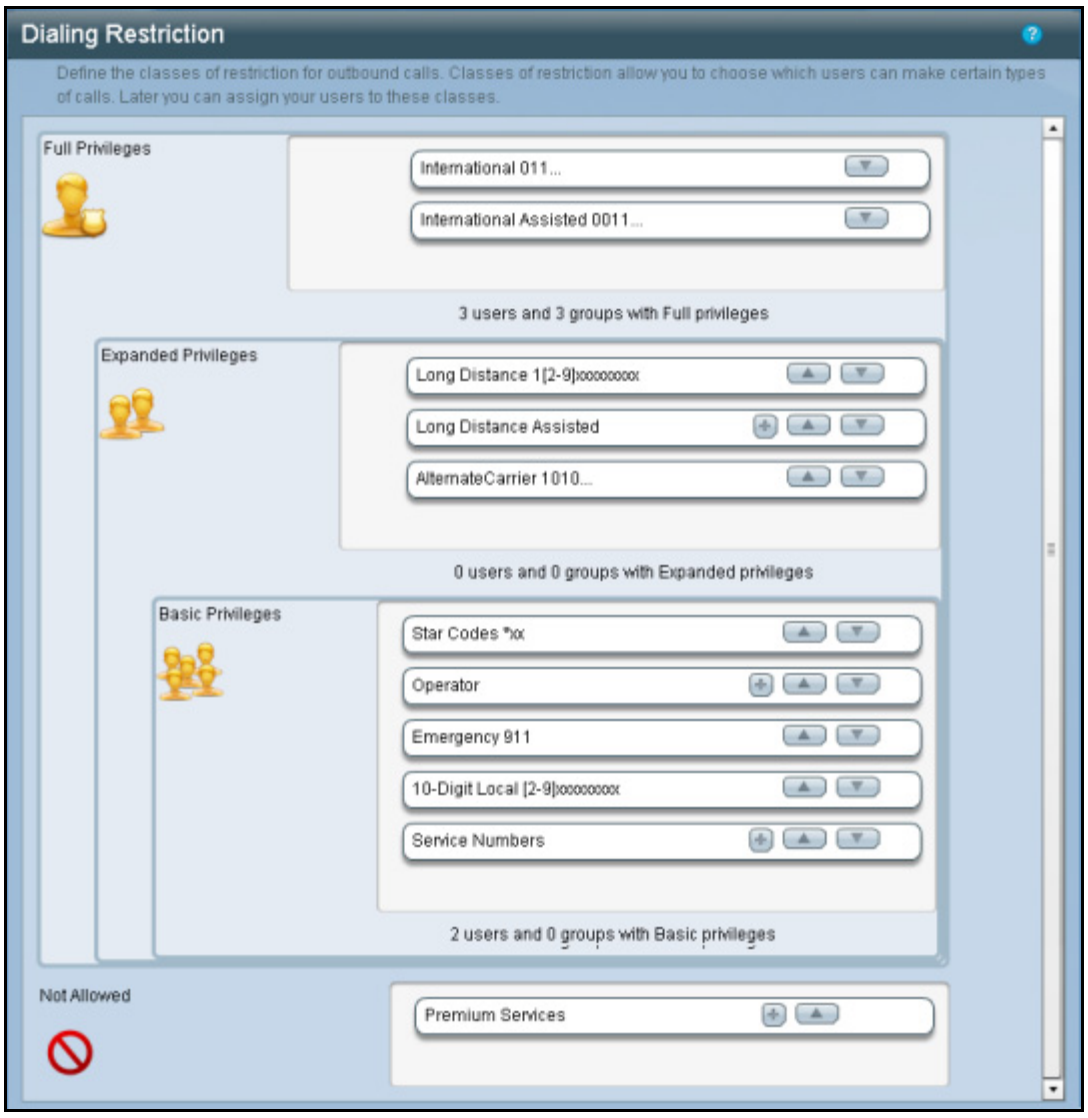
You can block or allow certain types of calls based on known dialing patterns. There are four classes: Not Allowed, Basic, Expanded, and Full. Keep the default settings, or customize them to meet your needs.

U.S. example:

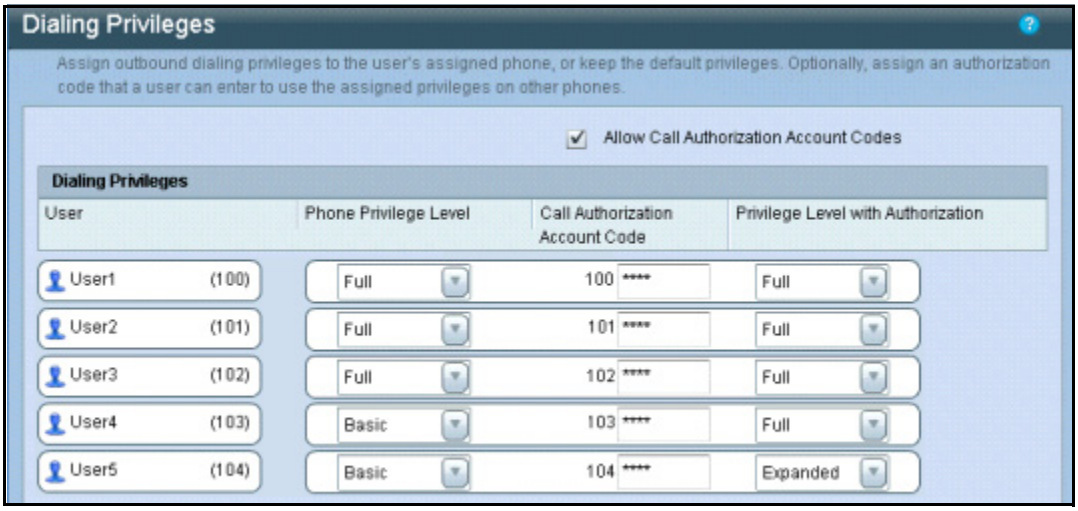
- A company wants to block all outbound calls to toll numbers such as 1900 or 1976 numbers. The administrator configures the Not Allowed class to include these dialing patterns.
- Visitors need to be able to place local calls from the lobby phone. The administrator configures the Basic class to allow only local dialing. The Lobby user is assigned Basic dialing privileges.
- Employees need to be able to dial long-distance calls. The administrator configures the Expanded class to allow long-distance calls. Most users are assigned Expanded dialing privileges.
- The CEO and Manager need to be able to dial international numbers. The administrator configures the Full class to allow international dialing patterns. The CEO and Manager are assigned Full privileges.

NOTE Dialing restrictions do not affect calls that are directed to external numbers from the Auto Attendant, Call Forwarding, or Call Routing.

Use the *Configuration > Telephony > Dialing Restriction* page to set up the classes of restriction.

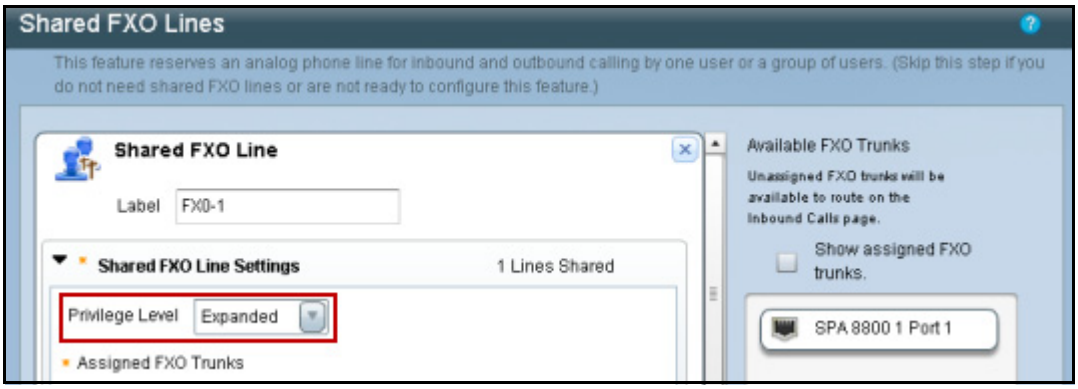


Use the *Configuration > User/Group Features > Dialing Privileges* page to assign dialing privileges to users. By default, all users have Full dialing privileges. The assigned privileges apply to a user's personal extensions and additional extensions. If needed, you can enable call authorization account codes to require a user to enter a code to access higher dialing privileges. With a code, users can access their dialing privileges from any phone in the office.



To ensure that each user has a unique call authorization account code, the system prepends the user's personal extension number to the configured authorization code. Example: The administrator configures a code of 1234 for the user at extension 101. When placing a restricted call, the user enters 1011234.

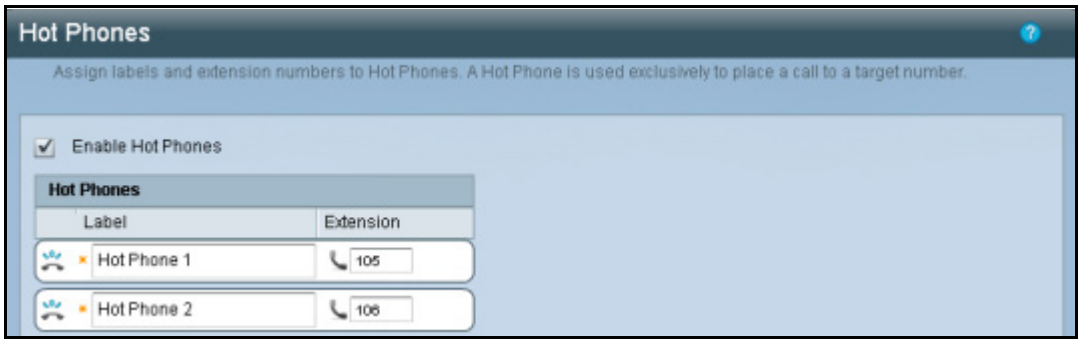
You can assign a dialing privileges to a Shared FXO Line or a Shared Extension by using the *Privilege Level* drop-down list. Be aware that members can be added to the group only if their dialing privileges are equal or greater than those of the group.



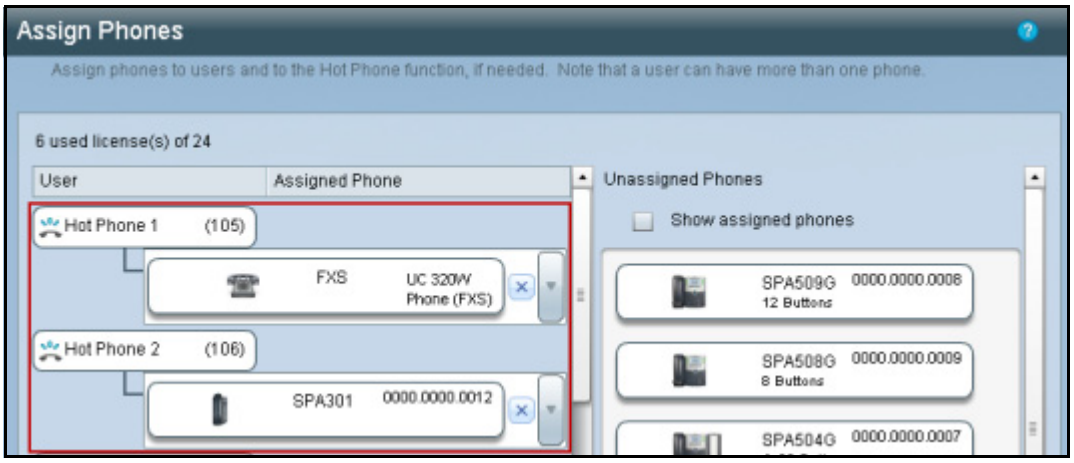
Hot Phones

In certain areas of the office, you may need a phone that customers, guests, or employees can use to call a target number quickly. A hot phone serves this purpose. For example, a delivery person at the back door could use a hot phone to immediately call an attendant. The system supports up to two hot phones.

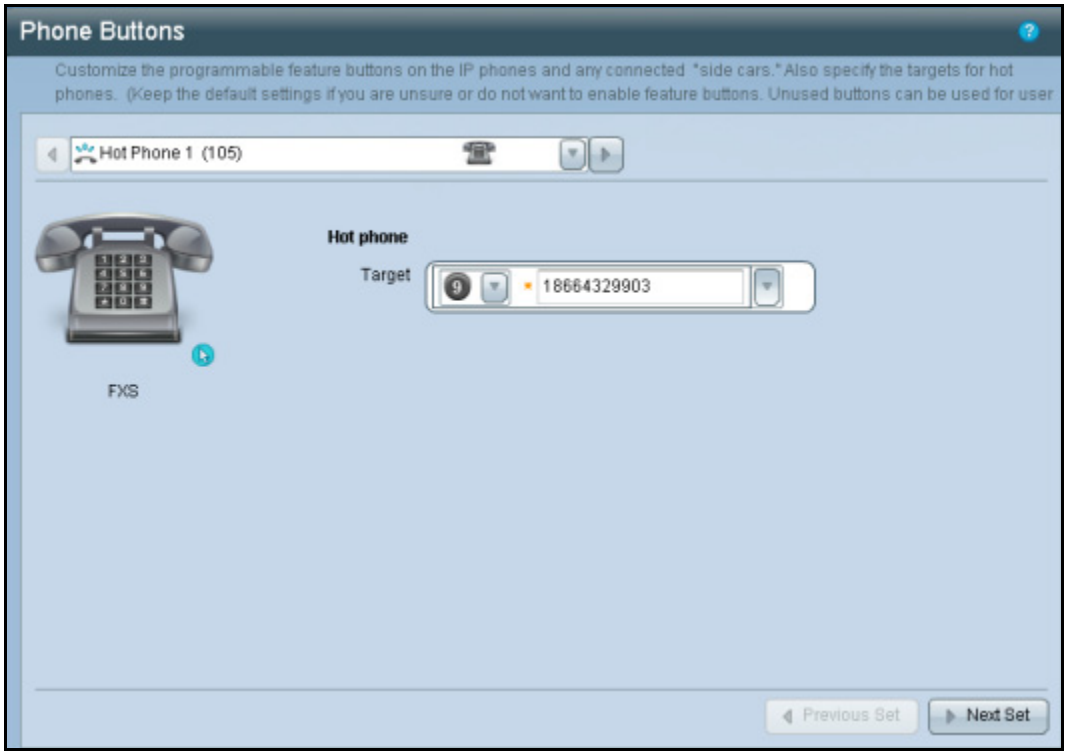
You can enable this function on the *Configuration > Users/Phones > Hot Phones* page.



Assign this function to phones on the *Assign Phones* page.

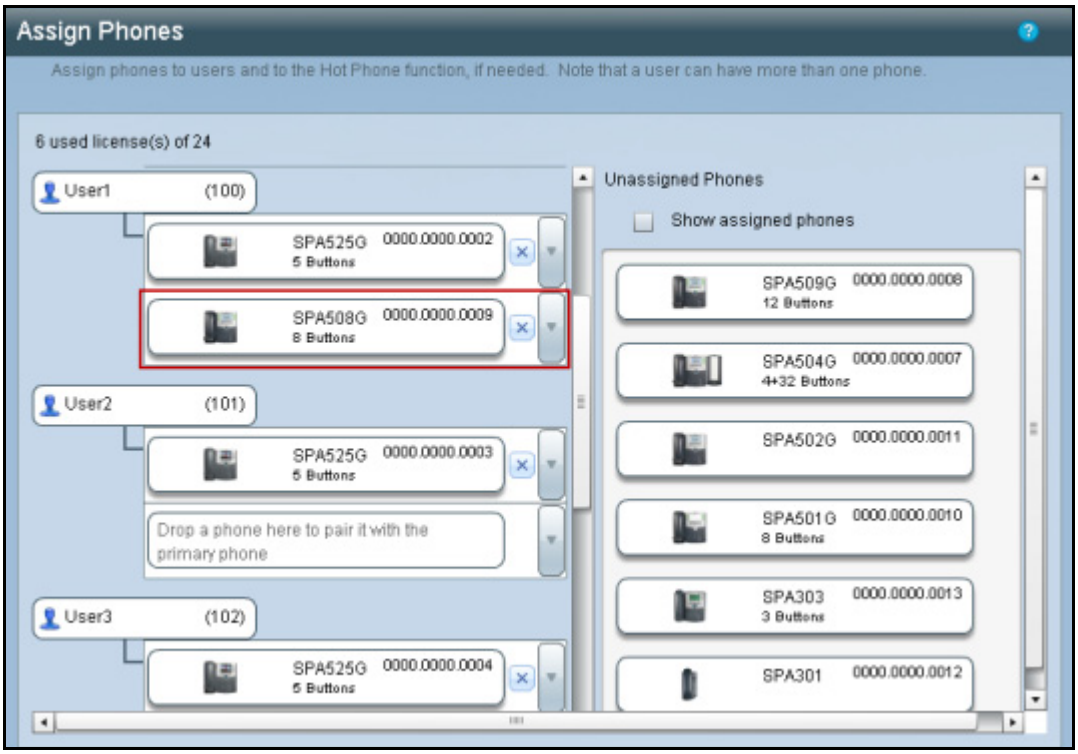


Finally, specify the target number on the *Configuration* > *User/Group Features* > *Phone Buttons* page.



Paired Phones

If a user divides time between two locations in the office, you can assign a secondary phone. The paired phone inherits the phone buttons from the primary phone, up to the total number of available buttons on the selected phone model. Make this pairing on the *Configuration* > *Users/Phones* > *Assign Phones* page.

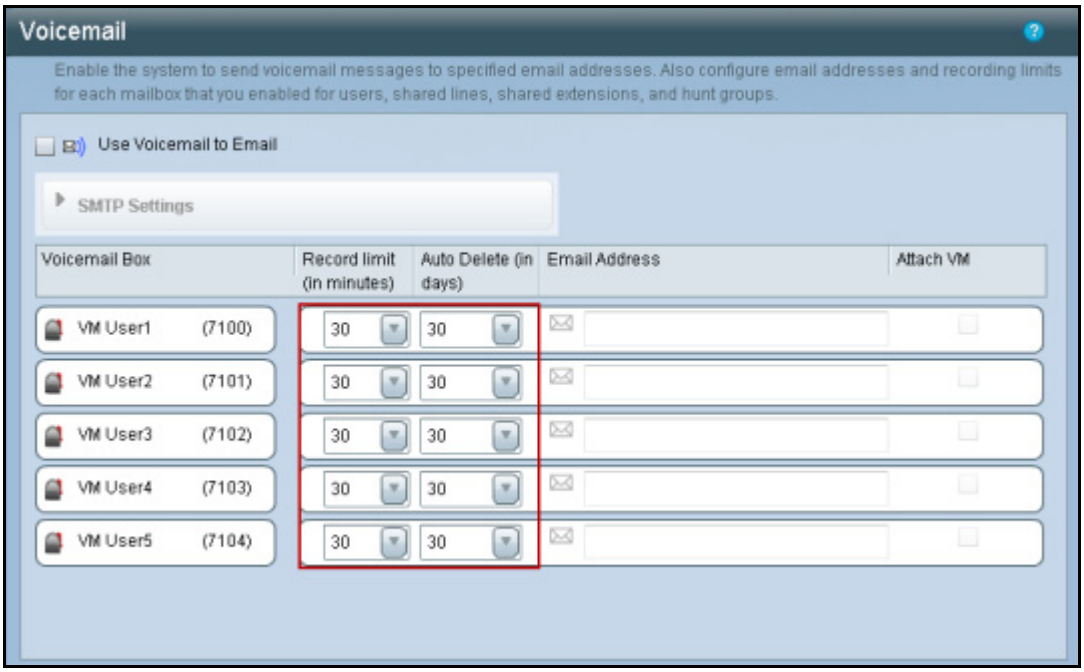


NOTE Because the paired phone is secondary to the primary phone, there are some differences in functionality.

- A paired phone has no soft key to forward all calls. It uses the call forward settings that are configured for the user in the Configuration Utility.
- Pressing the Do Not Disturb (DND) softkey on a primary phone will prevent calls from ringing on the phone; however, calls will ring on the paired phone. A call is not diverted to the Call Forward No Answer destination until the timeout limit is reached. Pressing the DND softkey on the paired phone will divert calls to the specified Call Forward No Answer destination.

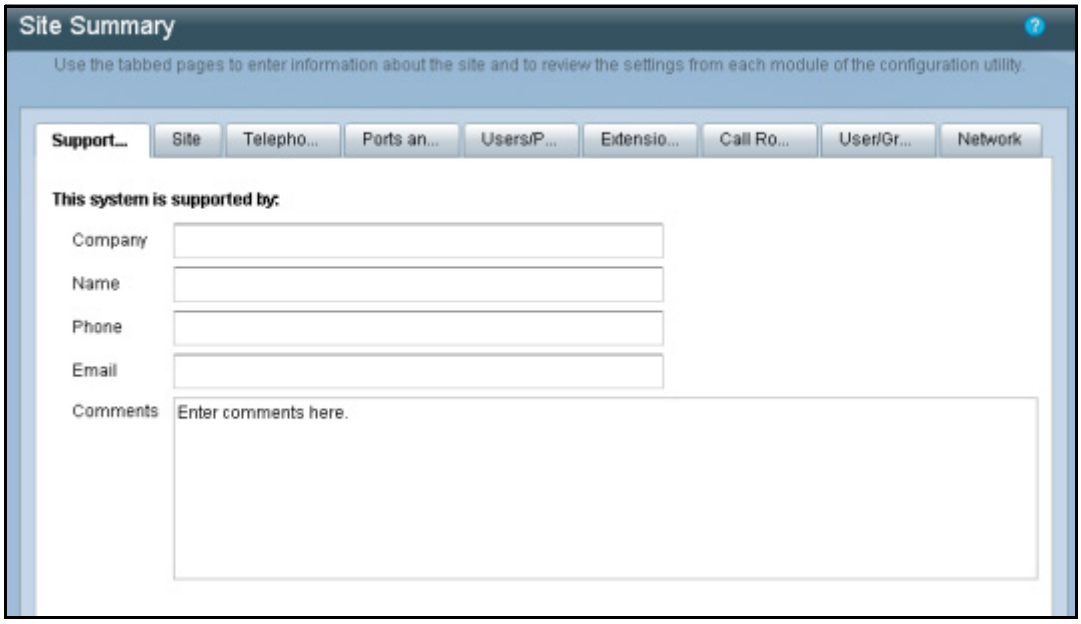
Per-user voicemail limits

Because the default per-user voicemail storage limit of 30 minutes may be inadequate for some users, you now can adjust the Record Limit for each user. You can also adjust the Auto Delete period; messages are automatically deleted after the specified number of days. Mailboxes are still subject to the system total voicemail storage limit of 20 hours and the per-user new-message limit of 100 new messages. You can set the Record Limit for each on the *Configuration > User/Group Features > Voicemail* page.



Partner contact information

You can record your contact information on the *Configuration > Apply Changes > Site Summary* page.



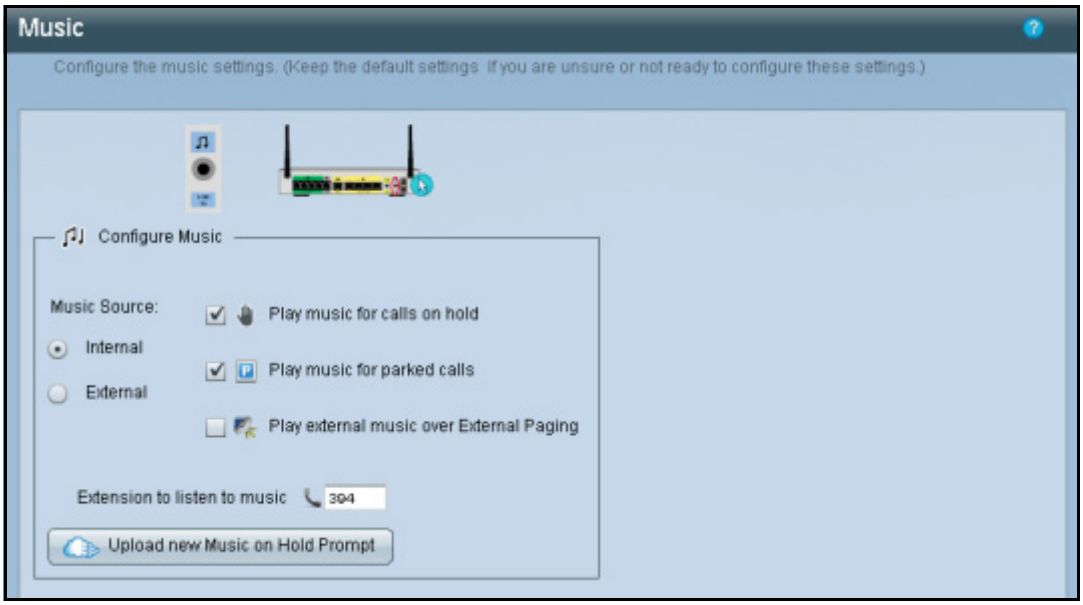
Expanded Options for Music on Hold and AA Prompts

When the Cisco UC320W is connected to Cloud Services, you can upload your own audio files for Auto Attendant prompts and Music On Hold. A service on the Cloud converts the files to the proper format and length and installs them on the Cisco UC320W, ready for use.

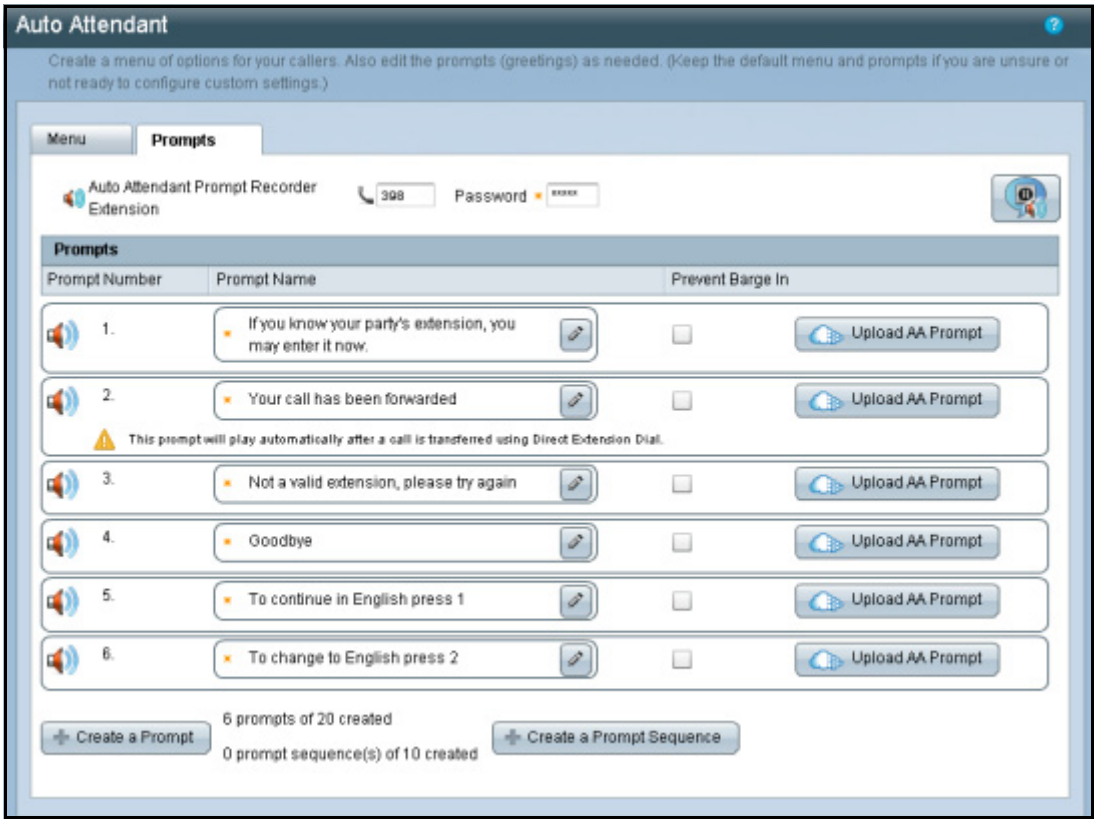
Requirements and limitations:

- The internal music on hold file is limited to 60 seconds.
- Each AA prompt file is limited to 120 seconds.
- The supported audio file formats are MP3, WAV, WMA, AAC, and AIF.

On the *Configuration* > *Telephony* > *Music* page, click the **Upload new Music on Hold Prompt** button. You will then be prompted to upload a file from your computer. Cloud Services will convert the file, which will become the **Internal** music source.



On the *Configuration > Call Routing > Auto Attendant* page, click the **Upload AA Prompt** button to upload a prompt into each position., as needed. Be sure to edit the Prompt Name to reflect the content of the custom file.



Packet Size Setting for SIP Trunks

You can set the packetization interval for your Voice over IP calls. This setting determines the size of the audio samples in each packet. A smaller value may prevent voice quality issues by reducing the overall delay. However, the bandwidth usage will be higher when sending more, smaller packets. A larger value may improve the network utilization. The default setting is recommended for most small businesses.

Modification of the Auto Attendant Prompt Recorder Password

You can change the Auto Attendant Prompt Recorder password from the *Configuration > Telephony > Internal Dialing* page and the *Configuration > Call Routing > Auto Attendant > Prompts* page.

Priority Paging

Paging group features are simplified in this release. By default, sending a page to a group will not interrupt any users who are on a call. However, you can configure a group with Priority Paging, which causes pages to sound on all members' phones.

Wireless Client Status

The status of wireless clients is shown on the new *Status > Wireless Clients* page.

New Ringtones

Two new ringtones are available on the IP phones: Du-Dut and Pulse.

Device Firmware

This version of the Cisco UC320W firmware includes the following device firmware.

- **Cisco SPA525G/G2:** 7.5.1(RC1)
- **Cisco SPA30x/SPA50x:** 7.5.1(RC1)
- **Cisco SPA8800:** 6.1.10(GW003)

Issues Fixed Since Firmware Version 2.2

- Fixed a Voicemail to Email issue involving addresses with more than one period in the domain name. (CSCty29315)
- Fixed an issue with firmware upgrades on systems with Region Packs. (CSCty30314)
- Fixed an issue with loading a saved configuration that included a Region Pack. (CSCts35159, CSCts35195)
- Fixed an issue in which the default dial plan was corrupted after installing a Region Pack from the Cloud. (CSCts38887)
- When the system is configured for Austria, the phone displays the extension number of the calling party with an exclamation point, such as !100) (CSCtr73551)

- Released new phone firmware to fix an issue in which the Cisco SPA301 IP phone became non-functional when the region was set to Ireland. (CSCtw64357)
- Fixed an issue with the DTMF playback parameters (DTMF_Playback_Level and DTMF_Playback_Twist) for DTMF signalling when the region is set to Malaysia. (CSCtt94775)
- Fixed an issue in which heavy use of Universal Plug and Play (UPnP) may have leaked resources and caused network performance to degrade. (CSCtu21473)
- Fixed intermittent issues in which the phone display froze and the call lost audio during callback or when receiving a second incoming call. (CSCtu31473)
- Fixed an issue in which the generation of an internal configuration file resulted in an empty configuration file, resulting in problems with impedance matching and failure of analog calls. This fix will rebuild the configuration file on impacted systems. (CSCtu21627)
- Fixed issues with the Italian dial plan settings that prevented outbound routing of emergency numbers through some FXO lines. (CSCtt42316)
- Fixed issues that prevented the dialing of 0825 and 07 numbers in the French dial plan. (CSCtu10072)
- Modified the North American dial plan for 0+ address dialing.
- Fixed issues that occurred in the internal dial plan after a region pack was installed from the Cloud. (CSCtu02726)
- Added the Puerto Rico Time Zone (GMT -4) to the time zone options for the United States. (CSCts71888)
- Fixed an issue with the caller ID for missed calls.
- Fixed an issue in which the voicemail system failed to detect user inputs on calls received via a SIP trunk. (CSCts56514)
- Fixed an issue in which callers heard garbled Auto Attendant prompts when the codec was set to G729a and the region was set to a dual language. (CSCts44317, CSCts41524)
- Fixed an issue in which the default Auto Attendant prompts were garbled when the codec was set to G729a and the prompts were played back through the Auto Attendant Prompt Recorder. (CSCts41524)

- Fixed an issue affecting the display of caller ID on FXO calls from certain telephone service providers. (CSCtt05088)

Known Issues

This section includes the following types of issues:

Browser Options for Configuration Utility

Cisco recommends the following web browsers for use with the Cisco UC320W Configuration Utility:

- Internet Explorer version 7, 8, or 9
  Note: Adobe Flash does not support 64 bit versions of IE on XP or Vista.
- Firefox version 3.6.19
- Safari version 4 or 5
- Google Chrome 10

NOTE

- Because the configuration utility requires Adobe Flash Player, it is not compatible with Apple iPhone, iPod Touch or iPad devices.
- Do not run the configuration utility from a computer that is connected to the PC port of a Cisco IP phone. When you apply the configuration, which causes the phone to reboot, you will lose connectivity to the configuration utility. Instead, run the configuration utility from a computer that is connected either to a LAN port of the Cisco UC320W or to the LAN port of a switch that has connectivity to the Cisco UC320W.

System Management

- When Internet Explorer is used to download a firmware file from the Cloud, the pop-up window may not appear after the Save As button is clicked. (CSCty16738)
  Work Around: Restart Internet Explorer and try the operation again.
- Login fails when using Google Chrome for remote management via HTTPS. (CSCtx77008)
  Work Around: Use Internet Explorer or Firefox for remote management of the Cisco UC320W. Note that this feature must be enabled on the *Configuration > Site > System Access* page.
- After restoring a configuration with different LAN or network topology settings than were in use for the current session, there may be issues launching the configuration utility. (CSCtn57188)
  Work Around: Ensure that your PC received an IP address in the correct range for the restored configuration. Restart the browser and enter the new IP address for the Cisco UC320W.
- With very high data traffic to and from the WAN (rates over 100MB), system performance may be slow. Administrators also will notice slow performance in the configuration utility. (CSCtj13887)
  Work Around: Configure the Cisco UC320W as a DHCP client of the data network, if WAN network throughput above 100 Mbps are required.
- There are intermittent issues in which configuration changes are not passed down to a Cisco SPA8800 gateway. (CSCtk15802)
  Work Around: To synchronize configuration changes, factory reset the Cisco SPA8800 by using the built-in IVR. Connect an analog phone to FXS Port 1 of the unit. Press the star key four times: ****. After the greeting plays, enter the R-E-S-E-T option, followed by the pound key: **73738#**. Press **1** to confirm.
- The Cisco UC320W does not support detailed logging of activity on Cisco SPA8800 FXO ports. Consequently the *Status > Support Tools > System Logs* page does not list those ports. (CSCtn59149)
  Work Around: If debug logging of a particular FXO line is required, swap ports to place that line on a UC320W FXO port.
- Spanning Tree Protocol is not currently implemented in the built-in switch of the Cisco UC320W. The administrator must be careful not to introduce any Layer 2 network loops. (CSCtl77145)

- Creating a new configuration does not erase Call History logs from the phones. (CSCtn08849)
  Work Around: After initiating a new configuration in the configuration utility, use the phone menus to factory reset the phones. Instructions are provided below.
  - **Cisco SPA301 or Cisco SPA501:** Lift the receiver, and access the Interactive Voice Response unit by pressing the * key four times: ****. Enter the R-E-S-E-T option, **73738**, followed by **#**. Press **1** to confirm. Wait about 40 seconds for the *Option Successful* message, and then hang up.
  - **Cisco SPA303 and other Cisco SPA50x Series models:** Press the Setup key on the phone keypad. Scroll down to **Factory Reset**, and press **Select**. When the confirmation message appears, select **OK**.
  - **Cisco SPA525G/G2:** Press the Setup key on the phone keypad. Scroll down to **Device Administration**, and press **Select**. Scroll down to **Factory Reset**, and press **Select**. When the confirmation message appears, select **OK**.
- After an attempt to load a configuration file with the same wireless settings as the current configuration, the wireless SPA525G phones get stuck in a resynchronization loop. (CSCtq64852)
  Work Around: Use the Setup menu on the phone to reboot the phone.
- Intermittently, during an attempt to restore a configuration, an error occurs and the Configuration Utility becomes non-responsive. (CSCts41575)
  Work Around: Wait a few minutes for the operation to finish. Then re-launch the Configuration Utility and apply the configuration.

Audio Quality

- Echo may be heard if the IP phones are connected to a switch that is not configured with a voice VLAN. (CSCth53813)
  Work Around: Cisco recommends Cisco Small Business 300 Series Managed Switches and Cisco ESW500 Series Ethernet Switches. These switches require no special configuration for use with the Cisco UC320W. Other switches may require special configuration of the voice VLAN (100). For more information about switch configuration, see www.cisco.com/go/partner/smartdesigns

Dialing and Call Routing

- Service Numbers [2-7]11 cannot be dialed if call authorization account codes are disabled. (CSCty35868)
  Work Around: Enable call authorization account codes.

- If a dial pattern is similar to a longer pattern, placing the shorter pattern in the Not Allowed class of restriction will also block the longer pattern. For example, when the United States is selected as the region, placing Operator (0) in the Not Allowed class will block the dial patterns for International 011 and International Assisted 0011. (CSCty33504)
  Work Around: Instead of blocking the shorter dial pattern, you can place it in the Full class of restriction, permitting this pattern only for authorized users.
- If calls over SIP trunks require Expanded dialing privileges, and a user with Basic dialing privileges uses an authorization code to access the higher privileges, the authorization code is rejected. This issue occurs only for calls over SIP trunks. (CSCty33247)
  Work Around: Assign higher dialing privileges to the user, or place the dialing pattern in a lower class of restriction.
- When a call is placed to an external number through an FXO trunk, there is a long delay before the ringback tone plays. (CSCtl49731, CSCtj57861)
- When the Outside Line digit is not 9, the system ignores the Emergency Trunk Assignment settings on the *Configuration > Ports and Trunks > Outbound Trunks* page. Instead, the Outbound Trunk Assignment settings are used for emergency calls. (CSCtq65533)
  Work Around: Use 9 as the Outside Line digit.

Voicemail

- On the *Status > Voicemail* page, the Used column does not reflect the Record Limit from the *Configuration > User/Group Features > Voicemail* page. (CSCtx76368)
- If a user records a temporary greeting, it remains in use until it is deleted. (CSCtn56684)
  Work Around: If a user no longer wants to use a temporary greeting, the user can log in to the mailbox and go through these options: Press **4** for setup options, press **4** for the temporary greeting, and then press **2** to erase the temporary greeting.
- When a Shared Extension or Hunt Group is busy, the caller hears the “unavailable” greeting instead of the “busy” greeting. (CSCtj21082)
- When all Hunt Group members are busy, the call is not forwarded to voicemail. (CSCtk68137)
- The voicemail callback feature fails for a message left by an external caller. (CSCtl20136)

- When voicemail boxes are reinitialized from the *Status > Voicemail* page, SIP calls may experience intermittent silences or distorted audio. (CSCtr70807)
  Work Around: Perform this type of task during periods when you are least likely to affect user activity.

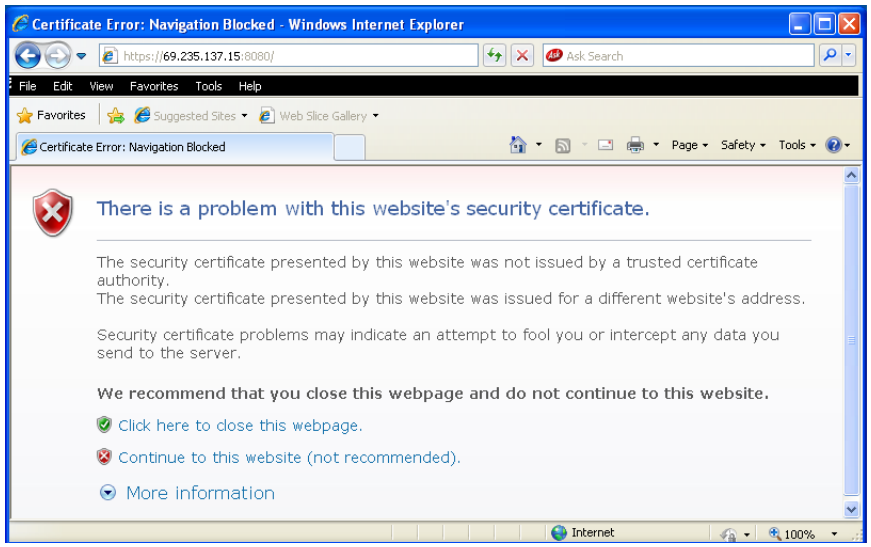
Display Issues in the Configuration Utility

- When Internet Explorer is used, the Upgrade button on the *Status > Devices* page may appear to be unavailable when in fact it is functional. (CSCty13494)
  Work Around: Click the button to upgrade the firmware.
- Very long drop-down lists, such as a long list of voicemail boxes, are partly hidden from view. (CSCtj61728)
- The *Status > External Trunks* page continues to show the state as Registered even when the Cisco UC320W loses its WAN connection. (CSCtr72901)
- After a user changes the phone language settings by using the phone menu, the SPA525G display remains in English. (CSCts21464)

Other

- In the Stations directory on the phone, extension numbers are prepended with the numerals 777. This issue is a display issue only, and does not cause any issues in dialing. (CSCty26565)
- Changes in wireless client status are not reflected promptly on the *Status > Wireless Clients* page. (CSCtx65911)
- FXS phones are omitted from the Stations Directory on the phones. (CSCtf45911)
- On a wireless network with Security Strength set to None, changes in the Network Name (SSID) are not successfully communicated to wirelessly connected phones. (CSCtl43344)
  Work Around: Use a stronger security setting (strongly recommended). Alternatively, work around this issue by temporarily connecting the wireless phones to the network with Ethernet cables. After the phone reboot, they will receive the new wireless network settings, and you can disconnect the cables.
- The star codes for parking and unparking calls (*38 and *39) do not work on FXS phones. (CSCth88200)

- The settings menu on the phone screen allows the user to edit the IP address and other network settings. Users should not change these settings. Any changes will be overwritten by the settings entered in the configuration utility. (CSCti02670)
- Star code 66 (call back) does not work on analog phones. (CSCto74691)
- After an initial configuration is applied, further changes in the phone language preference may be made only through the phone menus (to avoid losing user settings).
  Work Around:
  - On SPA50x models, press the Setup button and then choose the Language menu. Choose a language from the list, and then press Select.
  - On SPA525G/G2, press the Setup button and then choose the Device Administration menu. In the Language field, press the right-arrow navigation button, choose a language from the list, and then press Select.
- A certificate warning may appear when you connect to the configuration utility by using HTTPS. You can acknowledge the message and continue to the website. (CSCtn24097)



- When you restart the Cisco UC320W from the *Status* > *Devices* page, the phones' Call History records remain. To remove Call History records, reset the phones by using the phone menu.
- When a call is forwarded to an external number, the call is not identified with the user-specific CLID but instead uses the default CLID for the SIP trunk. (CSCtr07810)

- Call transfers to external numbers fail from an analog phone that is connected to a Cisco SPA8800 FXS port. (CSCtr76487)
- The Auto Attendant cannot successfully transfer a call to a “gentle page” group. The caller hears a disconnect tone after the transfer attempt. (CSCts55754)
- If the WAN is not connected or the NTP server is not reachable, you can set the system clock from a phone. Be aware that this manual setting will be lost if the Cisco UC320W loses power.

  To set the system time by using a Cisco SPA300 or SPA50x Series IP phone:

  1. Press the Setup button.
  2. Select **Time/Date**. Enter the date in the mm/dd/yy format. Press ***** or **#** for the forward slash. For example, enter 10*01*11 for Oct. 10, 2011.
  3. Press the down-arrow navigation button, and then enter the time in hh:mm:ss format. Press * or # for the colon. For example, enter 6*21 for 6:21.
  4. Press the down-arrow navigation button, and then enter the time zone **Offset** in ±H:m:s format. Press * for + or # for -. Press * or # for the colon. For example, in the U.S. Pacific Time zone, enter *8*00 for -8:00.
  5. Press **save**.
  6. Press the Setup button to close the window. The time setting is propagated to the UC320W and the other phones.

  To set the time on Cisco SPA525 and Cisco SPA525G IP phones:

  1. Press the Setup button.
  2. Select **Device Administration**.
  3. Select **Date/Time**.
  4. Move the cursor to **Set Current Time Manually**. Press the right-arrow navigation button.
  5. In the table, press the up or down navigation button to move up or down in the list. Press the right or left navigation button to move to a different field.
  6. After entering the year, month, day, hour, and minute, press **Save**.
  7. Press **Set**.

8. Press the Setup button to close the window. The time setting is propagated to the UC320W and the other phones.

Required Equipment and Services

For best results, please be aware of the following requirements:

- **Internet service:** An active Internet connection is required, and the system must be able to establish a WAN connection during the initial configuration process.
  Note: The phones and Cisco SPA8800 gateways restart when the Internet connection is lost or the WAN IP address changes (for example, when a DHCP lease expires). If you have ongoing issues with DHCP lease renewal, consider obtaining a static IP address from your Internet Service Provider.
- **Ethernet switch selection:** If you wish to install an Ethernet switch with your Unified Communications system, Cisco recommends Cisco Small Business 300 Series Managed Switches and Cisco ESW500 Series Ethernet Switches. These switches require no special configuration for use with the Cisco UC320W. Other switches may require special configuration of the voice VLAN (100). For more information about switch configuration, see www.cisco.com/go/partner/smartdesigns
  Note: Be sure to upgrade your switch to the latest firmware before installing it into the Cisco UC320W LAN.
- **Adobe Flash player**: The configuration utility requires the free Adobe Flash player version 10.1 or later. Only version 10.x is compatible with UC320W releases prior to UC320W version 2.1.2. To install version 10.x, see http://kb2.adobe.com/cps/142/tn_14266.html#main_Archived_versions. If you are upgrading from UC320W version 2.1.2 and wish to install the latest version of the Flash player, see http://get.adobe.com/flashplayer/.

Upgrading the Firmware

Cisco recommends that you install the latest firmware as it becomes available. You can install the firmware from the Cloud or from a file on your computer.

NOTE If you are upgrading from a firmware version earlier than 2.0.12, you must first install interim version 2.0.12(8). If you do not install the interim release first, the upgrade to 2.2.2 will fail. This two-part process is streamlined by installing the firmware from the Cloud.

See the following topics:

- **Installing Updates from the Cloud (Recommended), page 25**
- **Upgrading from a File on Your PC, page 25**

NOTE

- As a best practice, back up your configuration before you begin the upgrade process.
- If the new firmware involves changes in required settings, error icons may appear on some configuration pages after the upgrade is completed. Read the messages on the screen to learn more.
- Configuration files are not backward compatible. If you back up a configuration file and later downgrade to an earlier version of the firmware, you cannot restore that configuration file.
- For best results, close other browser windows before starting an upgrade. When other browser windows are open, the browser may display memory errors.
- Due to the large file size, do not use a wireless connection to upgrade the firmware.
- For best results, ensure that the WAN port of the Cisco UC320W is physically connected to your WAN or Internet access device.
- If you have a slow WAN link or are experiencing errors on the WAN connection, the application may stall when attempting to install updates from the Cloud. If this occurs, use the manual upgrade process instead. See **Upgrading from a File on Your PC, page 25**.

Installing Updates from the Cloud (Recommended)

When the Cisco UC320W has access to the Cloud, firmware updates are offered periodically. Cisco recommends installing the latest firmware. You can click a button to immediately upgrade the firmware, or wait for a more convenient time.

NOTE

- If you are upgrading from a firmware version earlier than 2.0.12, the Upgrade Utility streamlines the required two-step upgrade process.
- This process requires an active Internet connection.

Performing the two-step upgrade by installing from the Cloud:

STEP 1 When the *Firmware Available* window appears, click the **Install** button for firmware version 2.2.2. If this window does not appear, click the **Upgrade Available** link to display it.

STEP 2 Read the message about the two-step process, and then click **Continue**. The *Update Status* window appears, and status indicators display the progress of the upgrade.

STEP 3 When the **Restart the Configuration Utility** button appears, click it to continue with the second part of the upgrade process. The *Update Status* window reappears, and status indicators display the progress of upgrade.

STEP 4 When the login window appears, enter your username and password and click **Log In**.

STEP 5 Click the **Apply Configuration Required** button to apply the updates to the connected hardware.

Upgrading from a File on Your PC

Use this procedure if you have a slow WAN connection or if you prefer to upgrade the firmware without being connected to the Internet.

IMPORTANT: When using the Upgrade Utility, do not factory reset the Cisco UC320W.

NOTE If you are upgrading from a firmware version earlier than 2.0.12, download the files for firmware version 2.0.12(8) and version 2.2.2. Then follow this procedure to complete the two-part upgrade process. If you do not install firmware version 2.0.12(8) first, the upgrade to Release Candidate 2.2.2 will fail.

STEP 1 After downloading the firmware, extract the BIN file from the downloaded ZIP file.

STEP 2 Install the firmware as described below.

Note: If you are upgrading from a firmware version earlier than 2.0.12, first install firmware version 2.0.12(8) and then immediately repeat this procedure to install version 2.2.2.

a. Launch the Cisco UC320W Configuration Utility.

b. Click the **Status** menu, and then click **Devices**.

c. Click the **Upgrade from your PC** button.

d. When the confirmation message appears, click **OK** to continue.

e. Select the BIN file for the firmware, and click **Open**. Status indicators appear as the upgrade proceeds.

f. When the upgrade is complete, the device status window appears. You can wait for all devices to be detected, or click the button to launch the Configuration Utility without waiting.

STEP 3 When the login window appears, enter your username and password and click **Log In**.

STEP 4 Click the **Apply Configuration Required** button to apply the updates to the connected hardware.

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco UC320W.

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/go/sbsc
Cisco UC320W Firmware Downloads	www.cisco.com/go/uc300

Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Product Documentation	
Unified Communications Cisco UC320W	www.cisco.com/go/uc300 Select the Resources tab for links to all technical documentation.
Smart Designs	www.cisco.com/go/partner/smartdesigns
Cisco SPA300 Series IP Phones	www.cisco.com/go/300phones
Cisco SPA500 Series IP Phones	www.cisco.com/go/spa500phones
Cisco SA500 Series Security Appliances	www.cisco.com/go/sa500
Cisco ESW500 Ethernet Switches	www.cisco.com/go/esw500help
Cisco Small Business 300 Series Managed Switches	www.cisco.com/go/300switches
Cisco SPA8800 IP Telephony Gateway	www.cisco.com/go/gateways
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-24884-01