Cisco Unified IP Phones 8961, 9951, and 9971 (SIP) Release Notes for Firmware Release 9.2(4)

Published: March 29, 2012

The information in these release notes apply to the Cisco Unified IP Phone 8961, 9951, and 9971. Use these release notes with a Cisco Unified IP Phone running SIP Firmware Release 9.2(4).

Contents

These release notes provide the following information. You might need to notify your users about some of the information provided in this document.

Related Documentation

Cisco Unified IP Phones 9951 and 9971 Documentation

Refer to publications that are specific to your language, phone model, and Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/en/US/products/ps10453/tsd_products_support_series_home.html

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Unified IP Phone 8961 Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/en/US/products/ps10451/tsd_products_support_series_home.html

Cisco Unified Communications Manager Documentation

Refer to the *Cisco Unified Communications Manager Documentation Guide* and other publications specific to your Cisco Unified Communications Manager release. Navigate from the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Business Edition 5000 Documentation

Refer to the *Cisco Unified Communications Manager Business Edition 5000 Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager Business Edition 5000 release. Navigate from the following URL:

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

New and Changed

The following sections describe the features that are new and changed in this release:

Note All Cisco Unified IP Phone 8961, 9951, and 9971 Firmware release 9.2(4) features are supported by Cisco Unified Communications Manager release 7.1(3) or later. Some features require a device pack to be installed.

Features Available with Firmware Release 9.2(4)

The following feature do not require the installation of a Cisco Unified Communications Manager device pack. These features do not require configuration and work by default after this firmware release has been applied to the phone.

This section contains the following topic:

Enlarge Unique Call Identifier

The Enlarge Unique Call Identifier feature is a user interface enhancement for the caller ID information.

This feature increases the font size of the unique call identifier to the same size as the calling number. No configuration is required for this feature.

This feature is supported on the following SIP phones:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951

- Cisco Unified IP Phone 9971

Features Available with the Cisco Unified Communications Manager Device Pack Containing the Cisco IP Phone Configuration Files

The following features require the installation of a Cisco Unified Communications Manager device pack containing the Cisco IP Phone configuration files. The device pack installs the firmware and the configuration files needed to enable the features. These features can be configured and may be turned off by default. Once turned on, these features may also have attributes or settings that can be configured. Please see the sections below for more details.

For information on the availability of Cisco Unified Communications Manager Device Packs, see http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html

Provide Dial Tone From Release Button

The Provide Dial Tone From Release Button feature allows users to disconnect a call, get dial tone, and access the New Call window by pressing only one button. When the user presses the Release button while on an active call or while dialing off-hook, the active call ends and the dial tone sounds. The New Call window appears on the selected line on the phone screen. The system administrator enables this feature.

Note The New Call window appears only if the call ends when the Release button is pressed.

This feature is supported on the following SIP phones:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Hide Video Option

The Hide Video Option feature is a user interface enhancement to configure how the video displays by default (either hidden or displayed). When the video is displayed, the user sees the Hide Video softkey; when the video is hidden, the user sees the Show Video softkey. The video continues streaming when the video window is hidden.

The phone supports a new configuration parameter that enables the administrator to control whether the video is displayed or hidden. The parameter is Hide Video By Default, with values Disabled (default) and Enabled.

This feature is supported on the following SIP phones:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Installation Notes

This section contains these sections:

Installing Cisco Unified Communications Manager

Before using the Cisco Unified IP Phone with Cisco Unified Communications Manager, you must install the latest firmware on all Cisco Unified Communications Manager servers in the cluster.

Note You can install Cisco Unified Communications Manager 7.1(3) or 7.1(3a). After you install one of these releases, you must install Cisco Unified Communications Manager 7.1(5) and later.

To download and install the Cisco Unified Communications Manager version, refer to the Install and Upgrade Guides for Cisco Unified Communications Manager.

Installing Firmware Release 9.2(4) for SIP

To download and install the phone firmware, follow these steps:

Procedure

Step 1 Go to the following URL:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240.

Step 2 Sign in to the **Tools & Resources > Download Software** page.

Step 3 Click **+** and choose the **IP Telephony** folder.

Step 4 Click **+** and choose the **IP Phones** folder.

Step 5 Choose **Cisco Unified IP Phones 9900 Series** or **Cisco Unified IP Phones 8900 Series**.

Step 6 Choose your phone type.

Step 7 In the **Latest Releases** folder, choose **9.2(4)**.

Step 8 Select one of the following firmware files, click the **Download Now** or **Add to cart** button, and follow the prompts:

- **cmterm-8961.9-2-4-19.cop.sgn**
- **cmterm-9951.9-2-4-19.cop.sgn**
- **cmterm-9971.9-2-4-19.cop.sgn**

Note If you added the firmware file to the cart, click the **Download Cart** link when you are ready to download the file.

Step 9 Click the **+** next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware:

- **cmterm-8961.9-2-4-19-readme.html**
- **cmterm-9951.9-2-4-19-readme.html**
- **cmterm-9971.9-2-4-19-readme.html**

Step 10 Follow the instructions in the readme file to install the firmware.

Installing Firmware Zip Files

If a Cisco Unified Communications Manager is not available to load the installer program, the following .zip files are available to load the firmware. Go to Step 1 and follow the first seven steps.

- cmterm-8961.9-2-4-19.zip
- cmterm-9951.9-2-4-19.zip
- cmterm-9971.9-2-4-19.zip

After you unzip the files, you must manually copy them to the directory on the TFTP server. See *Cisco Unified Communications Operating System Administration Guide* for information about how to manually copy the firmware files to the server.

Note Firmware upgrades over the WLAN interface may take longer than upgrades using a wired connection. Upgrade times over the WLAN interface may take more than an hour, depending on the quality and bandwidth of the wireless connection.

Cisco Unified Video Camera Firmware

The Cisco Unified Video Camera is supported on Cisco Unified Communications Manager Versions 7.1(5) and later.

Important Notes

This section contains these topics:

Using a Plantronics Audio 615M Headset with the Cisco Unified IP Phone 8961

The Plantronics Audio 615M headset is not compatible with the Cisco Unified IP Phone 8961. You must use an alternate headset type for this IP Phone. For more information, see CSCth71104.

Using the Plantronics CS50 USB Headset with the Cisco Unified IP Color Key Expansion Module

The Plantronics CS50 USB headset causes the phone to request power from the switch even though the headset is self powered. In this case, if a device such as a camera or expansion module is connected and active on the phone, the switch will reject the power request for the headset because the power budget has been exceeded. In this case, the headset cannot be used.

One-Way Video Calls for the Cisco Unified IP Phone

Because of limitations in the H.264 video signaling standards, Cisco Unified IP Phones 9951 and 9971 may not correctly display video that is received from devices supporting resolutions greater than 640 x 480. In this case, the user will see a black video screen.

To ensure that video from such devices is properly displayed on the IP phone, the best solution is to configure high definition phones and Cisco Unified IP Phones 8961, 9951, and 9971 into different call regions and limit the video bandwidth to 384 kb/s when calling between regions.

Cisco Unified IP Phones 9951 and 9971 Power Negotiation when Using a Video Camera

An issue (CSCtf09186) with some 802.3af switches results in the Cisco Unified IP Phones 9951 and 9971 being unable to negotiate for the additional power required to operate the IP Phone camera. To power the camera, use the Cisco Unified IP Phones 9951 and 9971 Power Negotiation (Enabled/Disabled) parameter to disable the IP phone power negotiation. To disable the Power Negotiation parameter, access the Product Specific Configuration of Cisco Unified Communications Manager 8.5 and later releases. A device pack must be installed to add the configuration parameter to the database for Cisco Unified Communications Manager releases earlier than 8.5. Disabling power negotiation enables the IP phone to power up the camera and to use up to 15.4 watts (the AF maximum) without the need to negotiate with the switch. You must use this workaround until the switch software is updated.

Tracking the Cisco Unified IP Phone 9971 Using Cisco Emergency Responder

You must configure the Cisco Unified IP Phone 9971 in Wi-Fi mode. When using this phone in this mode, you must configure Cisco Emergency Responder appropriately for tracking wireless IP Phones. For more information, see *Cisco Emergency Responder Administration Guide*.

Cisco Virtualization Experience Client (VXC) 2100

The Cisco Virtualization Experience Client (VXC) 2100 Series are zero clients designed to deliver a user desktop from a centralized host server, providing access to desktop applications as if they were available locally. The Cisco VXC 2100 series attaches to the Cisco Unified IP Phones 8961, 9951, and 9971 through a spine connector cable. For more information, see *http://www.cisco.com/en/US/products/ps11499/tsd_products_support_series_home.html*.

Caveats

This section contains these topics:

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of the following:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 To access the Bug Toolkit, go to:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Log on with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the “Search for bug ID” field, then click **Go**.

Open Caveats

Table 1 lists severity 1, 2, and 3 defects that are open for the Cisco Unified IP Phones that use Firmware Release 9.2(4).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL that is shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that Table 1 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in the "Using Bug Toolkit" section on page 7.

Table 1 Open Caveats for Firmware Release 9.2.(4)

Identifier	Headline
CSCty72792	Phone is unable to send response to INVITE
CSCty30841	No PiP local view if remote video cannot be displayed
CSCty53321	No content for Messages/Contacts if service provisioning is External URL
CSCty63778	Secure phone register to CUCM about 3 minutes after VPN disconnected
CSCtt18467	Phone syslogs prints NOT[ice] level always
CSCtx82992	Pressing the Back button has no effect when on Edit Dial UI
CSCty03846	TFTP Server inputbox is not activated while enable alt-tftp
CSCtx85612	Lock icon may be displayed on non-secure idle UI
CSCty25822	Unable to show video of video call made with SIPp
CSCti79116	Memory leak during SIP Codenomicon run
CSCtn89145	Joggling fullscreen selview during VGA video call to CSF softphone
CSCtq47498	After SSO, RT phones with KEMs reboot
CSCtr13418	Phone keep alive timer issue in 9.2.(2) phone load
CSCtr51513	ETSGJ-CH: Conference message is showing in ENGLISH instead of JAPANESE
CSCtr92986	Can't connect and delete 9XX Plantronics BT headset from phone
CSCtr93019	Can't answer call through BT headset after hold revert
CSCts01615	99xx become abnormal or crash after long period of network impairments
CSCts63656	WVGA video image jumps & grey lines appear on the left of the screen
CSCtt05778	No UI feedback when dialing external speed dial using softkey in onhook
CSCtu10890	The 9971 when using option 66 displays the same IP in both TFTP settings
CSCtu53630	9971 May Intermittently Drop from WLAN and Begin Scanning
CSCtu84951	Phone does not send the xmlbody when sip runs only on UDP
CSCtv04593	Conference list is still shown when it is disabled in FCP
CSCtw97451	Blackwire C220 "accessory not supported"
CSCtx48830	RT phone lost wireless connectivity during call
CSCtx90826	the loading of image fail of phone 9951/9971 in option66 case
CSCtx94428	Dev-unreg:Wrong ucm ip address carried in refer msg when phone fallback
CSCty01167	OpenSSL SSL_CTX_new Uninitialized Buffer Remote Information Disclosure
CSCty20965	Backpack device get connect when side USB port of RT phone is disabled
CSCty29040	Freezing 9971 display when running 9.2(2) - exception in Java AWT

Table 1 Open Caveats for Firmware Release 9.2.(4) (continued)

CSCty31023	Dialed digits lost while making conf or xfer call quickly in video call
CSCty31533	Application Window stuck when browsing it during phone upgrade
CSCty31537	SenderReportsSent of "show stream active video" is incorrect
CSCty34439	99XX phone reboot due to chinese locale
CSCty44400	LED is still lighted after change phone button template
CSCty60735	Phone retries using same bad password if it contains space

Resolved Caveats

Table 2 lists severity 1, 2, and 3 defects that are resolved for the Cisco Unified IP Phones using Firmware Release 9.2(4).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that Table 2 reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access Bug Toolkit as described in the "Using Bug Toolkit" section on page 7.

Table 2 Resolved Caveats for Firmware Release 9.2.(4)

Identifier	Headline
CSCtb49983	pause/transfer/conf causes issues with VVM background call
CSCtj03643	Wrong display time length of toast for maximum number calls alert
CSCtn45922	BT: Can't get the hold reversion call by Jawbone Icon
CSCtr23945	RT 89XX 99XX phones should cache 'span to pc port' configuration
CSCtr66381	Audio is cut off seconds after making intercom call out with BT headset
CSCts18141	No alert when Headset/Speaker button is disabled on 8961 unlike RT Lite
CSCts25261	Call log problem if receive call from shared line with call history open
CSCts37494	phone should ignore speakerphone event at unregister state
CSCts49800	Phone does not log the call in call history when no answer timer is out
CSCts63720	UI incorrect when Intercom interact with new call
CSCts65938	A white screen is seen when reset all settings from phone
CSCts94193	Cisco Unified IP Phone 8961: Bluetooth is Yes if "show capabilities"
CSCtt24181	"X" softkey is still enabled when no digits could be deleted
CSCtt43276	"Display On When Incoming Call" didn't work when using Display URI
CSCtt45602	transfer works incorrectly during call routing
CSCtt46093	Fail to open status page due to Null pointer exception
CSCtt95558	Call can't be parked after Max Ad Hoc has been reached
CSCtu17419	Group Pickup and Meet-me are not disabled when speaker is disabled
CSCtu28658	Phone does not notify CUCM for offhook status when Meet Me is pressed

Table 2 Resolved Caveats for Firmware Release 9.2.(4) (continued)

CSCtu35626	No collapsed session bubble if privacy is on for 2 parties in conference
CSCtu38237	Phone status problems when Do Not Disturb on shared lines
CSCtu39847	CME: codec G.722 does not work on 9971 SIP phone
CSCtu63447	Phone keeps retrying auto registratio when auto registration is disabled
CSCtv08902	Phone keeps turning KEM on/off continuously when it is not in service
CSCtv11520	Forward All softkey may be hidden for non-primary line when on SRST
CSCtw50300	Cisco IP phone cannot add fourth party to an existing conference call
CSCtw50975	No status message and alarm for power save plus failure
CSCtw51085	“Last=” in Reason header of REGISTER is empty in case of EnergyWise
CSCtw62854	secure icon changed to non secure on srst after resume
CSCtw62971	Rarely PiP is not shown in video calls
CSCtw81031	debugsh doesn't always recognize “callhist” and “callagent” categories
CSCtw85696	'Sign In' Softkey may be greyed after VPN login is cancelled
CSCtw87046	99xx phone to preserve vpn config icon and vpn property when reset
CSCtw91200	Call softkey does not work in some scenerio after phone failover to srst
CSCtw91388	Occasionally an abnormal alert is shown after vpn is cancelled
CSCtw91410	Occasionally no way to input password after cert+pass vpn is cancelled
CSCtx04611	The unsaved settings alert is prompted when the user opens Network Setup
CSCtx35563	Video transmit stops when placing a call from shared line
CSCtx77199	Continuous tone after entering DTMF digits
CSCtx89324	phone continues to ring after answered on shared line by other device
CSCtx91192	the recipinet's Mute key is not illuminated in whisper state
CSCtx99667	plar can not take effect immediately on 8961 after setting DN on line 2
CSCty00808	IP phone resets when we connect or disconnect a PC on the PC port
CSCty05600	Launching MIDLets takes at least 20 seconds
CSCty12447	One of four shared line phones stuck in resume status
CSCty18510	Registration by TCP failed if network delay is longer than 1 second
CSCty18695	Phone should forbidden direct transfer when failover to SRST
CSCty20885	Secure call on SRST held by conference attempt has lock icon displayed
CSCty21493	Phone stuck in held call while ending a connected conf call on SRST
CSCty24962	KPML failed with SRST after pressed Forward All and Cancel
CSCty29704	Multicast RTP streaming does not work on 9971 phones
CSCty30814	Call bubble is still displayed if cancel onhook dialing after a call
CSCty31478	No tone is played if press digits to make intercom call

Documentation Updates

This section provides documentation changes that do not appear in the existing Cisco IP Phone 8961, 9951 or 9971 (SIP) documentation:

VPN Capability for the Cisco Virtualization Client VXC211X

VPN Capability for the Cisco Virtualization Client VXC211X

Note Update (July 2012) – If you use the Cisco VXC VPN feature, Cisco recommends that you upgrade to Firmware Release 9.3(1). Firmware Release 9.3(1) is the official supported release for the Cisco VXC VPN. Many performance and user experience issues present in the 9.2(3) firmware are fixed in Release 9.3(1).

The Cisco Virtualization Experience Client (VXC) 21xx devices provide the capability of an integrated VPN solution for Cisco users. It will allow a remote user to have an office worker's experience with a direct connection to their organization's network while achieving lower operating costs. By providing a seamless integrated solution, Cisco simplifies the home solution deployment for the worker and enterprise.

This feature enables VPN tunneling for the Cisco VXC 2111 and Cisco VXC 2112 clients when they are attached to a Cisco Unified IP Phone 8961, 9951 or 9971. It will only provide support for wired Cisco VXC 2111 and 2112 devices to Cisco Unified IP Phone 8961, 9951 or 9971.

Also there is no support for management of the VXC via the VXC Manager (VXC-M) when the device is connecting through the VXC VPN.

Table 3 compares the characteristics of single and dual tunnels.

Note The VPN function uses a dual tunnel approach - one tunnel for the phone's VPN and a second for the VXC.

Table 3 Single Tunnel and Dual Tunnel Characteristics

	Single Tunnel	Dual Tunnel
VPN Licenses	1	2
IP Addresses	1	2
Number of Logins	1 (all scenarios)	2 (not all scenarios)
Security	Normal	Normal
Performance	Possible negative performance regarding the Phone's UI and Video. Voice is preserved.	Phone's UI, Video, and Voice are preserved.

Note Note: Single Tunnel will be an optional feature released in the near future.

Dual Tunnel – Number of Logins:

1. In most cases, the normal use case will be two logins, one for the Phone's VPN and one for VXC_VPN.
2. In one circumstance a single-sign on is featured, but it is dependent on the power up procedure with the VXC 21xx. The user will have to enable the Phone's VPN and then proceed to power on the VXC 21xx. Once VXC 21xx is powered on, the user can enter the username/password and then login. Both phone's VPN and VXC_VPN will be connected.
3. For one-time passwords, you will enter your login credentials twice – once for the Phone's VPN and again for the VXC VPN. Users will not see a successful connection message displayed after signing into the Phone's VPN login. Instead, a successful login will display after logging into the VXC VPN.

The Cisco Unified IP Phone 8961, 9951, or 9971 and the Cisco VXC 2111 and Cisco VXC 2112 clients use identical VPN access credentials and control parameters. To enable the Cisco VXC feature, you must set up the VPN feature in Cisco Unified Communications Manager Administration, using the submenus under the **Advanced Features > VPN** menu path.

In addition, you must set the Enable VXC VPN for MAC Feature option to be the string FFFFFFFFFFFF. A value of FFFFFFFFFFFF allows all VXC users to complete the VPN tunnel.

If you set the Enable VXC VPN for MAC Feature option with a specific MAC address, this feature is enabled but it allows only a VXC user with the same MAC address to complete the VPN tunnel.

Use the Phone Configuration window (**Device > Phone**) to access this setting.

After the VXC VPN feature is enabled and the user signs in to the Phone's VPN, the phone initiates one VPN tunnel for phone traffic and a second data tunnel, VXC_VPN, to carry Cisco VXC traffic. In this case, both tunnels use the same configuration parameters.

Note No configuration is required on the Cisco VXC client to support the VPN. All VPN configuration is performed on your Cisco IP phone and the Unified CM.

Additional Configuration Requirements

The following sections describe additional phone configurations that are required to support the Cisco VXC VPN feature.

Cisco Unified Communications Manager Configuration

It is recommended that you set the PC Port to Enabled on Cisco Unified CM. If the PC port is disabled, the Cisco VXC client cannot access the network. The phone provides no enforcement of this configuration.

You can set the preceding parameters in Unified Communications Manager Administration using the Phone Configuration window (**Device > Phone**).

VPN Head-End Configuration

The recommended VPN concentrator (head-end) for use with this feature is the Cisco ASA 5500 Series Adaptive Security Appliance. To support the Cisco VXC VPN, you must set up the ASA for multisession support so that the phone can establish two tunnels using the same credentials.

Access Control List

The Access Control List (ACL) restricts network traffic to the display ports only. Table 4 shows the common ports and their corresponding protocols.

Table 4 Ports and Protocols

Protocol		Port	Comment
PCoIP	UDP and TCP	4172	New Port; IANA approved
	UDP and TCP	50002	Old Port, being phased out but should still be open
	TCP	32111	Used for communication between USB devices and the view agent on the VM
ICA	TCP	1494	Standard ICA traffic
	TCP	2598	Session reliability (if disabled, defaults to TCP 1494)
	TCP	1604	ICA Browser
	UDP	1604	ICA
RDP	TCP	3389	Standard RDP traffic
	TCP	9427	Multimedia Redirection (MMR)
Citrix Provisioning Services	UDP and TCP	54321	
	UDP and TCP	54322	
	UDP range	6910-6960	
View Services	TCP	4001	
Additional Ports needed	UDP	53	DNS
	UDP	137	NetBios
	TCP	80	HTTP
	TCP	443	HTTPS
Diagnostic purpose	ICMP		

The following limitations and restrictions apply when using the Cisco VXC VPN feature:

- Only Layer 3 packets are tunneled. The Cisco VXC VPN feature does not support Layer 2 tunneling and any Layer 2 capabilities are lost when the Cisco VXC connects through VPN.
- The VPN client supports only IPv4 addresses.
- The VXC VPN tunnel cannot be established over a Wi-Fi interface.
- You can configure the Enable VXC VPN Feature option after you set up the phone VPN parameters, including VPN Group and VPN Profile. This restriction exists because the VXC VPN shares the same VPN parameters as the phone VPN.

All existing limitations and restrictions related to the phone VPN support apply to the VXC VPN as well.

Troubleshooting FAQ

Table 5 shows four common troubleshooting scenarios. Use this information when you work with the Cisco VXC VPN feature and the Cisco VXC 2111 or Cisco VXC 2112 clients with Cisco Unified IP Phone 8961, 9951, or 9971.

Table 5 Troubleshooting FAQs

Scenario	Action
Why does the Cisco VXC client not appear in a phone Accessories menu?	1. Make sure that your Cisco IP Phone is powered by a Cisco power adapter. 2. Unplug the spine connector cable and reattach it to the phone, or power cycle the phone.
Why can't the Cisco VXC client get an IP address from a phone?	1. Make sure Cisco VXC VPN tunnel is shown as 'Connected' in the VPN menu. 2. Check the Cisco Unified CM and confirm that Enable VXC VPN for MAC is FFFFFFFFFFFF.
Why can't the Cisco VXC VPN tunnel be established?	1. Make sure your VPN login credentials are correct. 2. Make sure that VPN concentrator is configured to support more than one session for one user.
Why does the Span to PC not work?	When the Cisco VXC VPN feature is enabled, the Span to PC is turned off silently.

Additional Information

For more information about installing and using the Cisco VXC 2111 and Cisco VXC 2112 clients with Cisco Unified IP Phones 8961, 9951, or 9971, see http://www.cisco.com/en/US/products/ps11499/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.