Release Notes for *Cisco Unified Customer Voice Portal (CVP) Release 4.0(1) and Release 4.0(1) Service Release 1*

March 19, 2007

Contents

Introduction

This document discusses new features, changes, and caveats for Release 4.0(1) and Release 4.0(1) Service Release 1 of Cisco Unified Customer Voice Portal (CVP).

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

Additional information on new features, and on many of the product changes, is available in the relevant end-user documentation.

Note For the most up-to-date version of all Cisco documentation, go to the Cisco Web page: http://www.cisco.com/public/support/tac/documentation.html

In particular, for the most up-to-date version of these release notes, go to the Cisco Web page: http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_release_notes_list.html

Cisco Unified CVP 4.0(1) Service Release 1 Required

Installation of Cisco Unified CVP Release 4.0(1) Service Release 1 or later service or maintenance release is required after installing Cisco Unified CVP Release 4.0(1).

Two CDs are shipped with Cisco Unified CVP Release 4.0(1): a CD for Release 4.0(1), and a CD for Release 4.0(1) Service Release 1. You *must* install *both* products; Release 4.0(1) first, then Release 4.0(1) Service Release 1. See the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* for installation instructions.

System Requirements

For hardware and third-party software specifications for Release 4.0(1), refer to the *Hardware and Software System Specification for Cisco Unified Customer Voice Portal Software Release 4.0(1)*, which is accessible from http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html

Related Documentation

- Documentation for Cisco Unified Customer Voice Portal (CVP) is accessible from http://cisco.com/en/US/products/sw/custcosw/ps1006/tsd_products_support_series_home.html
- Documentation for Cisco Unified Intelligent Contact Management Enterprise (ICME) is accessible from http://www.cisco.com/en/US/products/sw/custcosw/ps1001/tsd_products_support_series_home.html
- Documentation for Cisco Unified Intelligent Contact Management Hosted (ICMH) is accessible from http://www.cisco.com/en/US/products/sw/custcosw/ps1973/tsd_products_support_series_home.html
- Documentation for Cisco Unified Customer Contact Enterprise (CCE) is accessible from http://www.cisco.com/en/US/products/sw/custcosw/ps1844/tsd_products_support_series_home.html
- Documentation for Cisco Unified Customer Contact Hosted (CCH) is accessible from http://www.cisco.com/en/US/products/sw/custcosw/ps5053/tsd_products_support_series_home.html

- Documentation for Cisco Unified CallManager is accessible from http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
- Technical Support documentation and tools can be accessed from http://www.cisco.com/en/US/support/index.html
- The Product Alert tool can be accessed through http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice

New and Changed Information

The following sections describe new features and changes that are pertinent to this release.

Session Initiation Protocol (SIP)

Unified CVP 4.0 provides the ability to switch calls using SIP rather than, or in addition to, H.323. Only H.323 was provided in earlier versions of CVP.

Operations Console

Unified CVP 4.0 provides the ability to monitor and configure the entire Unified CVP solution from a single operations console.

Reporting

Unified CVP 4.0 provides the ability to generate custom reports on the activities of Unified CVP components, Unified CVP IVR applications, and Unified CVP IVR callers.

Call Director Call Flow Model

The new Call Director call flow model is for customers who:

- Want to use Unified CVP only to provide Unified ICME with VoIP call switching capabilities
- Do not need to use Unified CVP to control queued calls
- Want to prompt/collect using third-party VRUs or ACDs

- Do not want to use Unified CVP VoiceXML Server

Deprecation of Queue and Transfer Model

The Queue and Transfer call flow model, which was supported in previous versions of CVP, is not supported for new customers in Unified Customer Voice Portal 4.0. New customers are advised to use the Comprehensive model instead.

Name Changes

- Advanced Speech model is now referred to as VRU-Only model
- CVP Voice Browser is now referred to as H.323 Service
- Cisco Customer Voice Portal is renamed Cisco Unified Customer Voice Portal (abbreviated as Unified CVP)
- Effective with Cisco CallManager Releases 4.1(3), 4.2(1), 5.0(2), Cisco CallManager is renamed Cisco Unified CallManager
- Effective with Release 7.1(1), Cisco ICM Enterprise Edition is renamed Cisco Unified Intelligent Contact Management Enterprise (abbreviated as Unified ICME). Cisco ICM Hosted Edition is renamed Cisco Unified Intelligent Contact Management Hosted (abbreviated as Unified ICMH). The Unified CVP manuals reference these products by the new names, though the new names do not appear in the Release 7.1(1) user interface.
- Effective with Release 7.1(1), Cisco IPCC Enterprise Edition is renamed Cisco Unified Contact Center Enterprise (abbreviated as Unified CCE). Cisco IPCC Hosted Edition is renamed Cisco Unified Contact Center Hosted (abbreviated as Unified CCH). The Unified CVP manuals reference these products by the new names, though the new names do not appear in the Release 7.1(1) user interface.

Note These new names are introduced in Release 7.1(1). They are referenced in opening screens and documentation, but they do not yet appear throughout the user interface.

Cisco Security Agent (CSA) for Unified CVP 4.0

The standalone Cisco Security Agent versions provided with earlier releases of CVP are not supported with Unified CVP 4.0. If you are upgrading from an earlier release of CVP/ISN, you must uninstall the version of CSA that you have, prior to upgrading to Unified CVP 4.0.

For more information on Cisco Security Agent for Cisco Unified Customer Voice Portal 4.0, and to download this product, refer to:
http://www.cisco.com/kobayashi/sw-center/contact_center/csa/
and to the document *Cisco Security Agent Installation/Deployment Guide for Cisco Unified Customer Voice Portal*.

Note If you plan to use the standalone Cisco Security Agent on a Reporting Server, please see Cisco Security Agent and Reporting Server, page 8.

User Documentation Changes

This section discusses changes and additions to the Unified CVP documentation set.

- *Planning Guide for Cisco Unified Customer Voice Portal*—provides a product overview and describes how to plan a Unified CVP deployment (should be used in conjunction with the *Cisco Unified Customer Voice Portal (CVP) Release 4.0 Solution Reference Network Design (SRND)* document). This document replaces the *Cisco Customer Voice Portal Product Description*.
- *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*—combines information formerly split between the *Cisco Customer Voice Portal Installation Guide* and the *Cisco CVP VoiceXML Installation Guide*, as well as containing information on installing the Unified CVP Reporting component.
- *Reporting Guide for Cisco Unified Customer Voice Portal*—a new manual that describes how to configure and manage the Reporting Server and reporting database.
- *Troubleshooting Guide for Cisco Unified Customer Voice Portal*—a new manual that describes how to isolate and solve problems in the Unified CVP solution.

Important Notes

The following sections contain important restrictions and requirements that apply to Unified Customer Voice Portal Release 4.0(1).

- OPSConsole Password Cannot Contain “Admin”, page 12

HTTP Server Must Be Running

In order for Unified CVP to operate correctly, the HTTP Server must be running.

Calls Not Working for Locations-based CAC with SIP Branch-office Model

Unified CVP SIP calls from branch-office locations, that are transferred to CallManager nodes at a data center (“hub”), do not undergo pass or reject validation according to bandwidth consumption computation for locations.

In the branch-office model, a call is sent from the Ingress Gateway at the branch into the Unified CVP at the hub. Unified CVP transfers the call to the Unified CallManager that is also at the hub. The SIP trunk for Unified CVP gets all the calls, as it is B2BUA. Therefore the source IP of a call appears as if from the hub instead of from a branch, so locations-based Call Admissions Control (CAC) does not work.

Long Failover Delay with SIP Calls Using TCP and Cisco Unified Presence Server’s Proxy Server

When TCP transport is being used, a SIP Call (INVITE message) sent via the SIP Proxy Server rings for some minutes, then times out. After approximately three (3) minutes, a new call is able to succeed. Every call encounters this long delay before failing over to a second priority destination (next hop).

TCP Transport is used on the static routes defined in Cisco Unified Presence Server. Two static routes are defined with the same DN pattern with priority 1 and priority 2. If a priority 1 destination, such as a VXML Gateway, is disconnected from the network, a long delay is encountered before a priority 2 destination is tried. For subsequent calls, the same delay occurs. There is no memory of the fact that the priority 1 destination is unavailable.

It is highly recommended that you use UDP instead of TCP for SIP signaling.

For the latest information on this problem, access CSCsg01564 through Bug Toolkit.

Restrictions on Importing a Database from One Operations Console to Another

Each Operations Console is identified by a unique identifier. The identifier is generated at the time of creating a first device through that Operations Console. Once generated, the identifier is then stored in the Operations Console database, and also in the Resource Manager Configuration file in every device that includes the Operations Console. The purpose of this unique identifier is to prevent multiple Operations Consoles from configuring the same device.

As a consequence, importing a database that was exported from another Operations Console is not supported if the other Operations Console was used at least once to manage one or more devices

For example, two effects of importing a database to an Operations Console that is managing at least one device—if the database to be imported is an exported database from a different Operations Console, or is an empty database which was never used to create a device—are:

- You may not be able to manage devices that were managed by the same Operations Console server prior to the import.

- You may not be able to create IOS devices—such as Gatekeepers, Gateways, and CSSs—from the Operations Console.

So, never import an empty database to an Operations Console, if the Operations Console is managing at least one device prior to import.

If you must replace the existing database with an empty database, reinstall the Operations Console software. Note, however, that if you do so, you can no longer manage devices that were previously managed by that Operations Console.

Microsoft Windows Hotfixes and /3GB Switch Required for Medium and Larger Reporting Servers

The following Windows 2003 hotfixes must be downloaded from Microsoft and installed on medium or larger Reporting Servers before installing Unified CVP, otherwise the installation will fail:

- 912570 Programs that require lots of memory may not run after you install Windows Server 2003 Service Pack 1
- 913409 A program that allocates a large block of contiguous memory may not start or may intermittently fail in Windows Server 2003
- 873453 The base memory address setting of the Samlib.dll file in Windows Server 2003 may interfere with programs that require a large shared memory setting

The installer sets the Microsoft /3GB switch.

Note Do not apply the hotfixes and /3GB switch to a small (laboratory) database.

Never Manipulate Reporting Database Backup File During Backup

Users should never access or manipulate the database backup file (cvp_backup_data). Users should never manipulate the old database backup file (cvp_backup_data.old) — for example, by performing a copy, rename or delete—just before or just after an Informix backup operation starts. In other words, an operating-system-level file operation and an Infomix backup operation should not happen at the same time. Otherwise, it might cause the Informix operation to enter an undesirable state, such as an infinite loop.

Remainder Fragment and Reporting Database Purge

In normal operations, there is always a managed fragment to accept data into the database. In the event that such a fragment does not exist, data will be accepted by the database and placed into the remainder fragment. At that point the data is lost in terms of purge manageability and cannot be managed easily as there is no label on the remainder fragment indicating what is in it.

If this case arises, an SNMP alert message is sent, indicating that data has been found in the remainder fragment and that the user must either execute a "manual" process to correct the condition or leave it as is.

The "manual" process is a stored procedure that currently performs the cleanup. The issue with this stored procedure is that it requires a large amount of logical logs and takes a variable amount of time to complete.

To run this cleanup procedure, you must:

1. Make sure that purge and backup are not running or scheduled to run in the next few hours.
2. Shut down the Call Server Service on the Reporting Server.
3. Notify users not to run reports.
4. Run the cleanup procedure.
   a. Open a command prompt and run dbaccess
   b. Start a connection as user cvp_dbuser (providing the correct password)
   c. Connect to the cvp_data database
   d. Run the following query "Execute procedure sp_remainder('X')" as a new query
5. Once the query finishes, restart the Call Server Service on the Reporting Server.
6. Turn applications back on.

Note After the cleanup procedure has been run, only one fragment per table is created, and all the days of data are put into it. The date associated with each fragment is that of the most recent data contained in the fragment.

If you do not execute the cleanup process within the retention period, the remainder fragment will be dropped and re-added. This clears up the problem, but at the cost of losing possibly recent data. (The issue is that if more than one day of data ends up in the remainder fragment, all data is lost when the fragment is dropped.)

Note The remainder fragment issue *must* be resolved within 14 days to avoid a drastic recovery process. If more than 14 days worth of data gets into the remainder fragment, the data will not be manageable through fragment management and will have to be manually corrected.

When the purge process is run, it checks for data in the remainder fragment. The first time it sees this condition, it logs a date stamp for the remainder. When that date stamp becomes older than the retention period, and if the condition has not been resolved, the purge process will get rid of the data.

However, if the purge process is never run, it will never place that date stamp. Similarly, if the retention period is longer than 14 days, the purge process will not get rid of the data within the required time.

For the latest information on this subject, access CSCsh55434 through Bug Toolkit.

Cisco Security Agent and Reporting Server

If you plan to install the standalone Cisco Security Agent on a Reporting Server, you must also install an additional patch. Please see the installation procedure in the *Cisco Security Agent Installation/Deployment Guide for Cisco Unified Customer Voice Portal* for details.

Support Tools and IOS Log Collection

For IOS log collection:

- the IOS log buffer should not exceed 10 MB (IOS command: logging buf 9999999)

- not more then 4 log files should be collected concurrently

TTS Error during Blind Transfer also Returns Semantic Error

When a VoiceXML Server performs a blind transfer, and a TTS error occurs during the blind transfer, multiple semantic errors are also returned.

The reason behind this is that Unified CVP 4.0 gateway treats a blind transfer as a consultation transfer, and therefore monitors the outcome after the call transfer is attempted.

To stop these semantic errors from occurring, in the application where a blind transfer is configured, add a Hotevent element with "Event" set to "error.com.cisco.media.resource.failure.tts" and the "Has Exit State" field checked. Then follow this Hotevent element with a Hang Up.

Deploying VoiceXML Application on AIX VoiceXML Server

When a VoiceXML application, created in VoiceXML Studio, is transferred to an AIX VoiceXML Server by means of the Operations Console, the application loses its file permissions. The application can be run; however, some administration functions will not function properly.

To allow the administration scripts to be executed, you must log into the AIX VoiceXML Server and issue the following command:

```
chmod +x <CVP_HOME>/VXMLServer/applications/<APP_NAME>/admin/*.sh
```

replacing <CVP_HOME> with your installation path and <APP_NAME> with your application name.

For the latest information on this problem, access CSCsf99414 through Bug Toolkit.

Writing of Server Messages Following Forced Shutdown

When the next upstream component is unavailable, VoiceXML Server and Call Server buffer messages in memory and write these messages to a .ser file. If a server is shutdown administratively, all messages may not get written to the .ser file during shutdown and reporting information on calls may be lost. Although the internal threads attempt to write all these messages to the .ser file, the SC.exe or the windows service does not allow more than one minute for the Tomcat service to run following a shutdown. All threads running in the context of Tomcat are interrupted, and therefore all messages do not get written. In particular, this can happen when the message buffer is storing information at or near its full capacity (100K messages for VoiceXML Server and 200K messages for Call Server).

The following workarounds are available to circumvent this problem:

- Connect VoiceXML Servers to a backup Call Server. This will eliminate the need to maintain a backlog of messages.
- Whenever possible, perform a graceful shutdown of the Call Server rather than a forced shutdown. This will enable the system to write all messages to the .ser file before exiting the process.

For the latest information on this problem, access CSCsh23259 through Bug Toolkit.

Picnix Utilities Copyright Information

The following third-party copyright information is missing from the Unified CVP Installer Copyright screen:

```
Picnix utilities
Copyright (c) 2001-2006 Peter Stephen Heitman. All rights reserved.
```

The following third-party copyright information is missing from the Unified CVP Installer License Agreement screen:

```
Picnix utilities
Copyright (c) 2001-2006 Peter Stephen Heitman. All rights reserved

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

Neither the name of Peter Stephen Heitman nor the names of his contributors may be
used to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

Close and Unlock all CVP Related Files Before Installing or Uninstalling

Before you attempt to install or uninstall Unified CVP Release 4.0(1) or any of its associated Service Releases or Maintenance Releases, make sure that all unnecessary applications are shut down and opened files are closed. If a file that the Unified CVP installation program requires is locked, a failed installation or uninstallation could result.

SNMP Support in CVP/ICM Co-resident Deployments

In deployments where the Unified CVP Call Server is co-resident with the VRU Peripheral Gateway (PG), SNMP functionality will work only if the installed ICM Release is Release 7.1(1) or later. This restriction does *not* apply in standalone CVP deployments.

Support Tools Trace Setting Defaults Not Restored

When you check the Restore Trace Setting Defaults checkbox in Support Tools, the VoiceXML Log Level and Trace Mask settings are not restored to the initial defaults. The initial defaults for these settings are the following:

```
VXML.logLevel = NOTICE
VXML.traceMask = 0x00000001
```

but the checkbox restores these settings as follows:

```
VXML.logLevel = INFO
VXML.traceMask = 0x0
```

No workaround for this problem is available at this time; you must manually restore the default settings.

For the latest information on this problem, access CSCsh35526 through Bug Toolkit.

Security Dialog Window During Release 4.0(1) SR1 Installation

During the installation process for Unified CVP Release 4.0(1) Service Release 1, if the installer detects the presence of VoiceXML Server for WebSphere Application Server, and administrative security is enabled in WebSphere Application Server, the installer prompts the user to supply a username and password. If you encounter this dialog window, enter your WebSphere username and password.

Avoid Full Fixed Disk Virus Scans on VoiceXML Server Machines Under Load

If the supported third party virus scan software is required on the VoiceXML Server machine, and a full fixed disk virus scan runs during a period of high call volume, the system resources that the virus scan software requires can impact the performance of the VoiceXML Server, particularly the loggers and the logging mechanism. When this occurs, the following messages may been seen in the system logs:

- "DatafeedMgr saves event into queue..." message listed in the CVP VXML log
- "IllegalStateException" message listed in the application error log
- "OutOfMemory" error message listed in the Tomcat log

Although virus scan software can be enabled on the VoiceXML Server, full fixed disk virus scans should take place either offline while calls have been diverted to a different system (preferred), or during a period of low call volume.

For the latest information on this problem, access CSCsh12470 through Bug Toolkit.

Notes About VoiceXML Server Audio Files

The following audio files are included in the VoiceXML Server web application by default.

- error.wav
- helloworld_audio.wav
- onhold_continue.wav
- onhold_initial.wav
- suspend_audio.wav

- suspended_audio.wav

These files are included in both initial deployments and in service and maintenance releases of VoiceXML Server.

For Tomcat installations, the audio directory is located at:

```
%CVP_HOME%\VXMLServer\Tomcat\webapps\CVP\audio\
```

For WebSphere Application installations, the audio directory is located at:

```
%WAS_HOME%\profiles\<application server name>\installedApps\<app node>\CVP VXML
server.ear\CVP.war\audio\
```

Back Up VoiceXML Server Custom Audio Files Before Installing Service or Maintenance Release

VoiceXML Server saves custom audio files in the VXMLServer\Tomcat\webapps\CVP\audio directory. When installation of a service release or maintenance release of Cisco Unified CVP includes updating of the Apache Tomcat deployments, the previous Tomcat deployment of VoiceXML Server, including any custom audio files in this directory, is completely removed. If you wish to continue using the custom audio files from the previous deployment, you must back up the files in this directory prior to installing or uninstalling the service or maintenance release.

For more information, access CSCsh49616 through Bug Toolkit.

OPSConsole Password Cannot Contain "Admin"

In addition to the criteria listed on the OPSConsole Password screen in the Unified CVP Install program, the OPSConsole password cannot contain the word "admin". If you specify a password that contains "admin" the install program does not set any password, even though the install program does not notify the user that such a password is not permitted.

For more information, access CSCsh53925 through Bug Toolkit.

Resolved Caveats in This Release

The latest resolved caveat information can be accessed through Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tips You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log onto
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser

- Cisco.com user ID and password

Procedure

Tips To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Step 1 Log on with your Cisco.com user ID and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for Cisco Unified CVP, go to the "Search for bugs in other Cisco software and hardware products" section, and enter **Cisco Unified Customer Voice Portal** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco Unified Customer Voice Portal**.

Step 4 Click **Next**. The Cisco Unified Customer Voice Portal search window displays.

Step 5 Choose the filters to query for caveats. You can choose any or all of the available options:

a. Select the Cisco Unified Customer Voice Portal Version:

- Choose the major version for the major releases.

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information.

  A revision release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

b. Choose the Features or Components to query; make your selection from the "Available" list and click **Add** to place your selection in the "Limit search to" list.

To query for all caveats for a specified release, choose "All Features" in the left window pane.

Note The default value specifies "All Features" and includes all of the items in the left window pane.

c. Enter keywords to search for a caveat title and description, if desired.

Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

d. Choose the Set Advanced Options, including the following items:

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the Fixed check box for resolved caveats.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

e. Click **Next**.

Step 6 Bug Toolkit returns the list of caveats on the basis of your query. You can modify your results by submitting another query and using different criteria.

Open Caveats in This Release

This section contains a list of defects that are currently pending in Cisco Unified Customer Voice Portal 4.0(1). Defects are listed by component and then by identifier.

Tips If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than is reflected in this document. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Table 1 Open Caveats for Cisco Unified Customer Voice Portal 4.0(1)

Identifier	Component	Headline
CSCsh33808	appsvr	Stopping CVP while calls already established drops calls
CSCsg89446	cp-sip	Locations Based CAC with branch model CVP calls not working.
CSCsg01564	esp	SIP system takes 3 min to recover from primary vxml gw going down
CSCsg51887	infrastructure	ICM SS goes into Partical Service and never moves to In Service
CSCsh23259	infrastructure	RPT: VXML Failover - all records from SER do not arrive at the DB
CSCsg96946	install	WAS Install: If WAS_HOME is not defined, warning message not enforced
CSCsh05670	install	WAS Install: no check for incorrect http admin password
CSCsh13925	install	CVP reporting install screen does not update/repaint
CSCsf96998	oamp	SRV records cannot be configured as SIP Proxy Server
CSCsf99414	oamp	After deploying an App on AIX, the admin scripts are not executable
CSCsg26246	oamp	Using Back button of browser should be warned and disabled
CSCsg99527	oamp	OAMP: Failed Transfer Files apper in the Available File List
CSCsh23831	oamp	OAMP: jmx security with aix orm
CSCsh28244	oamp	OMAP does not update Available script list with newest version.
CSCsh39913	oamp	Call Server SIP: Need warning to user to select Outbound Proxy Host
CSCsh53925	oamp	OAMP password will fail if contains 'admin' word in it
CSCsh49616	patch	Installing or Uninstalling SR results in deletion of Custom Audio files
CSCsg19173	reporting	SNMP Alert, At least 48 hours since last purge
CSCsh14662	reporting	Rpt: Returned success for Rpt backup when it should have failed
CSCsh16802	reporting	RPT: There is no SNMP Alert if backup fails due to lack of space
CSCsh28242	reporting	RPT: Unable to Insert Data into Tables after Restart (code -710)
CSCsh34517	reporting	RPT: Alerts needed when attempts to connect to the database fails
CSCsh36961	reporting	No State_Change Message on Rpt Srvr when Rpt Server goes to Partial Srvc
CSCsh43002	reporting	RPT: DB state should be validated before performing other operations
CSCsh55434	reporting	Unable to Manually Fix Remainders if there is more than 14 days of Data
CSCse65226	ss_ivr	microapp PM, vxml ignores network VRU script timeout value
CSCsg91737	ss_ivr	Microapp GS, Boolean bargein D does not work, but digits collected.

Table 1 Open Caveats for Cisco Unified Customer Voice Portal 4.0(1)

Identifier	Component	Headline
CSCsh26374	ss_vxml	AIX VXML Server performance issues can not handle supported load
CSCsh35526	ss_vxml	VXML trace settings not set back to correct default value

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security

Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.
If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the magazine for Cisco networking professionals. Each quarter, *Packet* delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *Packet* magazine at this URL:

  http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html