Release Notes for Cisco Unified Personal Communicator Release 8.6

October 3, 2012

These release notes describe the new features and caveats for Cisco Unified Personal Communicator Release 8.6(2).

To view the release notes for previous versions of Cisco Unified Personal Communicator, go to http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html.

For details about downloading the software, see Installation Notes, page 20.

Contents

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

Introduction

These release notes describe requirements, restrictions, and caveats for Cisco Unified Personal Communicator Release 8.6. These release notes are updated for every maintenance release but not for patches or hotfixes.

Cisco Unified Personal Communicator uses Cisco Unified Client Services Framework, which provides Cisco telephony services and media services for Cisco Unified Personal Communicator.

Before you install Cisco Unified Personal Communicator, review the list of open caveats. See Open Caveats, page 54.

System Requirements

Network Requirements

This section describes the network requirements for Cisco Unified Personal Communicator.

Voice over IP

You must configure voice over IP (VoIP) on your Cisco routers and gateways. See the applicable configuration guides for the models of routers and gateways in use.

Network Ports Used by Cisco Unified Personal Communicator

Cisco Unified Personal Communicator requires inbound and outbound traffic to occur on particular ports through particular protocols.

The operating system sets ports for all inbound traffic except the Real-Time Transport Protocol (RTP). Cisco Unified Personal Communicator sets the following ports to send and receive RTP traffic:

- 16384 is the base port for initial streams
- Ports ranging up to 32766 for additional RTP and RTCP streams.

Cisco Unified Personal Communicator uses the same ports in a given range to send and receive specific streams.

Table 1 describes the inbound ports used by Cisco Unified Client Services Framework.

Table 1 Ports Used for Inbound Traffic by Cisco Unified Client Services Framework

Port	Protocol	Description
16384-32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio and video. You configured these ports in Cisco Unified Communications Manager. For more information about device configuration files, see the *Cisco Unified Communications Manager System Guide*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Table 2 describe the outbound ports used by Cisco Unified Client Services Framework.

Table 2 Ports Used for Outbound Traffic by Cisco Unified Client Services Framework

Port	Protocol	Description
69	UDP	Connects to the Trivial File Transfer Protocol (TFTP) server to download files.
80	TCP HTTP	Connects to meetings and voicemail services such as Cisco Unified Meeting Place or Cisco WebEx for meetings and Cisco Unity or Cisco Unity Connection for voicemail features.
143	IMAP (TCP/TLS)	Connects to voicemail services to retrieve and manage voice messages from Cisco Unity or Cisco Unity Connection.
389	TCP	Connects to the LDAP server for contact searches.
443	TCP HTTPS	Connects to meetings and voicemail services such as Cisco Unified Meeting Place or Cisco WebEx for meetings and Cisco Unity or Cisco Unity Connection for voicemail features.
636	LDAPS	Connects to the secure LDAP server for contact searches.
993	IMAP (SSL)	Connects to voicemail services to retrieve and manage voice messages from Cisco Unity or Cisco Unity Connection.
2748	TCP	Connects to the CTI gateway, the CTI Manager component of Cisco Unified Communications Manager. This provides control of desktop phones.
4224	TCP (CAST)	Connects to the IP Phone through CAST for enabling video while in desktop phone mode.
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signaling.
5061	TCP	Provides secure SIP call signaling.
5222	TCP (XMPP)	Connects to the Cisco Unified Presence server for availability status and instant messaging features.
5445-5446	UDP	Provides desktop phone video regardless of the Cisco Unified Communications Manager SIP profile used. Port 5446 is used for RTP Control Protocol (RTCP) and provides out-of-band statistics and control information for an RTP flow.

Table 2 Ports Used for Outbound Traffic by Cisco Unified Client Services Framework

Port	Protocol	Description
7993	IMAP (TLS)	Connects to voicemail services to retrieve and manage voice messages from Cisco Unity or Cisco Unity Connection.
8191	TCP	Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.
8443	TCP	This port is used to perform the following tasks: • Connects to the Cisco Unified Communications Manager IP Phone (CCMCIP) server to get a list of currently-assigned devices. • Connects to the Cisco Unified Presence server via SOAP.
16384-32766	UDP	Sends RTP media streams for audio and video.

Table 3 describes the ports used by Cisco Unified Personal Communicator.

Table 3 Ports Used By Cisco Unified Personal Communicator

Port	Protocol	Description	Registry Key Value Name
44442	HTTP	The Cisco Unified Personal Communicator process, cupc.exe, listens for events from Cisco Unified Client Services Framework on this port.	CUCIMOCCSFPort

Note The registry key value names in Table 3 refer to another product, but are also correct for Cisco Unified Personal Communicator.

Configurations that Use Network Ports

You can use the network port information for these configurations:

- To unblock traffic destined for Cisco Unified Personal Communicator through a firewall. For details, see Configuring Network Ports on Client Computers, page 4.
- To avoid blocking availability status information, verify that firewalls on the client computer or on the network are configured to allow Cisco Unified Personal Communicator traffic.

Configuring Network Ports on Client Computers

The Microsoft Windows firewall prompts users to block Cisco Unified Personal Communicator when they run it for the first time. Ensure users select **Unblock**.

Troubleshooting Tips

If users encounter issues with Cisco Unified Personal Communicator functionality after configuring the Microsoft Windows firewall to allow traffic, do the following:

1. Restart Cisco Unified Personal Communicator.
2. Determine if users still encounter the issues.

3. Remove Cisco Unified Personal Communicator for the firewall settings.
4. Add Cisco Unified Personal Communicator to the list of applications that allow incoming connections.

Routing Access Control Lists

You must configure switching and routing ACLs so that Cisco Unified Personal Communicator can communicate with servers and endpoints that might be connected to the voice VLAN. The voice VLAN is the VLAN that carries voice traffic.

By using ACLs, you can permit Cisco Unified Personal Communicator to connect to each server through the appropriate protocol through which the application communicates with that server.

You can use ACLs to permit Cisco Unified Personal Communicator to connect to each server through the appropriate protocol for that server. For example, you can allow UDP traffic in the port range that Cisco Unified Personal Communicator uses for RTP, and then label it with the appropriate QoS actions.

When Cisco Unified Personal Communicator is in software phone mode, this configuration enables Cisco Unified Personal Communicator to send RTP media to, and receive RTP messages from, other audio and video endpoints across the IP network.

For details about ACLs, how to configure the voice VLAN, and how to configure QoS actions, see the switching and routing documentation for your network products.

Network Address Translation

The Cisco Unified Personal Communicator is not compatible with Network Address Translation (NAT). Cisco Unified Personal Communicator cannot use Simple Traversal of UDP through Network Address Translation (STUN), Traversal using NAT (TURN), or any other NAT-traversal scheme.

To traverse NAT, Cisco Unified Personal Communicator must be behind a virtual private network (VPN) connection.

Server Requirements

Note You can configure Cisco Unified Personal Communicator in a large number of contexts and you can include or exclude particular features. The application is tested in the most common configuration contexts, but due to production constraints, not all configurations are tested.

Table 4 Cisco Unified Personal Communicator Server Requirements

Item	Release
Cisco Unified Communications Manager	• 8.6(x) releases • 8.5(1) • 8.0(1) or later 8.0(*x*) releases • 7.1(5) or later 7.1(x) releases • 7.0(1) or later 7.0(*x*) releases **Note** Cisco Unified Personal Communicator only supports one Cisco Unified Client Services Framework device per user in Cisco Unified Communications Manager.
Cisco Unified Presence	• 8.6(*x*) releases • 8.5(1) or later 8.5(*x*) releases • 8.0(2) or later 8.0(*x*) releases
Cisco Unity	• 8.0 with Microsoft Exchange 2007 on another server, or in a failover configuration • 8.0 with Microsoft Exchange 2003 on the same server, on another server, or in a failover configuration • 7.0(2) with Engineering Special (ES) 19 or later, with Microsoft Exchange 2007 on another server, or in a failover configuration • 7.0(2) with Engineering Special (ES) 19 or later, with Microsoft Exchange 2003 on the same server, on another server, or in a failover configuration
Cisco Unity Connection	• 8.6(x) • 8.5(1) • 8.0(1) or later 8.0(*x*) releases • 7.1(4) or later 7.1(*x*) releases Cisco Unified Personal Communicator supports all of these releases in systems where publisher and subscriber Cisco Unity Connection servers are integrated in an active-active configuration, regardless whether or not failover is configured.

Table 4 Cisco Unified Personal Communicator Server Requirements (continued)

Item	Release
Cisco Unified Meeting Place	For conference calls with video: • 8.5(*x*) • 8.0(*x*) • 7.*x* • Cisco Unified Meeting Place Express VT 2.0[1] For meetings: • 8.5(*x*) • 8.0*(x)* • 7.*x*
Cisco WebEx Node for MCS	• T27LB or later
Cisco WebEx Meeting Center	• T27LB or later
Cisco Unified Videoconferencing Multiple Control Unit (MCU)	• 7.0 • 5.6 or later
Cisco Unified Survivable Remote Site Telephony	• 8.0 with Cisco Unified Communications Manager Release 8.0 • 7.1 with IOS 12.4(24)T with Cisco Unified Communications Manager Release 7.1(2) • 7.0 with IOS 12.4(20)T with Cisco Unified Communications Manager Release 7.0(1) • 4.2 with IOS 12.4(11)XW5 with Cisco Unified Communications Manager Release 6.1(3)
Cisco ASA Adaptive Security Appliances	• (Recommended for SIP interdomain federation) Cisco ASA 5500 Series Adaptive Security Appliance Software Release 8.3(0) For information on interdomain federation requirements, see the release notes for Cisco Unified Presence Release 8.0: http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html
LDAP	• Microsoft Active Directory 2008 • Microsoft Active Directory 2003 • OpenLDAP 2.4

1. Cisco Unified Meeting Place Express VT 2.0 does not support web meetings.

- Required Servers, page 8
- Recommended Servers, page 8

Required Servers

The following servers are required for Cisco Unified Personal Communicator operation:

- Cisco Unified Communications Manager is installed in your network and configured to handle call processing and point to point video. It provides Cisco Unified IP Phone control through the Cisco Unified Communications Manager computer telephony interface (CTI). It is not required to enable IP telephony for Cisco Unified Personal Communicator users, but those users will not have telephony capabilities. For Cisco Unified Communications Manager details, see the following URL:

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

- Cisco Unified Presence is installed and is operational. This server provides the Cisco Unified Personal Communicator client configuration and presence information. For Cisco Unified Presence details, see the following URL:

  http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

- LDAP/Active Directory server

Recommended Servers

To use the full functionality of Cisco Unified Personal Communicator, you must have the following products installed and operational:

- Voicemail servers, to retrieve and play voicemail messages. You can use one of the following products:
  - Cisco Unity Connection. For more information about this product, see the following URL:

    http://www.cisco.com/en/US/products/ps6509/tsd_products_support_series_home.html

  - Cisco Unity. For more information about this product, see the following URL:

    http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html

- Conferencing servers for audio and video conferencing. You can use one of the following products:
  - Cisco Unified Meeting Place. For information about this product, see the following URL:

    http://www.cisco.com/en/US/products/sw/ps5664/ps5669/index.html

  - Cisco Unified Meeting Place Express VT. For more information about Cisco Unified Meeting Place Express VT, see the following URL:

    http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5664/ps6533/ps7260/product_data_sheet0900aecd8061fae7.html

  - Cisco Unified Videoconferencing. This application provides audio and video functionality for merged conference calls of three or more parties, placed through Cisco Unified Personal Communicator. For details about the MCUs:

    http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html

- Conferencing servers for web collaboration including video. You can use one or both of the following products, depending on your deployment:
  - Cisco Unified Meeting Place. For information about this product, see the following URL:

    http://www.cisco.com/en/US/products/sw/ps5664/ps5669/index.html

  - Cisco WebEx. For more information about this product, see the following URL:

http://www.webex.com/smb/web-meeting-center.html

For details about how to integrate your conferencing server and Cisco Unified Personal Communicator, see the *Deployment Guide for Cisco Unified Presence* at the following URL:

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Client Computer Requirements

Before you install Cisco Unified Personal Communicator on any computer, the computer must meet the requirements described in these sections:

- Hardware Requirements, page 9
- Software Requirements, page 12
- Virtual Desktop Infrastructure (VDI) Support, page 15
- General Platform Requirement Notes, page 15
- Codecs for Use with Cisco Unified Personal Communicator, page 16

For more information about client PC requirements and audio quality impact see About Audio and Video Quality, page 18.

Hardware Requirements

Table 5 Hardware Requirements for Desktop and Laptop Computers for Audio and Video in Various Modes

Item	Audio Only/IM Only	QCIF	CIF	VGA	720HD
Memory	1 GB	1 GB	1 GB	1 GB	2 GB
Available disk space	1 GB	1 GB	1 GB	1 GB	1 GB
Minimum Windows Experience Index (WEI) processor score[1]	2.0	4.0	4.0	4.8	5.9 and a system with at least four CPU cores.

Table 5 Hardware Requirements for Desktop and Laptop Computers for Audio and Video in Various Modes (continued)

Item	Audio Only/IM Only	QCIF	CIF	VGA	720HD
Video card					
A DirectX 9-compatible graphics card with this video RAM:					
Microsoft Windows XP	Not applicable	128 MB	128 MB	128 MB	256 MB
Microsoft Windows Vista	Not applicable	256 MB	256 MB	256 MB	256 MB
Microsoft Windows 7	Not applicable	256 MB	256 MB	256 MB	256 MB
I/O ports	When you use USB audio and video, USB 2.0 is required.				HD-capable USB 2.0 web camera, HDMI capture card, and HD camera.

1. Microsoft Windows XP does not provide a WEI processor score.

Tested Video Devices

The video cameras tested with Cisco Unified Personal Communicator are as follows:

- Cisco VT Camera II
- Cisco VT Camera III
- HP Elite Autofocus
- Labtec Webcam 1200
- Logitech QuickCam Deluxe for Notebooks
- Logitech QuickCam Fusion
- Logitech QuickCam Pro 5000
- Logitech QuickCam Pro 9001
- Logitech QuickCam Pro for Notebooks
- Logitech QuickCam Ultra Vision
- Microsoft LifeCam Cinema
- Microsoft LifeCam NX-6000
- Microsoft LifeCam VX-6000
- Sony HDR-CX12
- Sony PCSACHG90
- Tandberg Precision HD

The following computers with built-in video cameras were tested with Cisco Unified Personal Communicator:

Laptop	Camera
Acer TravelMate 5730	Acer Crystal Eye
Dell Inspiron 1720 PP22X	Integrated Webcam
HP Compaq 6730b Notebook PC	HP Webcam (VGA)
HP Compaq 6735b Notebook PC	HP Webcam (VGA)
HP Pavilion DV6-2106EA	Integrated Camera
Lenovo ThinkPad W500	Integrated Camera
Lenovo ThinkPad W510	Integrated Camera
Samsung P460	USB 2.0, USB video class (UVC), 1.3 MP
Toshiba Satellite Pro P300	Chicony USB 2.0

Tested Audio Devices

The following Plantronics audio devices have been tested and work with Cisco Unified Personal Communicator:

- The Blackwire USB wired Headset family
- The Savi Office Dect Wireless Headset System family
- The Vpro UC Bluetooth headset system with Bluetooth Dongle family
- The CS 50/60 USB Wireless Headset System family
- The DA 45 USB adapter family for use with Plantronics H-Top headsets
- The Calisto USB Handset/Speakerphone family

Note The preceding list of Plantronics products does not include -M models of these devices. The -M models are not tested for compatibility with Cisco Unified Personal Communicator.

The following additional audio devices have been tested and work with Cisco Unified Personal Communicator:

- Jabra GN2100
- Jabra GN200 USB DUO Tube
- Jabra GN9120 Flex Boom NC
- Jabra GN9350e
- Jabra GO6470
- Jabra BIZ2400
- Jabra PRO9470
- Jabra GN2000
- Jabra BIZ620
- Polycom Speaker
- Clarisys-I750

Note All headsets were tested for audio sending and receiving only. Function buttons on particular headsets might not function correctly with Cisco Unified Personal Communicator. For additional call control functionality, you may need to install Plantronics or Jabra software on your PC. While Cisco does perform basic testing of third-party headsets and handsets for use with Cisco Unified Personal Communicator, it is ultimately the responsibility of the customer to test this equipment in their own environment to determine suitable performance.

Software Requirements

Table 6 Software Requirements for Cisco Unified Personal Communicator

Item	Description
Operating system	• Microsoft Windows 7 SP1 Professional, Enterprise or Ultimate, 32-bit or 64-bit • Microsoft Windows Vista SP2 Business or Ultimate, with DirectX 10, 32-bit or 64-bit • Microsoft Windows XP SP3 with DirectX 9.0c, 32-bit only **Note** Ensure that the latest display drivers are installed on your computer so that your display functions correctly with DirectX.
Software framework	• Microsoft .NET 3.5 SP1

Tested Software Integrations

The following table lists the applications that have been successfully tested for compatibility with Cisco Unified Personal Communicator and the features that are available for each application.

Table 7 Tested Software Applications and Feature Availability

Application	Call Options (Yes/No)	Availability Status (Yes/No)	Instant Messaging (Yes/No)
Microsoft Outlook 2010 SP1 (32 and 64 bit versions)	Yes • File > Info > Related People Pane > Contact Card • Outlook Ribbon > More> Call > Call Contact • Message Ribbon > Call > Call Contact	Yes • Next to contact name	Yes • Contact card • Outlook Ribbon > IM • Message Ribbon > IM > Reply with IM or Reply All with IM
Microsoft Outlook 2007 SP1 and SP2	Yes • Context menu > Call Contact > Call Contact • Message Ribbon > Click To Call group > Call Contact or Call With Edit	Yes • Next to contact name	Yes • Context menu • Message Ribbon > IM > Reply with Instant Message or Reply All with Instant Message
Microsoft Outlook 2003	Yes • Context menu > Additional Actions > Call Number or Call with Edit Number.	No	No
Microsoft Word 2010 (32 bit version only)	Yes • Context menu > Additional Actions > Instant Messaging Contacts Contact > Contact card • Word Ribbon > Click To Call Group > Call Number or Call with Edit Number • File > Info > Related People Pane > Contact Card	Yes • Context menu > Additional Actions > Instant Messaging Contacts > Contact Card and the availability is indicated to the left of the photo. • File > Info > Related People Pane > Contact Card.	Yes • Context menu > Additional Actions > Instant Messaging Contacts > Contact Card • File > Info > Related People Pane > Contact Card
Microsoft Word 2007	Yes • Context menu > Call Number or Call with Edit Number • Word Ribbon > Click To Call Group > Call	No	No
Microsoft Word 2003	Yes • Context menu > Call Number or Call with Edit Number.	No	No

Table 7 Tested Software Applications and Feature Availability

Application	Call Options (Yes/No)	Availability Status (Yes/No)	Instant Messaging (Yes/No)
Microsoft Excel 2010 (32 bit version only)	Yes • Context menu > Call Number or Call with Edit Number • Excel Ribbon > Click to Call group > Call Number or Call with Edit Number • File > Info > Related People Pane > Contact Card	Yes • File > Info > Related People Pane > Contact Card and the availability is indicated to the left of the photo.	Yes • File > Info > Related People Pane > Contact Card
Microsoft Excel 2007	Yes • Context menu > Call Number or Call with Edit Number • Excel Ribbon > Click to Call group > Call Number or Call with Edit Number	No	No
Microsoft Excel 2003	Yes • Context menu > Call Number or Call with Edit Number.	No	No
Microsoft PowerPoint 2010 (32 bit version only)	Yes • PowerPoint Ribbon > Click to Call group > Call Number or Call with Edit Number • File > Info > Related People Pane > Contact Card	Yes • File > Info > Related People Pane > Contact Card and the availability is indicated to the left of the photo.	Yes • File > Info > Related People Pane > Contact Card
Microsoft PowerPoint 2007	Yes • PowerPoint Ribbon > Click to Call group > Call Number or Call with Edit Number	No	No
Microsoft PowerPoint 2003	Yes • Context menu > Call Number or Call with Edit Number.	No	No
Microsoft SharePoint 2010	Yes • Context menu > Call Number or Call with Edit Number • Contact card	Yes • Next to contact name	Yes • Contact card
Microsoft SharePoint 2007	Yes • Context menu > Call Number or Call with Edit Number • Persona menu > Call Contact or Call with Edit Contact	Yes • Next to contact name	No

Table 7 Tested Software Applications and Feature Availability

Application	Call Options (Yes/No)	Availability Status (Yes/No)	Instant Messaging (Yes/No)
Microsoft SharePoint 2003	Yes • Context menu > Call Number or Call with Edit Number.	No	No
Microsoft Internet Explorer 7.0, 8.0, or 9.0 (32 bit)	Yes • Context menu > Call or Call with Edit	No	No
Mozilla Firefox 3.2 to 11.0 (32 bit)	Yes • Context menu > Call or Call with Edit	No	No

Tested VPN Clients

The virtual private network (VPN) clients tested with Cisco Unified Personal Communicator are as follows:

- Cisco VPN Client 5.0
- Cisco Anyconnect VPN Client 2.2, 2.3 and 2.4

Virtual Desktop Infrastructure (VDI) Support

Cisco Unified Personal Communicator Release 8.5(5) and later is supported on the following hosted virtual desktop applications:

- VMware View 4.5
- Citrix XenDesktop 4.0

Note In a virtualized desktop environment, full audio and video capabilities are only available on Cisco Unified Personal Communicator when you are using the desk phone for phone calls. If you are using the phone on your computer, only the voicemail features are supported in a virtualized environment.

General Platform Requirement Notes

- For information about requirements for video, see Notes on Video, page 48.
- The headsets were tested for audio sending and receiving only. Function buttons on particular headsets might not function correctly with Cisco Unified Personal Communicator.

  While Cisco does perform basic testing of third-party headsets and handsets for use with Cisco Unified Personal Communicator, it is ultimately the responsibility of the customer to test this equipment in their own environment to determine suitable performance.

  Due to the many inherent environmental and hardware inconsistencies in the locations where Cisco Unified Personal Communicator is deployed, there is not a single *best* solution that is optimal for all environments.

- Power management software on some laptop computers might reduce the speed of your processor temporarily to conserve power. When this occurs, Cisco Unified Personal Communicator cannot run calls that require higher processor speed, for example, video calls.

Additional Documentation

To access hardening guides from vendors of operating systems, see the following URL:

http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/default.mspx

To access security configuration guides, see the National Security Agency (NSA) website at the following URL:

http://www.nsa.gov/snac/

Software Interoperability

Before you deploy Cisco Unified Personal Communicator Release 8.6 to the computers of your users, ensure that there are no other applications installed on the computers of your users that use Cisco Unified Client Services Framework. The following applications use Cisco Unified Client Services Framework:

- Cisco Unified Communications Integration for Microsoft Office Communicator
- Cisco Unified Communications Integration for Microsoft Lync
- Cisco Unified Communications Integration for Cisco WebEx Connect
- Cisco WebEx Connect 7
- Cisco Unified Communications Integration for RTX

In addition, Cisco Unified Personal Communicator cannot co-exist with Microsoft Office Communicator/Microsoft Lync.

Codecs for Use with Cisco Unified Personal Communicator

A codec is an implementation of an algorithm capable of performing encoding and decoding on a digital data stream. Codecs are used to encode and decode data, such as sound and video streams, that would otherwise use large amounts of network bandwidth when transmitted or disk space when stored.

Video Codecs

You can use the following video codecs with Cisco Unified Personal Communicator:

- H.264/AVC

Audio Codecs

You can use the following audio codecs with Cisco Unified Personal Communicator:

- G.711a, µ-law
- G.722 (wide band)
- G.729a, G.729ab
- Internet Low Bit Rate Codec (iLBC)
- Internet Speech Audio Codec (iSAC). iSAC is only available on Cisco Unified Communications Manager Release 8.0 or later.

Compatibility Notes

- Adaptive Security Appliance Software can provide security features for business-to-business federation of presence and instant messaging between users of Cisco Unified Personal Communicator and other communications applications.
- For more information about interdomain federation of presence and IM, see the release notes for Cisco Unified Presence Release 8.6:

  http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html
- Releases of Cisco Unified Communications Manager and Cisco Unified Presence can co-reside on the same server.

For details about performing upgrades, see the *Deployment Guide for Cisco Unified Presence*:

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Cisco Unified IP Phone Requirements

Table 8 lists the Cisco Unified IP Phone models that are supported for Cisco Unified Personal Communicator, and whether Skinny Call Control Protocol (SCCP) and Session Initiation Protocol (SIP) are supported:

Table 8 Phones Supported by Cisco Unified Personal Communicator

Phone	SCCP	SIP	Supports Video with CAST
Cisco IP Communicator	Yes	Yes	Not applicable
9971	Not applicable	Yes	Yes[1] [8]
9951	Not applicable	Yes	Yes[2] [8]
8961	Not applicable	Yes	Yes[3] [8]
8945	Yes	Yes	No[4]
8941	Yes	Yes	No[4]
7975G	Yes	Yes	Yes[5]
7971G[6]	Yes	Yes	Yes[5]
7970G[6]	Yes	Yes	Yes[5]
7965G	Yes	Yes	Yes[5]
7962G	Yes	Yes	Yes[5]
7961G-GE[6]	Yes	Yes	Yes[5]
7961G[6]	Yes	Yes	Yes[5]
7945G	Yes	Yes	Yes[5]
7942G	Yes	Yes	Yes[5]
7941G-GE[6]	Yes	Yes	Yes[5]
7941G[6]	Yes	Yes	Yes[5]
7931G[7]	Yes	Not applicable	Yes
7925G	Yes	Not applicable	No

Table 8 Phones Supported by Cisco Unified Personal Communicator (continued)

Phone	SCCP	SIP	Supports Video with CAST
7921G	Yes	Not applicable	No
7920G[6]	Yes	Not applicable	No
7911G	Yes	Yes	Yes[5]
7906G	Yes	Yes	No
6961	Yes	Not applicable	Yes[5 8]
6945	Yes	Yes	Yes
6941	Yes	Not applicable	Yes[5 8]
6921	Yes	Not applicable	Yes[5 8]
6911	Yes	Not applicable	Yes[5 8]
6901[9]	Yes	Not applicable	No

1. Requires SIP firmware upgrade Sip9971.9-1-0PD0-97.
2. Requires SIP firmware upgrade Sip9951.9-1-0PD0-97.
3. Requires SIP firmware upgrade Sip8961.9-1-0PD0-97.
4. This phone does not have a detachable camera. CAST cannot be enabled. Video can only be displayed on the phone, not the desktop
5. An SCCP firmware load is required to support video.
6. This phone is at the end of software maintenance.
7. For 7931G phones to function correctly with Cisco Unified Personal Communicator, you must set the value of the Outbound Call Rollover to field to **No Rollover** in Cisco Unified Communications Manager.
8. You must unplug the video from this model of phone to get CAST to work.
9. This phone does not support speakerphones or headsets.

To enable video on phones, the following conditions must exist:

- The PC Port and Video Capabilities fields must be enabled for the phone in Cisco Unified Communications Manager.
- The phone must be connected to the computer on which Cisco Unified Personal Communicator is running by Ethernet cable.

For more information, see Users Might See Lower Video Quality When Computer Is Connected to Some Models of Cisco Unified IP Phone, page 52.

Note See Open Caveats, page 54 for information on a caveat pretaining to the 9971 model phone.

About Audio and Video Quality

Cisco Unified Personal Communicator is designed to provide premium voice and video quality under a variety of conditions; however, in some instances users may notice interruptions of transmission or temporary distortions (“Artifacts”) which are considered a normal part of the applications operation.

These artifacts should be infrequent and temporary when using:

- Cisco Unified Personal Communicator on a workstation meeting the recommended configuration requirements.

- A network that meets the recommended quality criteria in the Cisco Unified Communication Solution Reference Design Document.

We take reasonable measures to interface with the operating system in ways that decrease the likelihood that other applications running on the system will interfere with software phone audio and video quality. However, the shared nature of system environments in which these products run is very different than a closed environment like Cisco IP Phones and we cannot guarantee equivalent performance.

The following are some conditions that may cause artifacts:

- Spike in usage of the personal computer's CPU - where CPU utilization is between 75 to 100% - due to launching applications, system processes or processing happening within other applications running.
- The system is running low on available physical memory
- Other applications using large amounts of bandwidth to or from the workstation to the network
- Other network bandwidth impairments
- Dynamic reduction in CPU clock speed due to power management policy (for example, laptops running on battery power) or thermal protection causing the CPU to run in a more highly loaded condition
- Any other condition that causes the application to lose timely access to the network or audio system, for example, interference from third-party software

Avoiding or recovering from the conditions previously listed will help minimize audio and video distortion artifacts.

Related Documentation

For a list of complete documentation for Cisco Unified Personal Communicator, see the documentation guide:

http://www.cisco.com/en/US/products/ps6844/products_documentation_roadmaps_list.html

New and Changed Information

Release 8.6(3)

- This release provides fixes to functionality. Refer to Resolved Caveats, page 56 for information on these fixes.

Release 8.6(2)

- Registry key added to disable video and CDP driver in desktop phone mode.
- Registry key added to change the location of Local Data files.

- Registry key added to turn on video for all audio calls and make that a default setting during the first installation of Cisco Unified Personal Communicator.
- Fixes to functionality and performance. See Important Notes, page 30 and Resolved Caveats, page 56 for information on these fixes.

Release 8.6(1)

- Fixes to functionality and performance. See Important Notes, page 30 and Resolved Caveats, page 56 for information on these fixes.

Installation Notes

After you place the order, you receive information on where to find documentation for Cisco Unified Personal Communicator, along with the Product Authorization Key (PAK). The PAK provides the software activation key and the license file.

For details about obtaining the license file, see the *Deployment Guide for Cisco Unified Presence* at the following URL:

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

You download Cisco Unified Personal Communicator software from the Software Center (http://www.cisco.com/public/sw-center/sw-voice.shtml). You must have an account on Cisco.com to access this site.

Time Required to Install

If the computer on which you are installing Cisco Unified Personal Communicator does not already have Microsoft .NET installed, the Cisco Unified Personal Communicator installer installs Microsoft .NET. This will result in a longer installation time.

Installing Cisco Systems Network Protocol

When you install Cisco Unified Personal Communicator on Microsoft Windows Vista or Microsoft Windows 7, you might be prompted to install Cisco Systems Network Protocol device software. Install this software.

If you do not install this software, you cannot place video calls if you set your Cisco Unified Personal Communicator to use your desk phone for phone calls.

Installing Cisco Unified Personal Communicator Using MSI

The video components of Cisco Unified Client Services Framework require Microsoft Visual C++ 2005 version 8.0.59193 or later. Microsoft Visual C++ 2005 must be installed before you install Cisco Unified Personal Communicator, if you are using MSI to install.

Microsoft provides a Microsoft Visual C++ 2005 redistributable package, vcredist_x86.exe. You can download this package from the following links:

- http://go.microsoft.com/fwlink/?LinkId=169360
- http://www.microsoft.com/downloads/details.aspx?familyid=766a6af7-ec73-40ff-b072-9112bab119c2&displaylang=en

To see the command line options, execute the following command:

vcredist_x86.exe /?

The Microsoft Visual C++ 2008 redistributable package is not compatible with Cisco Unified Client Services Framework: the Microsoft Visual C++ 2005 package is required.

Installing the Microsoft Visual C++ 2005 Redistributable Package

You can use an MSI file to install the Microsoft Visual C++ 2005 redistributable package. Extract the files vcredist.msi and vcredis1.cab from vcredist_x86.exe to a temporary folder. Use the following command line option:

vcredist_x86.exe /C /T:<*full-path-to-folder*>

Example

vcredist_x86.exe /C /T:C:\VCRedist

Use the extracted files to install Microsoft Visual C++ 2005.

Using Translation Patterns Instead of Application Dialing Rules

Cisco Unified Personal Communicator is easiest to install with Cisco Unified Communications Manager Release 7.0 or later, although you can install it with Cisco Unified Communications Manager Release 6.1(3) or later.

Cisco Unified Communications Manager Release 7.0 and later support +E.164 phone numbers. Cisco recommends that you use +E.164 phone numbers with Cisco Unified Personal Communicator, so that outgoing calls are easier to set up.

If you are using Cisco Unified Communications Manager Release 7.0 or later, Cisco recommends that you use translation patterns to set up outbound calls, rather than application dialing rules. If you use translation patterns, the rules are dynamically applied, and you do not need to restart services.

For detailed information on translation patterns, see the Cisco Unified Communications Manager Administration online help, or the *Cisco Unified Communications Manager Administration Guide*:

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

Removing Cisco Unified Video Advantage

If Cisco Unified Video Advantage is installed on a client computer, you must uninstall it before you can install Cisco Unified Personal Communicator. If you do not uninstall Cisco Unified Video Advantage, you are prompted to do so during the Cisco Unified Personal Communicator installation.

Tip If you are performing a mass deployment of Cisco Unified Personal Communicator, you can use a software deployment tool to silently uninstall Cisco Unified Video Advantage from client computers prior to the installation.

Cisco Unified Personal Communicator Deployment

The Cisco Unified Personal Communicator installation application installs the following components:

- User interface for Cisco Unified Personal Communicator.
- The client-related components of the Cisco Unified Client Services Framework.
- Click to Call add-on (optional).
- Microsoft Office Integration (optional).

The Cisco Unified Personal Communicator application is provided in two separate installation formats as follows:

- Cisco Unified Personal Communicator executable file.
- Cisco Unified Personal Communicator Microsoft Windows Installer (MSI) file.

This section describes the installation formats and the deployment options.

- Executable File, page 22
- Microsoft Windows Installer (MSI) File, page 23
- Deployment Options, page 23

Executable File

Users can run the executable file on their own computers. The executable file includes the prerequisite software for the application, as follows:

- Microsoft .NET Framework 3.5 Service Pack 1 (installer stub)
- Microsoft Visual C++ 2005 Redistributable Package (x86)
- Additional software required for Click to Call functionality:
  - Microsoft Office 2003 Primary Interop Assemblies (for machines with Office 2003)
  - Microsoft Office 2007 Primary Interop Assemblies (for machines with Office 2007)
  - Microsoft Visual 2005 Tools for Office Second Edition Runtime (x86)

Cisco Unified Personal Communicator checks if the prerequisite software is installed on the computer and if not, it automatically installs the prerequisites. To save time during the installation process, we recommend that you install the prerequisite software in advance of installing Cisco Unified Personal Communicator. All of the prerequisite software is available from the Microsoft website.

Note If the minimum required version of .NET Framework is not installed on the computer, Cisco Unified Personal Communicator runs the installer stub provided for that application. The installer stub downloads the .NET Framework software from the Microsoft website. This action requires Internet access and takes a considerable amount of time. We recommend that you install the required release of Microsoft .NET Framework in advance of the Cisco Unified Personal Communicator installation to save time and avoid any Internet access issues.

Microsoft Windows Installer (MSI) File

You can use a software management system to push the Microsoft Windows Installer (MSI) file to the computers of your users. The MSI file does not contain any of the prerequisite software that is required for Cisco Unified Personal Communicator.

Note If you choose to install the MSI file, you must install the prerequisite software prior to installing Cisco Unified Personal Communicator.

The prerequisite software that you must install prior to installing the Cisco Unified Personal Communicator MSI file is:

- Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft Visual C++ 2005 Redistributable Package (x86)
- Additional software required for Click to Call functionality:
  - Microsoft Office 2003 Primary Interop Assemblies (for computers with Office 2003)
  - Microsoft Office 2007 Primary Interop Assemblies (for computers with Office 2007)
  - Microsoft Visual 2005 Tools for Office Second Edition Runtime (x86)

The prerequisite software is available from the Microsoft website.

Deployment Options

You can deploy the Cisco Unified Personal Communicator installation application in one of the following ways:

- Automated Mass Deployment, page 24
- Standalone Installation, page 24
- Deploying the MSI with Group Policy, page 24
- Deploying the MSI or Executable File from a Command, page 25
- Using the msiexec Command, page 25
- Using the CiscoUnifiedPersonalCommunicatorK9.exe Command, page 26
- Features Available with Cisco Unified Personal Communicator, page 27

Automated Mass Deployment

The mass deployment options for installing Cisco Unified Personal Communicator are as follows:

- Use Active Directory Group Policy. You can use group policy to deploy administrator configuration settings.
- Use a software management system, for example, Altiris Deployment Solution, Microsoft System Center Configuration Manager (SCCM), and so on.
- Use a self-extracting executable with a batch script. You can use the batch script to deploy administrator configuration settings.

Standalone Installation

The administrator can install Cisco Unified Personal Communicator on each individual client computer or users can install the application on their own computers. The administrator can use the options listed in Automated Mass Deployment, page 24 to deploy the administrator configuration settings.

Note We strongly recommend that you use the executable file for standalone installations.

Deploying the MSI with Group Policy

Before You Begin

Ensure that all the computers or users on which you want to install Cisco Unified Personal Communicator are in the same domain.

Procedure

Step 1 On the domain server, execute the following command to start the Group Policy Management Console:

gpmc.msc

Step 2 Expand the forest that contains the domain to which you want to deploy, then expand the domain.

Step 3 Right-click **Group Policy Objects**, then select **New**.

Step 4 Create a new group policy object.

Step 5 Select the new group policy object in the GPMC console tree.

Step 6 (Optional) To verify that you can deploy to one user with the new group policy object, deploy a desktop wallpaper image to one user or computer as follows:

a. Specify a user or computer to which you want to deploy the desktop wallpaper image in the Scope tab.

b. Right-click the group policy object in the GPMC console tree, then select **Edit**.

c. Select **User Configuration > Policies > Administrative Templates > Desktop > Desktop** in Group Policy Management Editor.

d. Double-click the **Desktop Wallpaper** setting.

e. Set the setting to **Enabled**, and specify other details for the desktop wallpaper.

f. To refresh the group policy for the user or computer, execute the following command on the computer that is affected by the group policy change:

gpupdate /force

g. Verify that the desktop wallpaper image is updated on the computer affected by the group policy change.

Step 7 Specify the users or computers to which you want to deploy in the Scope tab of the new group policy object.

Step 8 Right-click the group policy object in the GPMC console tree, then select **Edit**.

Step 9 Select **User Configuration** or **Computer Configuration**, then **Policies > Software Settings** in Group Policy Management Editor.

Step 10 Right-click **Software installation**, then select **New > Package**.

Step 11 Beside **File Name**, paste the name of the shared drive where the **MSI** packages are stored. This would be a network location such as *servername**sharename*\. Ensure a trailing backslash is used after the share name.

Step 12 Select the package from the share and select **Open**.

Note Ensure the file share is accessible to all computers and users or the deployment will fail.

Step 13 Select the MSI file that you want to install.

Step 14 Select **Assigned** in the Deploy Software dialog box, then select **OK**.

The MSI file appears in the details pane.

The MSI file is pushed to each computer the next time that the computer updates policy settings.

The next time that the computer is restarted, the changes that you deployed in the Computer Configuration section of the group policy object are applied before the log-in screen is displayed on the computer.

Any changes that you deployed in the User Configuration section are applied after the user logs in to the domain. An information window displays descriptions of the changes as they are being made.

Deploying the MSI or Executable File from a Command

You can use commands to install Cisco Unified Personal Communicator. You can use either the **msiexec** command, or the **CiscoUnifiedPersonalCommunicatorK9.exe** command. You can also specify features to install with Cisco Unified Personal Communicator.

- Using the msiexec Command, page 25
- Using the CiscoUnifiedPersonalCommunicatorK9.exe Command, page 26
- Features Available with Cisco Unified Personal Communicator, page 27

Using the msiexec Command

The syntax required for the **msiexec** command is as follows:

msiexec /i *MSI-filename* **/q** [*ADDLOCAL="feature1*[,...[*feature9*]]"]

The *ADDLOCAL* parameter specifies the features that you want to install. To successfully install Cisco Unified Personal Communicator, you must always include the CSF and JRE features.

Note

- If you do not specify the ADDLOCAL argument, all features are selected.
- Do not enter spaces in the list of features.
- The feature names are case sensitive.
- The syntax above specifies a silent installation.
- Users will be prompted to close the applications indicated when the following options are used:
  - Firefox - Firefox
  - InternetExplorer - Internet Explorer
  - Outlook - Outlook
  - OfficeIntegrationC2X - Outlook
  - Excel - Excel
  - PowerPoint - PowerPoint
  - Word - Word
  - SmartTags - Outlook, Excel, Powerpoint, Word

For example, to install Cisco Unified Personal Communicator with the click-to-call feature for Microsoft Excel and Microsoft Word, use the following command:

msiexec /i CiscoUnifiedPersonalCommunicatorK9.msi /q ADDLOCAL="CUPC,ClicktoCall,Word,Excel,CSF,PrivateJRE"

If you are deploying Cisco Unified Personal Communicator with Microsoft Office 2007 or 2010, you must include the Microsoft Office Integration feature, *OfficeIntegrationC2X*. Use the following command to install Cisco Unified Personal Communicator with the Microsoft Office Integration feature:

msiexec /i CiscoUnifiedPersonalCommunicatorK9.msi /q ADDLOCAL="CUPC,OfficeIntegrationC2X,CSF,PrivateJRE"

Related Topics

Features Available with Cisco Unified Personal Communicator, page 27

Using the CiscoUnifiedPersonalCommunicatorK9.exe Command

The syntax required for the **CiscoUnifiedPersonalCommunicatorK9.exe** command is as follows:

CiscoUnifiedPersonalCommunicatorK9.exe /s [**/v**"/q *ADDLOCAL*=\"*feature1*[,...[*feature9*]]\""]

For example, to install Cisco Unified Personal Communicator with the click-to-call feature for Microsoft Excel and Microsoft Word, use the following command:

CiscoUnifiedPersonalCommunicatorK9.exe /s /v"/q ADDLOCAL=\"CUPC,ClicktoCall,Word,Excel,CSF,PrivateJRE\""

Note

- If you do not specify the ADDLOCAL argument, all features are selected.
- Do not enter spaces in the list of features.
- The feature names are case sensitive.
- The syntax above specifies a silent installation.

- Users will be prompted to close the applications indicated when the following options are used:
  - Firefox - Firefox
  - InternetExplorer - Internet Explorer
  - Outlook - Outlook
  - OfficeIntegrationC2X - Outlook
  - Excel - Excel
  - PowerPoint - PowerPoint
  - Word - Word
  - SmartTags - Outlook, Excel, Powerpoint, Word

The syntax required to perform a silent uninstall from the **CiscoUnifiedPersonalCommunicatorK9.exe** command is as follows:

CiscoUnifiedPersonalCommunicatorK9.exe /S /x /v/qn

Related Topics

Features Available with Cisco Unified Personal Communicator, page 27

Features Available with Cisco Unified Personal Communicator

Table 9 lists the features that you can select when you install Cisco Unified Personal Communicator from a command.

Table 9 Features Available to Install with Cisco Unified Personal Communicator

Feature Name	Description
CUPC	Cisco Unified Personal Communicator.
CSF	Essential feature. This must be installed for Cisco Unified Personal Communicator to operate correctly.
PrivateJRE	Essential feature. This must be installed for Cisco Unified Personal Communicator to operate correctly.
ClicktoCall	The Application Programming Interface (API) that the click-to-call features use is also installed if you select this feature.
OfficeIntegrationC2X	Integration for Microsoft Office applications with Click to Call, IM, and Presence features. This should only be chosen if Microsoft Office 2007 or 2010 is installed.
Excel	Click-to-call features for Microsoft Excel. [1]
InternetExplorer	Click-to-call features for Microsoft Internet Explorer. [1]
Outlook	Click-to-call features for Microsoft Outlook. [1]
PowerPoint	Click-to-call features for Microsoft PowerPoint. [1]
Word	Click-to-call features for Microsoft Word. [1]
Firefox	Click-to-call features for Mozilla Firefox. [1]
SmartTags	Smart Tag call menu options in Microsoft Office. [1]

1. If you select this feature, the ClicktoCall feature is also selected automatically.

Users will be prompted to close the applications indicated when the following options are used:

- Firefox - Firefox
- InternetExplorer - Internet Explorer
- Outlook - Outlook
- OfficeIntegrationC2X - Outlook
- Excel - Excel
- PowerPoint - PowerPoint
- Word - Word
- SmartTags - Outlook, Excel, Powerpoint, Word

Related Topics

- Using the msiexec Command, page 25
- Using the CiscoUnifiedPersonalCommunicatorK9.exe Command, page 26

Installing Security Certificates on Client Computers for Client Services Framework (CSF)

The following procedure describes the steps that the administrator needs to take to add security certificates to the keystore on the computer on which Cisco Unified Personal Communicator is running. By default, Cisco Unified Personal Communicator expects self-signed certificates, except when the administrator configures a CCMCIP security profile with a specified certificate type.

Procedure

Step 1 Put the certificate file into the folder where you store your security certificates. The default location for storing security certificates is as follows:

- **Microsoft Windows XP** - <*drive*>:\Documents and Settings\<*username*>\Local Settings\Application Data\Cisco\Unified Communications\Client Services Framework\certificates
- **Microsoft Windows Vista and Microsoft Windows 7** - <*drive*>:\Users\<*username*>\AppData\Local\Cisco\Unified Communications\Client Services Framework\certificates

Step 2 (Optional) To specify a custom location for storing security certificates, do the following:

a. Select **Cisco Unified Presence Administration > Application > Cisco Unified Personal Communicator > Settings**.

b. Use the **CSF certificate directory** field to specify the absolute path to the folder where the certificates are stored.

Step 3 (Optional) To specify the Server Certificate Verification parameter for a CCMCIP security profile, do the following:

a. Select **Cisco Unified Presence Administration > Application > Cisco Unified Personal Communicator > CCMCIP Profile (CUPC 8.0 and higher)**.

b. Select the profile you want to change.

c. In the **Server Certificate Verification** field, select one of the following options:

- **Any Certificate**
- **Self Signed or Keystore**
- **Keystore Only**

Enabling Availability Status for Microsoft Office Users

To enable the availability status feature of Cisco Unified Personal Communicator to work with the supported Microsoft Office applications, the administrator must configure an attribute in Microsoft Active Directory.

Procedure

Step 1 Start the ADSIEdit administrative tool.

Step 2 Expand the domain that contains your users.

Step 3 Open the organizational unit (OU) that contains your users.

Add a new value to the proxyAddresses attribute in the format 'SIP:*email-address*', for example, 'SIP:johndoe@cisco.com'.

Limitations and Restrictions

Review Table 10 before you work with Cisco Unified Personal Communicator. Table 10 lists known limitations that will not be fixed, and there is not always a workaround. The table is sorted by severity, then by identifier in alphanumeric order.

Some features might not work as documented, and some features could be affected by recent changes to the product. Make sure to read the Important Notes, page 30.

Note Some of the headlines in Table 10 refer to Cisco Unified Integration for Microsoft Office Communicator, but are also relevant to Cisco Unified Personal Communicator.

Table 10 Closed Caveats for Cisco Unified Personal Communicator

Identifier	Severity	Component	Headline
CSCtf91411	2	phone-audio	Bad Echo with Tandberg Precision HD camera microphone
CSCtq29236	2	commoncomponents	C2X functionality does not work with Office 2010 64bit Vista 64bit
CSCti16856	3	video-svc	Crash when remote end answers a video call - seen intermittently
CSCtf34489	3	video-svc	Poor VQ over simulated Internet w constrained BW and heavy impairments
CSCtg05223	3	video-svc	Client does not fully adapt to available network bandwidth
CSCtg64841	3	video-svc	Some IDR frames lost by ECT router if packets sent in quick succession

Table 10 Closed Caveats for Cisco Unified Personal Communicator (continued)

Identifier	Severity	Component	Headline
CSCth66656	3	contact-svc	CSF client 8.0.1 LDAP query is causing high CPU in Domain Controller
CSCti35691	3	phone-softphone	OnConversationEnded not sent for 3.5 minutes after I ended the call
CSCti95902	3	video-svc	Severely lowered bit rate on overallocated link (2Mbits vs 1.3actual)
CSCtj04316	3	ms-integration	CUPC will not load when AVG V.9.0.851antivirus is used.
CSCtk36281	3	audio-svc	Disconnect headset when playing VM, loose audio & audio error on next call
CSCtr43595	3	media-escalations	Media Escalation fails if no default browser is defined
CSCtr78562	3	phone-softphone	Client intermittently freezes the laptop when the user disconnects the call
CSCty91451	3	phone-softphone	Apparent DOS attack from CUPC clients
CSCtk13400	4	cdp	CAST Service Won't Initialize Intermittently
CSCts34531	4	api-general	Headset not picked up by CUPC for first time it's connected to a usb port
CSCtk31734	6	audio-svc	CSF should also be able to support comfort noise payload type 19

Important Notes

Warning **IMPORTANT NOTICE - PLEASE READ: During an emergency, software phone technology may not provide the most timely or accurate location data if used for a 911 emergency call. Calls may be misdirected to the wrong emergency response center or the emergency response center may make errors when determining your location. USE A SOFTWARE PHONE ONLY AT YOUR OWN RISK DURING AN EMERGENCY. Cisco will not be liable for resulting errors or delays.**

Silent Uninstallation Command

Instructions for performing a silent uninstallation from the command line have been added to the documentation. This information has been added to the section Using the CiscoUnifiedPersonalCommunicatorK9.exe Command, page 26. This addition has been made as a resolution for the CDET **CSCub06302**.

Cisco Unified Communications Manager Express Video Escalation Support

For Cisco Unified Personal Communicator initiated calls in desktop phone mode the call gets escalated from audio to video. In the case of Cisco Unified Communications Manager integration with Cisco Unified Communications Manager Express, such calls will remain audio only as Cisco Unified Communications Manager Express does not support video escalation. This Cisco Unified Communications Manager Express limitation is documented in CSCub07600.

Microsoft Office 365 Support

Cisco Unified Personal Communicator supports Microsoft Office 365 with the following software:

- Microsoft Office 2007 32 bit
- Microsoft Office 2010 32 bit
- Microsoft Office 2010 64 bit
- Microsoft Sharepoint 2010

Disable Video in Desktop Phone Mode

The desktop phone mode video capabilities of Cisco Unified Personal Communicator can be disabled using the **DeskphoneVideoDisabled** registry key. This registry key also disables the CDP driver. Both actions are enabled by setting this registry key to **true**. This registry key is set to **false** by default.

This key is located in *HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData* or *HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData*.

Change Location of Local Data Files

The location of local data files is now configurable. This includes information such as the user profile, device configuration, and log files. Perform the following procedure to configure a custom location for this information:

Step 1 Create a new environment variable with a regular folder path as a value.

For example: *MyLocalData = C:\My Local Data*.

Step 2 Create a new registry key in *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Cisco Systems, Inc.* or *HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.* called **LocalAppDataEnvVariable** whose value is the environment variable created in previous step.

Note This key should be a located in the **Wow6432Node** subkey in 64 bit systems. The key would be located in *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Cisco Systems, Inc.* or *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, Inc.* in 64 bit systems.

Meeting Escalation with Cisco Unified MeetingPlace 8.5(x)

Meeting integration between Cisco Webex and Cisco Unified MeetingPlace 8.5(x) has a new set of requirements to follow. These new requirements allow you to create a meeting with the desired audio provider with Cisco Unified MeetingPlace 8.5(x) while preserving backward compatibility:

- Cisco Unified MeetingPlace Audio Conferencing must be configured in the Audio Conference section of the Cisco Webex One-Click Setup to be able to escalate a meeting with Cisco Unified MeetingPlace8.5(x) audio support.
- Ensure the key **WebConfSSOIdentityProvider** is no longer present in the following registry locations:
  - *HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData*
  - *HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData*

This value should not be present in these locations if Cisco Unified MeetingPlace 8.5(x) is used.

This configuration ensures Cisco Unified MeetingPlace is used as the audio provider.

Default Video for all Audio Calls

Cisco Unified Personal Communicator can now be configured to enable video by default for all audio calls and make it a default setting during the first installation of the application. Set the registry key *HKEY_CURRENT_USER\SOFTWARE\Policies\Cisco Systems, Inc.\Unified Communications\CUPC8\VideoCallByDefault* or *HKEY_CURRENT_USER\SOFTWARE\Cisco Systems, Inc.\Unified Communications\CUPC8\VideoCallByDefault* to **true** to enable this functionality.

If any of the registry keys are in the **Policies** hive, the key must be in that same hive or it will be ignored.

The value of this registry key will be **false** if the registry key value field is empty or if some exception occurs. Otherwise, it will be parsed and set to **true** or **false** acccording to what the user has set.

DOS Attack on Unity Connection Voicemail Server

Cisco Unified Personal Communicator does not use the Voicemail Web Service when it is connected to Cisco Unity Connection. Cisco Unified Personal Communicator will ping this service every two minutes if it becomes unavailable even though it is not actually used for Cisco Unity Connection connections. This fact, in combination with incorrect Cisco Unified Presence configurations, can have the same effect as a denial of service (DOS) attack on the Cisco Unity Connection server. The Voicemail Web Service should be disabled if Cisco Unity Connection is used.

Disable the Voicemail Web Service using the following procedure:

Step 1 Open Cisco Unified Presence Administration pages.

Step 2 Select **Application > Cisco Unified Personal Communicator > Voicemail Profile**.

Step 3 Choose the appropriate Cisco Unity Connection server profile.

Step 4 Select **<none>** for **Primary Voicemail Server**.

Step 5 Select **<none>** for **Backup Voicemail Server**.

Step 6 Save the configuration changes.

Note Repeat these steps for all profiles configured for the same server.

The next time Cisco Unified Personal Communicator starts, the server health information for the Voicemail Server is missing but information for the Voice Message Store should remain and show a connection.

Cisco Unified Personal Communicator will no longer send requests to the Voicemail Web Service. This change will take effect for users that are part of the changed profiles.

Installer Fix

An installer condition associated with the Microsoft Visual C++ 2005 Redistributable in previous versions of Cisco Unified Personal Communicator prevented the user from installing the client in certain situations. This condition would fail incorrectly when a user had a new version of the package installed. This condition is now fixed to ensure that if either the 8.0.59193 or 8.0.61001 versions of the package are installed, the condition will pass. The condition will fail once again however if any versions newer than this are subsequently installed.

A public installer property can be used to override this condition is necessary. Name the installer property to VCREDISTOVERRIDE and set its value to TRUE. The following is an example of how to override this condition when installing from the command line:

msiexec /i [Product].msi VCREDISTOVERRIDE=TRUE

Desktop Phone Mode Error

Cisco Unified Personal Communicator compares the local JTAPI file against the version hosted on Cisco Unified Communications Manager the first time it enters desktop phone mode each session. It downloads the server version to perform this comparison. If the server version cannot be downloaded within 30 seconds, an error is produced. Users can safely ignore this error and continue entering desktop phone mode.

DSCP Packet Marking

Differentiated Services Code Point (DSCP) is an IP field responsible for classification of IP packets. It allows for Quality of Service on IP networks where packet priority is dependent on the DSCP value. Packets with higher DSCP values are given a higher priority as they traverse the network.

Microsoft Windows Vista and 7 applications do not have the ability to set DSCP values. These operating systems reset all DSCP values to zero that have been set by the application if the user is not an administrator and the UAC user account control setting is turned on. This was the behavior on Cisco Unified Personal Communicator releases prior to 8.5(5). DSCP packet marking is operating system driven for Microsoft Windows Vista and 7 in the non-Administrative user / UAC case.

Cisco Unified Personal Communicator 8.5(5) includes changes to ensure that audio and video streams are always set up within separate, specific port ranges. This is necessary because the Microsoft Windows Vista and 7 operating systems need to mark DSCP values for audio and video packets differently and thus need a way to discover how to separately identify audio and video streams. Since the Cisco Unified Personal Communicator 8.5(5) changes guarantee that audio will always be set up within one port range

and video in another, an OS Group Policy can be configured to distinguish one from the other and mark the media packets appropriately. Perform the following procedure to create audio and video group policies:

Procedure

Step 1 Go to the Cisco Unified Communications Manager administration page.

Step 2 Select **Device > Device Settings > SIP Profile** from the menu and select the applicable SIP profile.

Step 3 Note the values in the **Start Media Port** and **Stop Media Port** fields.

The port range between these two numbers is the port range all media streams use. From that port range you need two port ranges; an audio port range and a video port range. Calculate these ranges by allocating the bottom half of the range to audio and the top half to video.

Step 4 Use the instructions found at the following link to create the new DSCP group policies: http://technet.microsoft.com/en-us/library/cc771283.aspx.

Step 5 Using the instructions from Step 4, create a new audio policy with the following attributes:

- **Policy name:** CUPC_Audio (Wizard Page 1)
- **Specify DSCP value:** 46 (Wizard Page 1)
- **Only applications with this executable name:** cucsf.exe (Wizard Page 2)
- **Select the protocol this QoS policy applies to:** UDP (Wizard Page 4)
- **From this source port number or range as:** The audio port range calculated in Step 3 (Wizard Page 4)

Step 6 Using the instructions from Step 4, create a new video policy with the following attributes:

- **Policy name:** CUPC_Video (Wizard Page 1)
- **Specify DSCP value:** 34 (Wizard Page 1)
- **Only applications with this executable name:** cucsf.exe (Wizard Page 2)
- **Select the protocol this QoS policy applies to:** UDP (Wizard Page 4)
- **From this source port number or range as:** The video port range calculated in Step 3 (Wizard Page 4)

Step 7 Using the instructions from Step 4, create a new video policy with the following attributes:

- **Policy name:** CUPC__Deskphone_Video (Wizard Page 1)
- **Specify DSCP value:** 34 (Wizard Page 1)
- **Only applications with this executable name:** cucsf.exe (Wizard Page 2)
- **Select the protocol this QoS policy applies to:** UDP (Wizard Page 4)
- **From this source port number or range as:** 5445:5446

Automatic Tethered Phone Selection

Cisco Unified Personal Communicator has capabilities for the automatic selection of a tethered phone. Cisco Unified Personal Communicator users will often have multiple desktop phone devices assigned to them but only one that is tethered to their workstation through an Ethernet cable. This new feature ensures that the tethered phone is always selected when a Cisco Unified Personal Communicator user enters desktop phone mode.

This feature is disabled by default. Set the **AutomaticTetheredPhoneSelection** registry key to true through a group policy setting to enable it. This key is located in *HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData*. For additional information on setting group policies and registry settings in Cisco Unified Personal Communicator, see the following chapters in the *Deployment Guide for Cisco Unified Presence Release 8.6*:

- Configuring Active Directory for Cisco Unified Personal Communicator
- Configuring Additional Registry Keys for Cisco Unified Personal Communicator

The following usage scenarios outline the operation of this feature when it is enabled through the registry:

- If the user manually changes their desktop phone device from the tethered device to a new one while the device is available, the new device will be chosen and automatic selection will be switched off.
- If the user manually changes their desktop phone device from tethered while the device is not available, the new phone device will be selected but when the tethered phone becomes available again Cisco Unified Personal Communicator will automatically switch back to it.
- If the user manually changes the desktop phone device to tethered, automatic selection will be switched on.
- If the user changes phone modes, automatic selection will be switched on.

Note This feature will also work if the user is logged in to their tethered phone with extension mobility.

Preferred Audio and Video Device Selection

Cisco Unified Personal Communicator has capabilities for the selection of preferred audio and video devices.

When Cisco Unified Personal Communicator is first installed, the devices selected as defaults by the operating system become the currently selected devices. If the user has a preferred audio or video device they wish to use when it is available, they will select it on the **Audio** or **Video** tab of the **Options** window and click **Apply** after selection is complete. Once applied, the chosen devices will override any other plugged in devices.

If the preferred device is removed from the workstation, Cisco Unified Personal Communicator will revert to using the operating system default devices. If the preferred device is removed from the workstation and a new device of the same type (audio or video) is introduced, this new device will become the currently selected device. If an additional device is introduced to the workstation while the preferred device is still present, it must be explicitly selected to become the new preferred device.

Automatic Server Discovery

Cisco Unified Personal Communicator contains a feature for the automatic discovery of Cisco Unified Presence servers. Previous versions of Cisco Unified Personal Communicator required either the administrator to push the server address to a client through a registry key or the client to manually enter the server address on the logon screen. Cisco Unified Personal Communicator can now use DNS SRV lookup to automatically find the Cisco Unified Presence server in the client's Active Directory domain.

DNS SRV is a record an administrator adds to a DNS server. This record can be added to any DNS domain but its addition to the Active Directory domain is recommended. A DNS SRV record is unlike a typical DNS record. Instead of storing a simple Host name and IP address pairing, DNS SRV records details about a particular service on a network. A DNS administrator can map many hosts to the same service name and assign a priority and weighting to each. This provides support for load balancing and failover services.

Cisco Unified Personal Communicator uses the following logon process when making use of the DNS SRV feature:

1. Application start up.
2. Local cache file is checked for server address.
3. If the cache file does not have the address, the local registry is checked for the server address.
4. If the local registry does not have the address, a DNS request is made against the connection specific suffix. If that fails the default Active Directory domain is queried. If the registry is populated, a DNS SRV request is made against the value in the registry. If the registry is populated and the DNS SRV request against the registry value fails, the registry value is put into the Login Address field in Cisco Unified Personal Communicator.

Cisco Unified Personal Communicator continues to support server identification through a registry key pushed to the client or manual entry.

See the section **Automatic Server Discovery** in Chapter 13 of the *Deployment Guide for Cisco Unified Presence Release 8.6* for additional information on configuring this feature. This section is available at the following location:

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_6/english/install_upgrade/deployment/guide/deploy.html#wp1102338

Dial via Office

Cisco Unified Personal Communicator contains Dial via Office (DVO) functionality. DVO is a feature that allows a user to configure an additional phone number for the purposes of call forwarding. Users who have configured a DVO number are called through their standard office phone number and the call is then forwarded to the additional number specified. Calls placed by the user display the caller ID of their standard office phone number.

Note Dial via Office functionality requires access to both the enterprise network and the applicable Cisco Unified Communications Manager. If the user is not directly connected to both, a VPN connection may be required to use this functionality.

DVO is configured on the **Call Options** window. Click **Calls** and then select the **Dial via Office** checkbox. Enter the DVO number in the space provided.

DVO functionality is triggered when the call is answered. This can be through the user answering the call or the call being routed to voicemail.

Note A call routed using DVO cannot be ended if the call is on hold. The call must first be resumed before it can be ended.

Enhanced Directory Integration

Enhanced Directory Integration (EDI) was introduced in Cisco Unified Personal Communicator 8.5(2). EDI provides additional capabilities to the basic directory integration already present in Cisco Unified Personal Communicator. EDI simplifies the integration of Cisco Unified Personal Communicator and corporate directory services. This improved integration provides benefits to organizations of any size with different directory architectures and sizes. Advantages of Enhanced Directory Integration include:

- auto discover of directory services
- use of Microsoft Windows integrated authentication for directory access
- encrypted credentials
- support for backup / alternative directory server
- support for ADAM/AD LDS Directory services
- support for administrator configured alternative credentials

Table 11 lists the differences between basic and enhanced integration.

Table 11 Basic and Enhanced Directory Integration

Function	Basic Directory Integration	Enhanced Directory Integration
Default directory integration	Yes	No
Zero configuration option	No	Yes
Automatic discovery of directory services	No (Administrator configured)	Yes
Connection to Active Directory Domain Controller	Yes (Administrator configured)	Yes
Connection to Active Directory Global Catalog	Yes (Administrator configured)	Yes (Default)
Connection to ADAM/AD LDS directory	Partial (Proxy authentication not supported)	Yes
Administrator defined service and port configuration	Yes (Required)	Yes (Optional)
Backup/alternative directory server support	No	Yes
Administrator defined search base	Yes (up to 5)	Yes (up to 5)
SSL support	Yes	Yes
Use Microsoft Windows certificate store for SSL	No (Java store)	Yes
Encrypted credentials support	No (Unless using SSL)	Yes
Integrated authentication using Microsoft Windows credentials	No	Yes
Administrator defined alternative credentials	No	Yes
User defined alternative credentials	Yes	Yes
Custom attribute maps	Yes (Map must be defined)	Yes
Phone attribute search scope control	No	Yes
LDAP query customization	No	Yes
Phone number format mask	Yes	Yes

Table 11 Basic and Enhanced Directory Integration

Function	Basic Directory Integration	Enhanced Directory Integration
Retrieval of contact photo URL	Yes	Yes
Retrieval of binary photo object	No	Yes

This section contains the following topics:

Configuration

EDI is enabled using either an Active Directory group policy or Microsoft Windows registry settings. Cisco provides group policy template files that include directory configuration settings. These templates are available in ADM and ADMX formats for Microsoft Windows Server 2003 and 2008 environments.

Once enabled, most administrators should not need to provide additional directory integration configuration. Cisco directory integration uses automatic discovery to find the directory service Microsoft Windows uses to discover a domain controller or global catalog server. This discovery is performed with a DNS Service request. This request will search for the domain controller or global catalog server in the native domain of the user's workstation. The native domain can be identified by examining the USERDNSDOMAIN environment variable.

Directory server information can be configured manually if the directory server is not discoverable through a DNS query. Configuration is performed using a group policy or through manipulation of the registry. The administrator should configure the IP address or Host Name of the primary and backup directory server as well as the port requests are received on.

Connections to a global catalog server are recommended. This server contains the primary directory attributes for all users in a Microsoft Windows domain forest. Administrators can connect to a domain controller instead if the required search attributes are not present on the global catalog server. If possible, administrators should enable missing search attributes on the global catalog server so it can be used. Administrators should confirm with directory managers that photo attributes are available on the global catalog server when using contact photographs. If possible, enable these attributes on the global catalog server instead of relying on the domain controller. Directory integration looks for domain controllers on port 389 and global catalog servers on port 3268 by default. Specifying a port during configuration overrides these defaults.

Security

EDI encrypts all authentication data by default. If encryption is required for user credential and query data, SSL can be enabled. In this scenario, the SSL connection certificate must be present in the Microsoft Windows certificate store. In a Microsoft Windows domain, this certificate would typically be part of the workstation certificate store by default. SSL uses port 636 when communicating with a domain controller and port 3269 when communicating with a global catalog server. These defaults can be changed.

Microsoft Windows encryption may need to be disabled in non-Microsoft Windows Server environments. In such instances a basic bind will be used to connect to the directory. Credentials are transmitted in clear text when a basic bind is in use. SSL usage is highly recommended in this scenario.

Administrators can use a common set of credentials for directory integration to authenticate for directory queries. Administrators would push the credentials out to all workstations using a group policy or manipulation of registry settings. This is typically used when third party directory services are used. If credentials are not provided but required for the query, directory integration will attempt an anonymous bind to the service.

Photo Retrieval

Basic directory integration provides for the retrieval for contact photograph Universal Resource Indicators (URI). EDI provides three methods for photo retrieval:

- **Binary photograph retrieval**

  EDI retrieves the attribute content of the directory attribute defined by PhotoUri group policy or registry setting. Directory integration then parses the attribute content. If the attribute contains binary data it will be displayed as a JPEG photograph. If the attribute contains a URI the photo will be retrieved from it. If a directory user object stores photos in the “thumbnailphoto” attribute, setting the PhotoURI setting to “thumbnailphoto” forces directory integration to retrieve the photo from this field. A photo can also be stored in the “jpegPhoto” attribute in the active directory.

- **Photo URI retrieval**

  EDI retrieves a contact photo based on the provided resource indicator. This resource indicator is formatted as a static HTTP request. No error checking is provided.

- **Enhanced URL retrieval**

  EDI retrieves a contact photo based on a dynamically constructed resource indicator using directory attributes. The URI is typically constructed using a base value plus the dynamic portion of the URI drawn from directory attributes.

Forced Authorization Codes Support

Forced Authorization Codes (FAC) allow for the limiting of phone usage to certain numbers by requiring users to enter authorization codes. When the user calls a number associated with an FAC route pattern, they will be prompted to enter the associated code. If the code is correct the call is allowed to proceed.

Client Matter Codes

Client matter codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients by forcing the user to enter a code to specify that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes.

TLS and SRTP Support

Cisco Unified Personal Communicator supports TLS for signaling and SRTP for secure media streaming.

Cisco VPN Client and CAST video

The Cisco VPN Client does not support CAST video on computers running in a 64 bit environment. Use the Cisco AnyConnect Client instead of the Cisco VPN Client in 64 bit environments.

Cisco VT Camera II Support on Microsoft Windows 7 64-bit

Cisco Unified Personal Communicator includes support for the Microsoft Windows 7 64-bit and the Cisco VT Camera II. The Cisco VT Camera II however is not supported on Microsoft Windows 7 64-bit. Although Cisco Unified Personal Communicator provides support for both, this does not mean the Cisco VT Camera II will run on Microsoft Windows 7 64-bit using Cisco Unified Personal Communicator. Users of the Cisco VT Camera II running a Microsoft Windows 7 64-bit environment must use a different camera.

Enhanced Directory Integration Functionality and Cisco Unified Personal Communicator

Please note the following items when using the Enhanced Directory Integration functionality introduced in Cisco Unified Personal Communicator 8.5(2):

- Do not deploy the Enhanced Directory Integration features of Cisco Unified Personal Communicator to clients still running Cisco Unified Personal Communicator 8.5(1).
- Contact names may be abbreviated if populated using Enhanced Directory Integration functionality. In this instance, the native value must be overridden with a custom value.
- Three characters must be specified when using the Enhanced Directory Integration search provider with Cisco Unified Personal Communicator before results are returned.
- Phone or directory number searches are not available using Enhanced Directory Integration functionality.
- The following registry keys may require population in some instances to use photographs after enabling Enhanced Directory Integration functionality:
  - PhotoUriSubstitutionEnabled
  - PhotoUriSubstitutionToken
  - PhotoUriWithToken

Cisco Unified Communications Manager 6.1(3) and Conference Participant Lists

If you use Cisco Unified Communications Manager 6.1(3), in conference calls the names of the participants are incorrect in the participant list.

Other Party Hears Cuts or Clips in Audio on a Call

When you are on a call with audio, or with audio and video, the other party might hear cuts or clips in your audio. The following table shows a possible solution to this problem. This solution relates only to particular audio devices, so you might not see the microphone boost setting referred to in the solution.

Operating System	Suggested Solution
Microsoft Windows Vista, Microsoft Windows 7	1. Open the Control Panel. 2. Select **Hardware and Sound**. 3. Select **Manage audio devices**. 4. Select the **Recording** tab. 5. Select the microphone that is currently in use. 6. Select **Properties**. 7. Select the **Levels** tab on the Microphone Properties dialog box. 8. Adjust the volume and the microphone boost settings to suit your requirements.
Microsoft Windows XP	1. Open the Control Panel. 2. Select **Sounds and Audio Devices**. 3. Select the **Audio** tab. 4. Select **Volume** in the Sound recording section. 5. Select the **Advanced** button under the Microphone section in the Capture dialog box. 6. Ensure that **Microphone Boost** check box is not checked.

Users Hear Echo on Calls

When you are on a call with audio, or with audio and video, you might hear an echo. Camera microphones often have issues with echo. If you have selected your camera microphone as your microphone device, consider using a non-camera microphone as your microphone device.

To select another microphone device, follow these steps:

Procedure

Step 1 Plug in your headset or other microphone device to the appropriate USB port.

Step 2 Wait for your operating system to recognize the device.

Step 3 Select **File > Options > Audio** in Cisco Unified Personal Communicator.

Step 4 Select your device from drop-down list. You can also set the volume of the device if required.

Voice Messages Show a Duration of Zero

When you view your voice messages, the duration of some messages might appear as zero. This problem occurs in releases of Cisco Unity and Cisco Unity Connection that are not supported by Cisco Unified Personal Communicator. To resolve this issue, upgrade your release of Cisco Unity or Cisco Unity Connection to a release that is supported by Cisco Unified Personal Communicator. For information on supported releases of Cisco Unity and Cisco Unity Connection, see Server Requirements, page 5.

Adding an Audio Call to a Video Call Results in an Audio Call

When you add an audio call to a video call, the party on the audio call does not receive a request to add video to their call. When the calls are merged, the call becomes an audio call.

Users of Cisco Unified IP Phone 8961, 6900 Series, and 9900 Series Models Cannot Control Desk Phone

If users with a Cisco Unified IP Phone 8961, 69*xx*, or 99*xx* model desk phone cannot use their desk phone from Cisco Unified Personal Communicator, you must add the users to the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** user group. For more information about how to do this, see the *Deployment Guide for Cisco Unified Presence*:

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

JTAPI Error When a Call Is Placed

Users might see a JTAPI error about 15 seconds after they place a call, when Cisco Unified Personal Communicator is set to use the desk phone for phone calls.

To resolve this issue, ensure that your dial plan is set up correctly on Cisco Unified Communications Manager. In particular, ensure that Cisco Unified Communications Manager does not need to wait for more digits to be dialed.

For detailed information on setting up your dial plan, see the Cisco Unified Communications Manager Administration online help, or the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*:

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

Limitation with Shared Lines When Deploying with Cisco Unified SRST

If you have Cisco Unified Survivable Remote Site Telephony (SRST) set up in your Cisco Unified Communication system, you can continue to place and receive calls during a system failure. In these circumstances, the Cisco Unified Personal Communicator uses shared lines to enable you to continue to place and receive calls.

Cisco Unified SRST does not support shared lines with SIP phones. Cisco Unified Personal Communicator receives only alternate calls if both of the following conditions occur:

- Cisco Unified Personal Communicator is set to use your computer for phone calls.
- Cisco Unified Personal Communicator has the same directory number as a SIP desk phone.

However, the desk phone receives all calls.

Specifying Audio Value Names

Before you install Cisco Unified Personal Communicator, you must perform some configuration on the computers of your users. You can specify the Cisco Unified Client Services Framework client settings, including an Audio_ISAC_Advertised setting. This specifies whether to enable the advertising of the availability of the audio iSAC codec. Enter one of the following values for this setting:

- 0: Disables advertising.
- 1: Enables advertising.

The iSAC audio codec is only supported in Cisco Unified Communications Manager Release 8.0 and later.

How Cisco Unified Personal Communicator Determines the Audio Codec to Use on a Call

Cisco Unified Personal Communicator uses Cisco Unified Communications Manager devices for your Cisco Unified Personal Communicator software, and for your desk phone.

The audio bit rate capability of these devices is one of several factors that determine the audio capability of Cisco Unified Personal Communicator for the user. You specify this bit rate capability in Cisco Unified Communications Manager.

To configure the bit rate capability of these devices, use the region settings of the device pool that the devices are in. The following settings affect the audio bit rate capability of the devices:

Release of Cisco Unified Communications Manager	Settings
8.0 or later	Max Audio Bit Rate
Earlier than 8.0	Audio Codec

For more information about region and device pool configuration in Cisco Unified Communications Manager, see the Cisco Unified Communications Manager Administration online help, or the *Cisco Unified Communications Manager Administration Guide*:

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

When you place a call in Cisco Unified Personal Communicator, both endpoints advertise their audio codec capability to the Cisco Unified Communications Manager. The Cisco Unified Communications Manager selects the highest possible common codec between them. The default audio codec is G.711.

Chat Slow with Wireless Connection from Some Laptops

On some laptop computers, after you connect to a wireless network, then start a chat with a contact, CPU usage by the cupc.exe process might increase significantly.

To resolve this problem, install the latest display drivers for your laptop computer. If your computer is a Lenovo ThinkPad R400, T400, T500, or W500, install the drivers at the following URL:

http://www-307.ibm.com/pc/support/site.wss/MIGR-70366.html

16-Bit Color Quality Might Cause High CPU Usage

Under certain rare conditions, Cisco Unified Personal Communicator might use higher than expected CPU resources. Users might notice that typing becomes slow, and see irregular movement when they move windows.

Try the following workarounds for this issue:

- Install the latest display drivers for your laptop computer.
- Change your display color quality from 16 bit to another setting.

Availability Status Not Displayed in Microsoft Office

Both Cisco Unified Personal Communicator and Microsoft Office Communicator use the Microsoft Office Communicator Automation API to provide availability status, instant messaging, and telephony features to Microsoft Office. These features can only be provided by one of these applications at a time.

If you install Cisco Unified Personal Communicator after Microsoft Office Communicator, then you want to use these features from the Cisco Unified Personal Communicator integration, you must uninstall Microsoft Office Communicator, then run the Cisco Unified Personal Communicator installer again, and select the Repair option. If your availability status is not displayed in the To and Cc fields of your messages in Microsoft Office, then update the following group policy settings or registry settings on your computer:

Policy	Set Value To...
EnablePresence	2
SetOnlineStatusLevel	2

Alternatively, you can apply the following keys to set the policies manually:

Microsoft Office 2007

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\IM]"EnablePresence"=dword:00000002

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\IM]"SetOnlineStatusLevel"=dword:00000002

Microsoft Office 2010

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\14.0\Outlook\IM]"EnablePresence"=dword:00000002

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\14.0\Outlook\IM]"SetOnlineStatusLevel"=dword:00000002

Uninstalling Microsoft Office Communicator

After you uninstall Microsoft Office Communicator, delete the contents of the folders listed in the following table:

Operating System	Delete the Contents of These Folders...
Microsoft Windows Vista, Microsoft Windows 7	<*drive*>:\Users\<*username*>\AppData\Local\Cisco\Unified Communications\ <*drive*>:\Users\<*username*>\AppData\Roaming \Cisco\Unified Communications\
Microsoft Windows XP	<*drive*>:\Documents and Settings\<*username*>\Local Settings\Application Data\Cisco\Unified Communications\ <*drive*>:\Documents and Settings\<*username*>\Application Data\Cisco\Unified Communications\

Also clear the contents of the following registry key value name:

HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData

Overriding the Default Language and Regional Settings Used by Cisco Unified Personal Communicator

Cisco Unified Personal Communicator uses the operating system settings (GetUserDefaultLCID) to determine the desired language and regional settings. To override these settings, you can add values to the following registry key:

HKEY_CURRENT_USER\SOFTWARE\Cisco Systems, Inc.\Unified Communications\CUPC\

The values that you can add are:

- UseThisLanguageCulture - sets the language, specified as a four digit locale, for example, en-US.
- UseThisFlowDirection sets the flow direction, for example, RightToLeft. This should only be set for RTL languages.
- UseThisLocaleCulture sets the culture, specified as a four digit locale, for example, en-US.

Errors Displayed After Signing In to a Different Cisco Unified Presence Server

Problem After switching to a different Cisco Unified Presence server during sign-in, you encounter some functional errors.

Solution Do the following:

1. Delete the contents of the following directory:
   - **Microsoft Windows Vista/Microsoft Windows 7:** <*drive*>:\Users\<*username*>\AppData\Roaming\Cisco\Unified Communications\Client Services Framework\
   - **Microsoft Windows XP:** <*drive*>:\Documents and Settings\<*username*>\Application Data\Cisco\Unified Communications\Client Services Framework\
2. Restart Cisco Unified Personal Communicator.

Long Meeting Passwords in Cisco WebEx Cause Problems

Problem Long meeting passwords in Cisco WebEx cause Cisco Unified Personal Communicator to disconnect from Cisco WebEx temporarily.

Solution There is a server limit on the number of characters that can be used for a meeting password. Cisco Unified Personal Communicator does not display an error if this limit is exceeded. For some languages such as Japanese, the number of characters is reduced.

Additions to Deployment Documentation

Configuring Mailstore Server Names and Addresses on Cisco Unified Presence for Secure Voicemail

In Chapter 12 of the *Cisco Unified Presence Release 8.5 Deployment Guide*, in the section entitled "Configuring Mailstore Server Names and Addresses on Cisco Unified Presence", there should be a note saying:

Note To configure Cisco Unified Personal Communicator for secure message playback from Cisco Unity Connection, you must select **TLS** as the protocol and set the IMAP port to **7993**.

Before You Start Cisco Unified Personal Communicator as a Desktop Agent

In Chapter 12 of the *Cisco Unified Presence Release 8.5 Deployment Guide*, in the section entitled "Before You Start Cisco Unified Personal Communicator as a Desktop Agent", in addition to the two registry keys described in Step 1 of the procedure, you must also set the following registry key:

- PhoneService_UseCredentialsFrom = optional_cup

This specifies that your Cisco Unified Presence credentials are used to sign into Cisco Unified Communications Manager.

Notes on Video

Factors That Affect the Video Capability of Users

Factors that affect the frame format and frame rate that can be achieved on a video call are:

- Cisco Unified Communications Manager configuration of device bit rate limits.
- User settings, such as the options that are available to the user through the Options dialog box in Cisco Unified Personal Communicator.
- Selected camera.
- CPU speed and usage.
- Cisco Unified Meeting Place or Cisco Unified Video Advantage configuration of videoconferencing parameters.
- Video capability of the other endpoints on a call.
- The parameters of the network between the two endpoints, such as, the physical network bandwidth and the router configuration in the network path of the call.

Determining the Bit Rate Required for a Particular Video Capability

Use Table 12 to determine the minimum bit rate that your Cisco Unified Personal Communicator requires to attain a particular frame format and frame rate.

Table 12 Minimum Bit Rates to Use for Particular Frame Formats and Frame Rates

Combined Bit Rate for Audio and Video (kb/s)	Audio Codec Allowance (kb/s)	Minimum Video Call Bit Rate (kb/s)	Frame Format	Frames per Second
78	14	64	QCIF	15
142	14	128	QCIF	30
206	14	192	CIF	15
320	64	256	CIF	30
448	64	384	VGA	15
576	64	512	VGA	30
832	64	768	VGA	30
1064	64	1000	720p	15
2064	64	2000	720p	30

Example

To configure Cisco Unified Personal Communicator for a user to be capable of video with VGA frame size, at 30 frames per second, Cisco Unified Personal Communicator requires a combined audio and video bit rate of at least 768 kb/s. Allow 64 kb/s for the audio codec to use with VGA frame format.

Configuring the Bit Rate Capability for Cisco Unified Personal Communicator

Cisco Unified Personal Communicator uses Cisco Unified Communications Manager devices for your Cisco Unified Personal Communicator software, and for your desk phone.

The bit rate, or bandwidth, capability of these devices is one of several factors that determine the video capability of Cisco Unified Personal Communicator for the user. You specify this bit rate capability in Cisco Unified Communications Manager.

To configure the bit rate capability of the devices, use the region settings of the device pool that the devices are in. The following settings affect the bit rate capability of the devices:

Release of Cisco Unified Communications Manager	Settings
8.0 or later	• Max Audio Bit Rate • Max Video Call Bit Rate
Earlier than 8.0	• Audio Codec • Video Call Bandwidth

For more information about region and device pool configuration in Cisco Unified Communications Manager, see the Cisco Unified Communications Manager Administration online help, or the *Cisco Unified Communications Manager Administration Guide*:

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

Example

If you want your devices to be capable of 720p HD video calls at 30 frames per second (fps), configure the Region Settings to allocate a bit rate that can handle the 720p HD video at 30 fps, as well as the audio for the call.

If Cisco Unified Personal Communicator requires a minimum bit rate of 2000 kb/s to make a HD video call, and the audio bit rate for the region is set to 64 kb/s (G.722, G.711), then you must put the devices in a device pool that is in a region that is configured to have a video call bit rate as shown in the following table:

Release of Cisco Unified Communications Manager	Video Call Bit Rate
8.0 or later	Greater than or equal to 2064 kb/s.
Earlier than 8.0	Greater than or equal to 2000 kb/s. Releases of Cisco Unified Communications Manager earlier than 8.0 automatically add the audio bandwidth to the configured video bandwidth to allocate bandwidth for the call.

How Cisco Unified Client Services Framework Determines the Video Capability of Your Computer

Cisco Unified Client Services Framework derives the hardware profile of the machine as a WEI score. Cisco Unified Client Services Framework uses the WEI processor subscore to determine the send and receive video profile that is appropriate for your computer.

Table 13 lists the H.264/AVC levels that are supported, the bit rate and frame format for each level, and the minimum WEI processor subscore that is required to support each level

Table 13 Video Capabilities Supported for WEI Processor Subscores

H.264/AVC Level	Maximum Bit Rate (kb/s)	Maximum Frame Format	Minimum WEI Processor Subscore Required to Send and Receive Video at This Level
1.0	64	QCIF	4.0
1b	128	QCIF	4.0
1.1	192	CIF	4.0
1.2	384	CIF	4.0
1.3	768	CIF	4.0
2	768	CIF	4.0
2.1	768	CIF	4.0
2.2	1350	VGA	4.8
3	1350	VGA	4.8
3.1	4000	HD	5.9

Limiting of Usage of Bandwidth by Users

The Video section in the Cisco Unified Personal Communicator Options dialog box contains a slider that enables you to limit the bandwidth that Cisco Unified Personal Communicator uses for video calls. Table 14 lists the bandwidth settings that are available on the slider, from highest to lowest, and the video implications for each level.

Table 14 Bandwidth Settings Available to Users

Bandwidth Settings Available	H.264/ AVC Level	Maximum Decoder Bit Rate	Maximum Encoder Bit Rate	Description
Highest video quality (Level 6)	3.1	4 Mb/s	4 Mb/s	Allows the maximum video capabilities supported by Cisco Unified Client Services Framework, currently 720p HD.
Level 5	2.2	4 Mb/s	768 kb/s	Supports VGA in both directions.
Level 4	2.2	4 Mb/s	384 kb/s	Supports scenarios where downstream bandwidth is less than upstream. Supports incoming VGA.

Table 14 Bandwidth Settings Available to Users (continued)

Bandwidth Settings Available	H.264/ AVC Level	Maximum Decoder Bit Rate	Maximum Encoder Bit Rate	Description
Level 3	1.3	768 kb/s	384 kb/s	Limits incoming video to CIF at 30 frames per second (fps).
Level 2	1.2	384 kb/s	128 kb/s	Limits incoming video to CIF at 15 fps.
Lowest bandwidth usage (Level 1)	1.1	192 kb/s	64 kb/s	Limits incoming video to QCIF at 30 fps, or potentially CIF at 7.5 fps. **Note** This setting can render QCIF video at 6 fps, which may result in poor image rendering with some cameras.

About Tuning Computers for Maximum Video Performance

To tune your computer for maximum video performance, do the following:

- Set your CPU speed to maximum performance. Open the power options tool in your Control Panel and select the highest possible power plan or scheme.
- Set your graphics hardware to full acceleration. Open the display tool in your Control Panel and set the hardware acceleration slider to full.

Note To support this setting, you may need to update the driver for your video adapter. For information about how to obtain an updated driver for your video adapter, contact the manufacturer of your video adapter or the manufacturer of your computer.

Video Troubleshooting Tips

- Users See Video Impairments, page 51
- Video Conversations with Multiple Displays, page 52
- Users Might See Lower Video Quality When Computer Is Connected to Some Models of Cisco Unified IP Phone, page 52

Users See Video Impairments

Problem Under certain rare conditions, users may see some video impairment such as blockiness, smearing, streaking, or ghosting in the following situations:

- At the start of a video call or during a video call when the Hold or Resume functions are used.
- During a call when the user adjusts the video quality using the slider in the Video section of the Options dialog box.

This problem occurs when:

- The client computer is capable of handling high-resolution video but the network or switch has insufficient bandwidth to support the video resolution.
- There is packet loss on the network.
- There is packet loss along the network due to video packet fragmentation, if the Maximum Transmission Unit (MTU) of the network interface card at either endpoint is set lower than the Cisco Unified Personal Communicator MTU of 1270.
- There are packets dropped at routers along the call path.
- The Cisco Unified Client Services Framework device that is associated with the installation of Cisco Unified Personal Communicator is set up in Cisco Unified Communications Manager for a bandwidth that the physical network that the device is located on does not support. For example, if you are on a physical network that has a 128 kb/s bandwidth and you configure the Cisco Unified Client Services Framework device for a bandwidth setting of 4 Mb/s, then the call starts at a higher video codec level than the underlying physical network actually supports.

Try one or more of the following suggested solutions.

Solution Put the Cisco Unified Client Services Framework device in a device pool that is in a region that is configured to have a maximum video bit rate that is less than the bandwidth of your physical network. For more information, see Determining the Bit Rate Required for a Particular Video Capability, page 48.

Solution Perform the following steps:

1. Open the Options dialog box.
2. Select **Video**.
3. Use the slider to set the balance between bandwidth usage and video quality.
4. Ensure that the **Optimize video quality for your computer** option is selected.

Video Conversations with Multiple Displays

If your computer displays on more than one device, use the primary display for video conversations. Video hardware acceleration is generally not supported on non-primary displays, so CPU usage on non-primary displays becomes very high.

Users Might See Lower Video Quality When Computer Is Connected to Some Models of Cisco Unified IP Phone

Problem Users might see lower video quality in Cisco Unified Personal Communicator when their computer is connected to some Cisco Unified IP Phone models, such as 7945G, 7965G, and 7975G.

This problem occurs if the link speeds and duplex configuration on either end of the connection are not the same. For example, if the link speed of the port at the PC port is 1000 Mb/s and the switch port is connected at 100 Mb/s. Alternatively, if the link on one end of the connection is half duplex, and the link on the other end is full duplex.

Contact your Cisco Support representative to get the latest update on this issue.

Solution To address this issue, perform the following steps:

1. Go to the Network Configuration settings for your phone.
2. Set the **SW Port Configuration** setting to **100 Full**.
3. Set the **PC Port Configuration** setting to **100 Full**.

For information about how to set network configuration settings on your Cisco Unified IP Phone, see the documentation for your phone. See publications that are specific to your language, phone model, and Cisco Unified Communications Manager release. You can navigate to the documentation for your phone from the following URL:

http://www.cisco.com/cisco/web/psa/maintain.html?mode=prod&level0=278875240

Camera Troubleshooting Tips

Some Web Cameras Start When Users Sign In

The correct behavior of web cameras is that web cameras start when users start a video call, or a video conference call. In particular circumstances, some web cameras start when users sign in to Cisco Unified Personal Communicator. This occurs on particular hardware configurations, with particular web camera driver software.

In these circumstances, Cisco Unified Personal Communicator controls the web camera. Other applications cannot access the camera. However, you can still use the web camera for video calls, video conference calls, and so on.

To resolve this problem, install the latest drivers from the manufacturer of your web camera. If your computer is a Lenovo ThinkPad W500, install the drivers at the following URL:

http://www-307.ibm.com/pc/support/site.wss/MIGR-70600.html

Poor Sound Quality on the Tandberg PrecisionHD USB Camera on Microsoft Windows 7

Problem When using the Tandberg PrecisionHD USB Camera Version 1.0 or 1.1 with Microsoft Windows 7, a very high input gain is set for your microphone, which can cause the sound to be distorted or extremely low.

Solution To fix this problem in the short-term, lower the recording volume for your microphone in the Microsoft Windows settings.

To resolve this issue completely, install the software upgrade version 1.2 for the PrecisionHD USB Camera, as follows:

1. Download the upgrade from the following location:

   http://www.tandberg.com/support/video-conferencing-software-download.jsp?t=2&p=94
2. Connect your PrecisionHD USB camera to your computer.
3. Make sure the LED is green before you start the upgrade.
4. Install the software upgrade.

Tandberg PrecisionHD Camera Requires Microsoft Windows Security Update

Problem The video image from a Tandberg PrecisionHD camera might not be displayed if the video quality slider setting in the video options is set to a value greater than 384 Kb/s up, 4 Mb/s down.

Solution Install the following Microsoft Windows security update:

http://support.microsoft.com/kb/975560

Caveats

Using the Bug Toolkit

You can search for problems by using the Cisco Software Bug Toolkit. Known problems (bugs) are graded according to severity level. These release notes list the following types of bugs:

- All severity level 1, 2, or 3 bugs.
- Significant severity level 4 or 5 bugs.
- All customer-found bugs.

Before You Begin

To access Bug Toolkit, you need the following:

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

Procedure

Step 1 To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Sign in 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**.

For information about how to search for bugs, create saved searches, create bug groups, and so on, click **Help** on the Bug Toolkit page.

Open Caveats

Table 15 describes possible unexpected behavior by Cisco Unified Personal Communicator on Microsoft Windows. The table is sorted by severity, then by identifier in alphanumeric order.

Unless otherwise noted, these caveats apply to all Cisco Unified Personal Communicator releases. Because defect status continually changes, be aware that the tables reflects a snapshot of the defects that were open at the time this report was compiled. For more information about an individual defect, click

the associated identifier in the table to access the online record for that defect, including workarounds. For an updated view of open defects, access the Bug Toolkit. For details, see Using the Bug Toolkit, page 54.

Note Some of the headlines in Table 15 refer to Cisco Unified Integration for Microsoft Office Communicator, but are also relevant to Cisco Unified Personal Communicator.

Note Some caveats described in the Cisco Unified Presence release notes and in the Cisco Unified Communications Manager release notes might appear to be Cisco Unified Personal Communicator caveats. Use these links to access them:
http:/www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Table 15 Open Caveats for Cisco Unified Personal Communicator

Identifier	Severity	Component	Headline
CSCts13307	3	ms-integration	C2C ribon button calls myself rather than the sender of meeting requests
CSCts18483	3	install-and-deploy	CUPC crashes when launched or uninstalled as guest user
CSCtt01275	3	video-svc	Video conference: user has to hold and resume call to get video feed
CSCtu07138	3	performance	CUP Client 8.5.2 Takes More CPU Cycles Then 8.5.1 When Virtualized
CSCtz24058	3	telephony.video	No video after hold & resume in DP mode - CUCM 8.5 & SCCP specific
CSCtz24083	4	telephony.video	No video between CUPC clients with particular bandwidth settings in CUCM
CSCtz28276	4	presence	Presence not available in Outlook if it's started before CUPC.

Resolved Caveats

This section lists caveats that may have been open in previous releases and are now resolved.

Caveats are listed in order of severity and then in alphanumeric order by bug identifier. Only severity 1, severity 2, and select severity 3, 4, 5, and 6 resolved defects, as well as all customer-found defects, are listed in this section. Because defect status continually changes, be aware that this document reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access the Bug Toolkit (see the Using the Bug Toolkit, page 54).

The following sections list caveats that are resolved in Cisco Unified Personal Communicator but that may have been open in previous releases:

Release 8.6(3)

Table 16 lists the caveats that were resolved in Release 8.6(3).

Table 16 Resolved Caveats for Cisco Unified Personal Communicator 8.6(3)

Identifier	Severity	Component	Headline
CSCtz52872	2	system-svc	Group Chat freezes CUPC when Groupname contains Hebrew characters
CSCty88864	3	video-svc	DP video does not work when controlling 9971 with latest firmware 9-3-27
CSCub06302	3	documentation	Unable to uninstall CUPC 8.5.5 from command line
CSCub38189	3	video-svc	CUCI-Lync\CUPC intermittently shows error message "Video subscription error.."
CSCub66388	3	cdp	CDP driver is not uninstalled properly
CSCub68454	4	presence	CUPC Inconsistent Presence Status when Search Directory window is opened
CSCub89383	4	im.groupchat	CUPC - Cursor is not placed in the chat entry space
CSCtz57316	6	click2call-docs	Extra prompt to save template in Word

Release 8.6(2)

Table 17 lists the caveats that were resolved in Release 8.6(2).

Table 17 Resolved Caveats for Cisco Unified Personal Communicator 8.6(2)

Identifier	Severity	Component	Headline
CSCty68194	2	webconf-svc	CUPC does not Support New Interface to MP 8.5
CSCua31395	2	system-svc	CUPC 8.6 - Wrong time Zone when Webex meeting is started from CUPC
CSCua38521	2	ms-integration	Application does not Minimize/Maximize on click on Windows Taskbar

Table 17 Resolved Caveats for Cisco Unified Personal Communicator 8.6(2)

Identifier	Severity	Component	Headline
CSCua73132	2	ms-integration	The first chat in CUPC will grab window and cursor focus
CSCty64291	3	cdp	CUPC client creates bogus MAC address for CDP
CSCua24727	3	system-logging	Core Log files stored in incorrect location
CSCua73189	3	ms-integration	The first chat in the session is always sent with the "system" font
CSCtr62194	4	phone-deskphone	Jtapi error when ringing FAC/CMC number & wrong code entered - dp mode
CSCtx66063	4	ms-integration	CUPC Chat Window Closes when Closing Outlook Email with ESC Key
CSCtx89372	4	phone-deskphone	CSF should handle JTAPI error condition of busy.
CSCtz58756	4	hub.login	CUPC does not launch due to DNS lookup
CSCua68155	4	presence-svc	Client timeout for SOAP/HTTP connections (to CUP) to be increased to 15s
CSCua70807	4	presence-svc	CUPC 8.6.1 Error starting adhoc group chat
CSCua95555	4	telephony.audio	CUPC 8.6 - Video on by Default for all Audio Calls
CSCty84106	6	ms-integration	c2x integration with sharepoint doesn't work properly
CSCua11785	6	performance	Make location that CUPC use %localappdata% to be configurable
CSCua33796	6	video-svc	Disable CDP through registry key

Release 8.6(1)

Table 18 lists the caveats that were resolved in Release 8.6(1).

Table 18 Resolved Caveats for Cisco Unified Personal Communicator 8.6(1)

Identifier	Severity	Component	Headline
CSCty70853	2	documentation	MP interop has to be changed to show releases we do support not MP 8.5
CSCto35556	3	audio-svc	One way audio with CUCIMOC/CUPC (CSF Client)
CSCtw55923	3	phone-softphone	RTP packets not marked for Windows XP in user mode.
CSCtw97148	3	video-svc	CUPC crash when making video call to Polycom RMX 1500MCU
CSCtx86489	3	ms-integration	OutOfMemory exception causes CUPC to crash intermittently
CSCtx89637	3	api-general	CUPC Client cannot login when Special Character is in the Password
CSCtz20605	3	config-svc	Turkish Localisation - no contacts shown or options to make call.
CSCtr94349	4	phone-svc	Primary client does not unregister softphone device when user logs off
CSCty26353	4	audio-svc	CUPC sends its RTP packets in multiple stages
CSCty26511	4	audio-svc	CUPC sends RTPs with delay up to 600 ms in case of Early Media
CSCth40288	6	install-and-deploy	Include the VC++ libraries in the CSF as private assemblies

Table 18 Resolved Caveats for Cisco Unified Personal Communicator 8.6(1)

Identifier	Severity	Component	Headline
CSCty38098	6	video-svc	CUPC selects a video device (Bloomberg) which is not a webcam
CSCty63071	6	documentation	CUPC 8.5 Release Notes states support for CUCM 6.1(3) or 6.1(x) Wrong

Accessibility Notes

Cisco Unified Personal Communicator is introducing accessibility features in phases. Users familiar with previous versions of Cisco Unified Personal Communicator will see a subset of keyboard shortcuts and features in this release.

For additional information, see:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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 uses RSS version 2.0.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending e-mail to export@cisco.com.
