Release Notes for Cisco Unified Customer Voice Portal (CVP) Release 4.0(2)

June 22, 2007

Contents

- Introduction, page 1
- System Requirements, page 3
- New and Changed Information, page 3
- Unified CVP Maintenance Release Installation Planning, page 11
- Installation Notes, page 11
- Important Notes, page 15
- Resolved Caveats in This Release, page 17
- Open Caveats in This Release, page 19
- Obtaining Documentation, page 20
- Documentation Feedback, page 21
- Field Alerts and Field Notices, page 21
- Cisco Product Security Overview, page 21
- Obtaining Technical Assistance, page 22
- Obtaining Additional Publications and Information, page 24

Introduction

This document discusses new features, changes, and caveats for Maintenance Release 4.0(2) of Cisco Unified Customer Voice Portal (CVP) software.

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

This document is a supplement to the Release Notes for Cisco Unified Customer Voice Portal (CVP) Release 4.0(1) and Release 4.0(1) Service Release 1, which is available at:
http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_release_notes_list.html

The Release Notes for Cisco Unified Customer Voice Portal (CVP) Release 4.0(2) **must** be used in conjunction with the just mentioned Release Notes. The latest version of this release can be found at:

http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=cc

Step 1 Click **Cisco Unified Contact Center Products**

Step 2 Click **Cisco Unified Customer Voice Portal**

Step 3 Click **Cisco Customer Voice Portal Software Releases**

Step 4 Select the release you want then click the link to the desired release notes.

About Release 4.0(2)

Maintenance Releases are cumulative updates to previous releases. As a result, applying Release 4.0(2) installs all the functionality contained in Unified CVP 4.0(1) SR1, as well as the new 4.0(2) content. Due to this, ensure you read the relevant Release Notes prior to installing Release 4.0(2).

Release 4.0(2) can be installed as follows:

- an existing installation of Unified CVP 4.0 would already have Unified CVP 4.0(1) + Unified CVP 4.0(1) SR1 installed; Release 4.0(2) would be installed over this
- for a new installation of Unified CVP 4.0 that uses only Microsoft Windows, install Unified CVP 4.0(1) and then immediately install Release 4.0(2) over this—do not install Unified CVP 4.0(1) SR1, do not perform any configuration between the installation of Release 4.0(1) and Release 4.0(2)
- for a new installation of Unified CVP 4.0 that uses AIX, install Unified CVP 4.0(1), then immediately install Unified CVP 4.0(1) SR1, and then install Release 4.0(2) over this—do not perform any configuration between the installation of Release 4.0(1) and Release 4.0(1) SR1, configuration between the installation of Release 4.0(1) SR1 and Release 4.0(2) is allowed but optional

Unified CVP 4.0(2) also contains functionality delivered in Engineering Specials (ESs) built on Unified CVP 4.0(1), Unified CVP 4.0(1) SR1 at least 60 days prior to the release date of 4.0(2). If your system has an ES installed whose functionality is not contained in 4.0(2), the installer displays a warning prior to performing any modifications to the system. The pre-4.0(2) ES must be uninstalled before the installation of 4.0(2) can be restarted.

For more information, and to obtain a replacement ES to be installed, refer to the Cisco Bug Toolkit located at:
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

The maintenance release is available on CD and as downloadable installers from cisco.com.

A Note about Product Naming

Cisco Unified CallManager is being renamed to Cisco Unified Communications Manager.

These release notes use the previous naming convention.

System Requirements

For hardware and third-party software specifications for Maintenance Release 4.0(2), refer to the *Hardware and System Software Specification for Cisco Unified CVP, Releases 4.0(1), 4.0(1) SR1 and 4.0(2)*, which is accessible from http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html

Unified CVP Version Support

Unified CVP Maintenance Release 4.0(2) can only be installed on systems running Unified CVP 4.0(1) or Unified CVP 4.0(1) SR1.

Unified CVP Maintenance Release 4.0(2) has been tested and verified to be compatible with the interoperability criteria for Unified CVP Release 4.0(1). Additional Unified CVP Maintenance Release 4.0(2) interoperability support information is available from the *Hardware and System Software Specification for Cisco Unified CVP, Releases 4.0(1), 4.0(1) SR1and 4.0(2)*, which is accessible from: http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html

New and Changed Information

Unified CVP Release 4.0(2) is a maintenance release that contains fixes and a limited set of new functionality. Release 4.0(2) is incremental and cumulative, and can be rolled back.

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

Note Unified CVP 4.0(2) provides support for HTTPS and the new VXML adapters only if used with IOS 12.4(15)T or later.

- HTTPS Support, page 3
- VXML Gateway Configuration Changes for HTTPS, page 8
- New Property to Control VXML Generation of URLs, page 9
- VXML 2.1 Adapters for VoiceXML Studio and Server, page 10
- Support Large Database Size (100GB) for Reporting Server, page 10
- Cisco Security Agent (CSA) 5.2, page 10
- Equivalent UNIX Commands Support on Unified CVP Servers, page 11

HTTPS Support

Along with the release of IOS version 12.4(15)T, Unified CVP 4.0(2) can be configured to use HTTPS on the VoiceXML Server, and on the IVR leg of the Call Server. Only signed server certificates can be applied to the IOS gateway; self-signed certificates are not accepted. Unified CVP 4.0(2) will generate self-signed certificates for Tomcat applications. These certificates must be signed by a Certificate Authority prior to use. Tomcat VoiceXML Server users and Call Server users must follow these steps to have the certificate signed. Please refer to the 12.4(15)T IOS documentation for instructions on how to apply the certificates to the VXML gateway.

Tomcat users follow the steps below to present a CA-signed certificate to inbound HTTPS clients

Due to the large processing overhead of HTTPS, the Tomcat application server can only achieve up to 100 simultaneous connections dependent on the configuration (see the *Cisco Unified Customer Voice Portal (CVP) Release 4.0 Solution Reference Network Design (SRND)* document for further details). For better performance from the VXML Server with HTTPS it is recommended that WebSphere be used as the application server.

VXML Server with WebSphere in a Standalone model (Reporting and Datafeed disabled) can support up to 275 calls.

VXML Server with WebSphere in a Standalone model (Reporting and Datafeed enabled) can support up to 200 calls.

Comprehensive deployment using Call Server and VXML Server with Tomcat can support up to 100 calls.

For higher performance in a Comprehensive model, it is recommended that VXML Server with WebSphere be used in conjunction with Call Server. Up to 250 calls can be run in the above combination when most of the VXML processing is being handled by the VXML Server running with WebSphere.

The certificate and private key used for HTTPS are:
Self-signed certificate: %CVP_HOME%\conf\security\xxxx.crt

Private key for self-signed certificate: %CVP_HOME%\conf\security\xxxx.key

where xxxx represents the key and the certificate files. Call Server key and certificate files will be named callserver.key and callserver.crt. VXML Server key and certificate files will be named vxml.key and vxml.crt.

Step 1 Access the OpenSSL command line:

Note You must first install OpenSSL (http://www.openssl.org), as it is not included with Unified CVP. Refer to the OpenSSL documentation for details.

Step 2 Generate a Certificate Signing Request (CSR) by entering the following command:

```
openssl req -new -key xxxx.key -out xxxx.csr
```

Step 3 Send the xxxx.csr certificate file to a Certificate Authority (CA) for sign-off. Once the certificate is signed, it will be returned with a root certificate of a CA.

Step 4 Replace the original xxxx.crt file with the signed certificate.

Step 5 Restart the CVP server to apply the new signed certificate.

WebSphere users follow the steps below to present a CA-signed certificate to inbound HTTPS clients

Step 1 Run IBM's ikeyman utility to create a keystore

C:\Program Files\IBM\HTTPServer\bin\ikeyman.bat

Create a new Key database file:

Key Database File -> new

Database type: CMS

Filename: key.kdb

Location: C:\Program Files\IBM\HTTPServer\keys

Notes:

a) "keys" directory will have to be explicitly created if it does not exist

b) keystore will prompt for password and expiration information

c) Check off - create a Stash file

Step 2 Create a new Certificate Request in ikeyman

Create->New Certificate Request

Key Label: <hostname>

Version: V509 v3

Key Size: 1024

Common Name: <hostname>

Organization: <Company Name>

Organization Unit: <Group Name>

Locality: <Town>

State: <State>

Zip Code: <Zip Code>

Country: <Country>

Validity Period: 730 days

This saves a file certreq.arm.

Present this certificate request to a Certificate Authority for sign-off. Once the certificate is signed, it will be returned with the root certificate of a CA.

Step 3 Import the CA root certificate into the Key Database.

If the CA is not listed in the Key Database Content->Signer Certificates, then the root certificate of the CA must be imported into this list for the signed certificate to be installed into the database. Click Add, and provide the path of the DER certificate file of the Root CA certificate.

Step 4 Import the signed certificate into the key database.

Save the signed certificate from the CA as a DER file format and locate it on the machine in which you will install it into the key database. Then import the signed certificate into the database with the ikeyman utility. Key Database Content -> Personal Certificates, click Receive. Provide the path of the signed certificate from the CA.

Setup SSL as follows:

1. Set IHS_HOME=<location of IBM HTTPServer> (e.g. set IHS_HOME=C:\Program Files\IBM\HTTPServer)
2. Modify the %IHS_HOME%\conf\httpd.conf file as follows:

Current configuration for HTTP/port 7000:

```
##
## To enable AFPA on supported Windows Operating Systems delete the "#" symbol in
## front of the "LoadModule ibm_afpa_module modules/mod_afpa_cache.so" directive
```

```
##
LoadModule ibm_afpa_module modules/mod_afpa_cache.so
<IfModule mod_afpa_cache.c>
  AfpaEnable
  AfpaCache on
  AfpaPort 7000
  AfpaLogFile "C:/Program Files/IBM/HTTPServer/logs/afpalog"
</IfModule>

##
## Configuration with AFPA disabled
##
<IfModule !mod_afpa_cache.c>
Listen 0.0.0.0:7000
```

Should be commented out and changed to HTTPS/port 7443:

```
##
#LoadModule ibm_afpa_module modules/mod_afpa_cache.so
#<IfModule mod_afpa_cache.c>
#  AfpaEnable
#  AfpaCache on
#  AfpaPort 7000
#  AfpaLogFile "C:/Program Files/IBM/HTTPServer/logs/afpalog"
#</IfModule>

##
## Configuration with AFPA disabled
##
#<IfModule !mod_afpa_cache.c>
#  Listen 0.0.0.0:7000

# Use Win32DisableAcceptEx to downgrade to use winsock 1.1 network APIs.
# Note: You can use Win32DisableAcceptEx only if mod_afpa_cache.so is disabled.
# Win32DisableAcceptEx
#</IfModule>


LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:7443
<VirtualHost 0.0.0.0:7443>
     SSLEnable
     SSLClientAuth none
      KeyFile "c:\Program Files\IBM\HTTPServer\keys\key.kdb"
      SSLStashfile "c:\Program Files\IBM\HTTPServer\keys\key.sth"
      ErrorLog "c:\Program Files\IBM\HTTPServer\logs\sslerror.log"
      TransferLog "c:\Program Files\IBM\HTTPServer\logs\sslaccess.log"
</VirtualHost>
SSLDisable
```

3. Open up the WebSphere Integrated Solutions Console (http://localhost:9080/ibm/console) and log in if necessary.
4. Using the WebSphere Integrated Solutions Console, navigate to Servers > Web servers. Delete "webserver1" by selecting and hitting <Delete> button. (Be sure to <Save> the configuration when prompted.)
5. Using the WebSphere Integrated Solutions Console, navigate to Environment > Virtual Hosts. Add the port mapping: Hostname = *; Port = 7443 (Be sure to <Save> the configuration when prompted.)

6. Log out of the WebSphere Integrated Solutions Console.
7. Copy %CVP_HOME%\bin\DefineWebContainer.bat to %CVP_HOME%\bin\DefineWebContainerHTTPS.bat
8. Edit %CVP_HOME%\bin\DefineWebContainerHTTPS.bat as follows:

Current HTTP port definition:

```
set PORT=7000
```

Change to new HTTPS port definition:

```
set PORT=7443
```

9. Open up the WebSphere Integrated Solutions Console (http://localhost:9080/ibm/console) and log in if necessary.
10. Using the WebSphere Integrated Solutions Console, navigate to Servers > Web servers.
    a) Click on "webserver1".
    b) Then click on the "Plugin properties" link.
    c) Hit the "Copy to Web server key store directory" button and then the <OK> button.
    d) <Save> the configuration when complete
11. Reboot the machine
12. After the machine restarts, try to load the standard HTTPServer HTTPS web page (e.g. https://localhost:7443/)
13. Try to load the CVP Licensing web page using HTTPS (e.g. https://localhost:7443/CVP/Licensing)

Securing Communications Between Unified CVP and IOS Devices

To secure file transfer between Cisco Gateways and/or Gatekeepers and the Unified CVP Operations Console, you need to import the Operations Console Server certificate on the IOS device during device configuration.

How to Export the Operations Console Certificate to a File

Step 1 From the web browser, access the secure Call Server with [https://<ServerIP>:8443/] or the secure VXML Server with [https://<ServerIP>:7443/]

The Security Alert dialog box appears.

Step 2 Click View Certificate.

The Certificate dialog box appears.

Step 3 Select the Details tab.

<All> will be highlighted in the Show drop-down list.

Step 4 Click Copy to File.

The Certificate Export Wizard dialog appears.

Step 5 Select the Base-64 encoded X.509 (.CER) radio button and click Next.

Step 6 Specify a file name in the File to Export dialog and click Next.

Step 7 Click Finish.

An Export was Successful message appears.

Step 8 Click OK and close the Security Alert dialog.

Step 9 Open the exported file in Notepad and copy the text that appears between the ---BEGIN CERTIFICATE-- and --END CERTIFICATE-- tags.

You are now ready to copy the Operations Console certificate information to the IOS device.

How to Import the Operations Console Certificate to a Gatekeeper or Gateway

Step 1 Access the IOS device in privileged EXEC mode.

Note: For more information, see the Cisco IOS Command-Line Interface documentation.

Step 2 Access global configuration mode by entering:

configuration terminal

Step 3 Create and enroll a trustpoint by entering the following commands:

```
crypto pki trustpoint xxxx
en terminal
exit
```

Where xxxx is a trustpoint name.

The IOS device exits conf t mode and returns to privileged EXEC mode.

Step 4 Do the following to copy the certificate exported to the Notepad to the IOS device:

1. Enter crypto pki auth xxxx

Where xxxx is the trustpoint name specified in the previous step.

2. Paste the certificate from the Notepad clipboard.

3. Enter quit.

The following happens:

- A message displays describing the certificate attributes.
- A confirmation prompt appears.

Step 5 Enter yes.

A message reports that the certificate was successfully imported.

VXML Gateway Configuration Changes for HTTPS

VoiceXML Standalone Applications

For standalone VoiceXML Server applications, the VXML gateway application must be configured as follows in order to utilize HTTPS communications with the VoiceXML Server.

```
application service Secure flash:CVPSelfService.tcl
paramspace english index 0
paramspace english language en
```

```
paramspace english location flash
param CVPSelfService-app WeatherApp
param CVPPrimaryVXMLServer 192.168.150.114
param CVPSelfService-port 7443
param CVPSelfService-SSL 1
```

The new CVPSelfService-SSL parameter added to the application declares that connectivity to the VoiceXML Server is done via HTTPS. A value of 1 enables HTTPS. A value of 0, or having the variable undeclared, will keep the connections at HTTP.

Comprehensive Call Flow Applications

For Comprehensive call flow, the bootstrap application will be configured as follows in order to utilize HTTPS communications with the Call Server IVR Service.

```
service bootstrap flash:bootstrap.tcl
paramspace english language en
paramspace english index 0
paramspace english location flash
param cvpserverssl 1
paramspace english prefix en
```

The new VXML gateway application variable declares that connectivity with the Call Server will happen via HTTPS. A value of 1 enables HTTPS. A value of 0, or having the variable undefined, will default to HTTP connectivity.

New Property to Control VXML Generation of URLs

The VXML that the IVR Service returns as a response to an HTTP/HTTPS request from the VXML gateway contains URLs to media servers so that the gateway knows where to fetch the media files from.

In CVP 4.0(2), the URLs to the media servers in the VXML returned by the IVR Service can be controlled so that they are either HTTP or HTTPS URLs. This new property is a boolean property called "Use Security For Media Fetches". By default, it is set to "false". A value of "true" means to generate HTTPS URLs to media servers and a value of "false" means to generate HTTP URLs to media servers. However, this property is only applicable if both of the following conditions are true:

- The client is not the H.323 Service (i.e. CVP Voice Browser). This is because the H.323 Service does not support HTTPS.
- In the ICM script, the media server (specified in ECC variable "call.user.microapp.media_server") is not set to a URL that explicitly specifies an HTTP or HTTPS scheme. An example of a URL that explicitly specifies an HTTP scheme is "http://<servername>". One that specifies an HTTPS scheme is "https://<servername>". An example of a URL that does not specifies the scheme is "<servername>". In the Operations Console, the user visible text for this property is "Use Security For Media Fetches". The Call Server does not have to be re-started for this property to take effect.

VXML 2.1 Adapters for VoiceXML Studio and Server

In addition to the existing gateway adapters, four new gateway adapters will be added to both VoiceXML Server and VoiceXML Studio by the 4.0(2) patch installation. The new gateway adapters are:

"Cisco Unified CVP 4.0 VoiceXML 2.1 with Cisco DTMF"

"Cisco Unified CVP 4.0 VoiceXML 2.1 with Nuance 8.5"

"Cisco Unified CVP 4.0 VoiceXML 2.1 with OSR 3"

"Cisco Unified CVP 4.0 VoiceXML 2.1 with IBM WebSphere Voice Server 5.1"

These gateway adapters provide support for VoiceXML 2.1 features added in the 12.4(15)T IOS Gateway image.

Support Large Database Size (100GB) for Reporting Server

Unified CVP 4.0(1) base installer shipped without displaying the large database option (by default it only displays the small and medium database options). Unified CVP release 4.0(2) provides an option to select a large database size during Reporting Server install. A batch file called 'AllowCVP2SupportLargeDb.bat' is provided which will enable the large database option in the Unified CVP 4.0(1) base installer. It is available on cisco.com. Please note that this batch file **MUST** be run prior to installation of CVP 4.0(1) base installer. Open a command window on the Reporting Server machine, and perform the follows tasks:

1) Copy the batch file to a well known location on the machine (e.g. C:\).

2) Double click the batch file to run it.

Note To select the large database size option, the Reporting Server must be a Cisco MCS 7845-H2 or MCS 784-I2 machine (2 Intel Xeon Dual-core 2.33+ GHz CPU, 8+GB PC2-5300 667 MHz DDR2 RAM and two 72 GB SAS disks (RAID 10) for C:\ drive and six 146GB SAS disks (RAID 10) for E:\ drive)

Cisco Security Agent (CSA) 5.2

In Unified CVP 4.0(2), a newer standalone version of CSA for Unified CVP, based on CSA engine version 5.2, is available. This means that the CSA agent kits and policies that worked with Unified CVP 4.0(1) will **NOT** work with Unified CVP 4.0(2). Hence, you must uninstall CSA 4.5 prior to upgrading to Unified CVP 4.0(2). New CSA agent kits and policies are available for download on cisco.com.

For information on uninstalling and installing CSA, see the *Cisco Security Agent Installation/Deployment Guide for Cisco Unified Customer Voice Portal*.

Equivalent UNIX Commands Support on Unified CVP Servers

Users can now execute the some UNIX equivalent command, such as more, grep, diff, tail, tee on Unified CVP 4.0(2) servers during troubleshooting. These commands are part of Support Tools installation and for Unified CVP 4.0(2), the PATH environment variable is updated to allow these commands to be accessible via command line.

Unified CVP Maintenance Release Installation Planning

This section provides information to help you understand when to install a Unified CVP maintenance release and the tasks it involves. It contains the following subsections:

- When to Install a Unified CVP Maintenance Release, page 11
- Installation Order for Unified CVP Components, page 11
- Unified CVP Maintenance Release Installation Checklist, page 11

When to Install a Unified CVP Maintenance Release

Installing a Unified CVP maintenance release requires temporarily stopping all Unified CVP services and processes on your Unified CVP components. Therefore, to limit impact to a live Unified CVP system, schedule and install Unified CVP maintenance releases during a maintenance period when your Unified CVP system is out of production.

Installation Order for Unified CVP Components

Unified CVP maintenance releases do not need to be installed on Unified CVP components in a specific order.

Unified CVP Maintenance Release Installation Checklist

Deploying a Unified CVP Maintenance Release requires the following general tasks:

- Schedule a maintenance period for installation: Because Unified CVP maintenance release installation requires bringing down a Unified CVP system, schedule maintenance release installation for a maintenance period when your Unified CVP system is out of production.
- Test and troubleshoot the installation: After installation, test your Unified CVP system to ensure that it is working properly.

Installation Notes

- Close and Unlock All Unified CVP Related Files Before Installing, page 12
- Cisco Unified CVP VoiceXML Server and IBM WebSphere Application Server, page 12
- Backup VoiceXML Server Custom Audio Files, page 12
- Installation Requirements, page 12

- Windows Installation Steps, page 13
- IBM WebSphere Application Server Redeployment Automation, page 13
- Informix Services Unable to Stop upon Certain Patch Installations and Uninstallations, page 13
- AIX Installation Steps, page 14
- AIX Uninstallation Steps, page 14

Close and Unlock All Unified CVP Related Files Before Installing

Before you attempt to install or uninstall Cisco Unified CVP Release 4.0(2) Maintenance Release, 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.

Cisco Unified CVP VoiceXML Server and IBM WebSphere Application Server

During the installation or uninstallation process for Unified CVP Release 4.0(2) Maintenance Release, if the installer detects the presence of VoiceXML Server for IBM WebSphere Application Server it may prompt the user to supply a username and password. If you encounter this dialog window, enter your WebSphere Application Server administrative username and password.

Backup VoiceXML Server Custom Audio Files

VoiceXML Server saves custom audio files in the web deployment directory of either Apache Tomcat or IBM WebSphere Application Server. When installation or uninstallation of the Unified CVP 4.0(2) Maintenance Release of Cisco Unified CVP includes updating of the VoiceXML Server component, the previous deployment of VoiceXML Server, including any custom audio files in this directory, is completely removed. The Unified CVP 4.0(2) patch installer will attempt to automatically backup your custom audio files in a temporary directory and restore the custom audio files upon redeployment of the updated VoiceXML Server. As an additional backup precaution, if you wish to continue using the custom audio files from the previous deployment, you must back up the files manually in a temporary directory prior to installing or uninstalling the service release. These files may be restored back to their deployment location:

Deployment directory examples:

Tomcat deployments - %CVP_HOME%\VXMLServer\Tomcat\webapps\CVP\audio

WebSphere deployments - %WAS_HOME%\profiles\AppSrv01\installedApps\serverCell\CVP VXML server.ear\CVP.war\audio

Installation Requirements

Unified CVP 4.0(2) can be installed in the following ways:

- an existing installation of Unified CVP 4.0 would already have Unified CVP 4.0(1) + Unified CVP 4.0(1) SR1 installed; Release 4.0(2) would be installed over this
- for a new installation of Unified CVP 4.0 that uses only Microsoft Windows, install Unified CVP 4.0(1) and then immediately install Release 4.0(2) over this—do not install Unified CVP 4.0(1) SR1, do not perform any configuration between the installation of Release 4.0(1) and Release 4.0(2)

- for a new installation of Unified CVP 4.0 that uses AIX, install Unified CVP 4.0(1), then immediately install Unified CVP 4.0(1) SR1, and then install Release 4.0(2) over this—do not perform any configuration between the installation of Release 4.0(1) and Release 4.0(1) SR1, configuration between the installation of Release 4.0(1) SR1 and Release 4.0(2) is allowed but optional

Windows Installation Steps

1. Open and run the Windows Unified CVP 4.0(2) patch installer executable.
2. Follow the instructions within installer screens.
3. Restart your server upon successful completion of patch installation or uninstallation.

IBM WebSphere Application Server Redeployment Automation

Upon certain patch installations or uninstallations of Unified CVP VoiceXML Server deployments to IBM WebSphere Application Service (WAS), the patch automated redeployment process may hang, causing an unsuccessful redeployment of VoiceXML Server to WAS. Also, a patch installer error message will display stating that the WAS redeployment of VoiceXML Server has been unsuccessful. If this occurs, the system should be restarted or the WAS java process should be ended within the Windows Task Manager. After the restart, please view the Unified CVP installation log file and follow the manual WAS deployment steps as detailed in the log file. The log file location is shown in any error message windows that display during a patch installation or uninstallation.

Alternatively, here is an example of a sample Unified CVP path installation log location:

C:\Temp\Maintenance Release CVP4.0(2)\20070514_132933_Maintenance Release CVP4.0(2).log

Informix Services Unable to Stop upon Certain Patch Installations and Uninstallations

Upon Unified CVP patch installation or uninstallation, one or more Informix-related services may not stop as requested by the Unified CVP patch installer. This symptom has been found to occur when a patch installation or uninstallation is kicked off under heavy Informix load or processes. These services can include:

- ISM Local Execution (nsrexecd)
- ISM Portmapper (portmap)
- ISM Server (nsrd)

An administrator can workaround these issues by stopping Informix processes and services before running a patch installation or uninstallation:

In Windows, the end-user should perform the following steps:

Step 1 Start -> Settings -> Control Panel -> Administrative Tools -> Services

Step 2 All started Informix services should be stopped manually.

Step 3 Verify the Informix services are in a stopped/offline state.

Step 4 Run the Unified CVP patch installer.

Alternatively, these processes may be stopped/killed within the Windows Task Manager.

AIX Installation Steps

1. Run cvp402_aix.bin.
2. The patch includes a new CVP.war file that must be redeployed manually. To do so, you will use the WebSphere web admin (e.g. http://<server_ip_address>:9060/ibm/console/login.do)
   - Goto Applications -> Enterprise Applications
   - Select "CVP VXML server" and click on "Update"
   - In the "Preparing for the application installation" page, select "Replace the entire application"
   - Keep all parameters to their default values on Step 1, 2 and 3
   - Click "Finish" on step 4, "Save" the changes to the master configuration
   - Restart WebSphere

AIX Uninstallation Steps

Note In those rare cases where the Unified CVP 4.0(2) patch must be removed, care must be taken that most recent patch is removed first. For example, do not remove 4.0(1)SR1 if 4.0(2) is installed. You would have to remove the latest version first.

1. Find and delete the files that were new with the 4.0(2) patch.
   - Run the following command from root directory to locate those files: find ./ -name *new_for_cvp402
   - Use the "del" command to delete them.
2. Find and restore the files that were backup and updated by the 4.0(2) patch.
   - Run the following command from root directory: find ./ -name *cvp402
   - Rename and replace all of these backedup files to their original.
     cd /home/cvp/CVP/doc/
     mv copyrights.txt.cvp402 copyrights.txt
3. Repeat Step#2 from the install instructions to redeploy the original CVP.war file. That is:
   - Go into the WebSphere web admin (e.g. http://<server_ip>:9060/ibm/console/login.do)
   - Goto Applications -> Enterprise Applications
   - In the "Preparing for the application installation" page, select "Replace the entire application"
   - Select "CVP VXML server" and click on "Update"
   - Keep all parameters to their default values on Step 1, 2 and 3
   - Click "Finish" on step 4, "Save" the changes to the master configuration
   - Restart WebSphere

Important Notes

The following sections contain restrictions that apply to Release 4.0(2).

- Support for Nuance Recognizer 9, page 15
- Content Services Switches Not Supported with HTTPS, page 15
- Operations Console: Save&Deploy Slow to Complete, page 15
- AS5400 and AS5400HPX Do Not Support IP-to-IP Transfer, page 15
- Unable to Invoke Voice / DTMF grammar for Nuance SWMS, page 15
- user.microapp.locale, ICM Scripts, and Case Sensitivity, page 16

Support for Nuance Recognizer 9

Nuance Recognizer 9.0.0 has been qualified with Unified CVP 4.0(2), but this information is missing from the gateway adapter drop-down menu in Unified CVP 4.0 VoiceXML Studio.

Until the specific item is added to the drop-down menu, in order to use Nuance Recognizer 9, select **Cisco Unified CVP 4.0 VoiceXML 2.1 with OSR 3** from the list.

Content Services Switches Not Supported with HTTPS

Content Services Switches (CSSs) are not supported by Unified CVP 4.0(2) if the HTTPS feature is used.

Operations Console: Save&Deploy Slow to Complete

When performing a Save&Deploy on an existing device, the time to complete the operation can take 3-5 minutes.

The problem appears when several servers are Not Reachable because, although these servers were initially saved and deployed, they no longer exist. This causes a degradation in performance.

To improve performance, delete from the Operations Console devices that are physically not available.

AS5400 and AS5400HPX Do Not Support IP-to-IP Transfer

Gateways AS5400 and AS5400HPX do not support the IP Plus feature. Thus, with AS5400 and AS5400HPX, IP-to-IP transfer does not work. These restrict customers from using Unified CVP functionality when the gateway has to perform IP-to-IP transfer, as in VoiceXML transfer element for an IP originated call. The IP Plus feature is supported with AS5400XM only. So, if a customer has a scenario where the gateway has to perform IP-to-IP transfer, then AS5400XM is required.

Unable to Invoke Voice / DTMF grammar for Nuance SWMS

Observed the behavior that in some Nuance SWMS (formerly Scansoft) boxes, .grxml grammar files are not getting loaded.

The following errors show up in C:\Program Files\SpeechWorks\MediaServer\server\logContent\log.txt under default logging.

```
May 22 18:07:12.82|700|0||OSR Plugin|0||Grammar
<session:field122@field.grammar> is not found in grammar tree=|UCPU=0|SCPU=0

May 22 18:07:12.84|700|0||OSR Plugin|0||Could not load grammar=|UCPU=15|SCPU=0

May 22 18:07:12.84|700|0||OSR Plugin|0||Grammar
<http://10.77.60.173:7000/grammar/test_month_osr20_cisco.grxml> is not
loaded=|UCPU=15|SCPU=0

May 22 18:07:13.90|1164|0||OSR Plugin|0||Grammar
<session:link123@document.grammar> is not activated=|UCPU=0|SCPU=0
```

If this happens, Gateways, VoiceXML Server and Unified CVP Logs will also show up errors indicating resource issues or general failures in ASR/TTS.

The call will get connected but will disconnect and may receive error treatment.

To resolve the issue

1. Configure C:\Program Files\SpeechWorks\MediaServer\server\config\OSSServer.cfg

   Under the following section:

   ```
   ##############################################
   # File extension to MIME type mapping rules #
   ##############################################
   ```

   Add the following line (cut and paste from here to avoid typos)

   ```
   server.inet.extensionRule.grxml          VXIString     application/srgs+xml
   ```

2. From the windows services panel:

   Stop "Speechworks MediaServer"

   Stop "OpenSpeech Recognizer Monitor"

3. Start services:

   Start "OpenSpeech Recognizer Monitor"

   Start "Speechworks MediaServer"

user.microapp.locale, ICM Scripts, and Case Sensitivity

When using user.microapp.locale in an ICM script for use with Nuance SWMS (formerly Scansoft) ASR/TTS, the ECC variable must be set to "en-US" (for example). If it is set to "en-us" (for example), an error will occur.

Conversely, when using user.microapp.locale in an ICM script for use with Nuance, the ECC variable must be set to "en-us" (for example). If it is set to "en-US" (for example), an error will occur.

Obviously, care must be taken regarding these conflicting case sensitivities.

Resolved Caveats in This Release

This section lists caveats specifically resolved by Unified CVP Maintenance Release 4.0(2). Defects are listed by component and then by identifier.

Table 1 Resolved Caveats for Cisco Unified Customer Voice Portal Release 4.0(2)

Identifier	Component	Headline
CSCsg87980	doc	survivability script does not support REFERS
CSCsh33808	doc	Please update OAMP Help to Note Shutdown CVP will drop existing Calls.
CSCsh55434	doc	Unable to Manually Fix Remainder's if there is more than 14 days of Data
CSCsh23259	infrastructure	RPT: VXML Failover - all records from SER do not arrive at the DB
CSCsg82133	ios	Memory leak in CC-API_VCM process at tcl_chunk_malloc
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
CSCsh39913	oamp	Call Server SIP: Need warning to user to select 'Outbound Proxy Host
CSCsh96739	oamp	Maximum length of DNIS should be set to 32
CSCsh98371	oamp	Unable to enter DNIS greater than 214xxxxxxx on CVP ICM cnfg
CSCsh23831	patch	OAMP: jmx security with aix orm
CSCsh49616	patch	Installing or Uninstalling SR results in deletion of Custom Audio files
CSCsg19173	reporting	SNMP Altert, At least 48 hours since last purge
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 shoud be validated before performing other operations
CSCsi21958	snmp	CVP 4.0 returning incorrect sysobjectID.
CSCsi77184	ss_ged	CVP Call Server sending Run Script Result to incorrect Dialogue ID
CSCsh89829	ss_sip	NO moh when agent puts the pstn caller on hold
CSCsh92260	vbrowse	Change CVP ephemeral port range
CSCsi33002	vbrowse	cvp: no TCS send to ccm
CSCsh26374	vxml_server	AIX VXML Server performance issues can not handle supported load
CSCsi62903	vxml_server	tel url parsing error from transfer tag in CVP 4.0(2)

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.

Tip 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

Tip 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 ICM/IPCC Enterprise and Hosted Editions, go to the "Search for bugs in other Cisco software and hardware products" section, and enter **Cisco Unified Intelligent Contact Management Enterprise** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco Unified Intelligent Contact Management Enterprise**.

Step 4 Click **Next**. The Cisco Unified Intelligent Contact Management Enterprise 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 Intelligent Contact Management Enterprise 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 Release 4.0(2). Defects are listed by component and then by identifier.

Tip 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 2 Open Caveats for Cisco Unified Customer Voice Portal Release 4.0(2)

Identifier	Component	Headline
CSCsf27612	install	ST INSTALL: unable to uninstall supp tools when cvp install is aborted.
CSCsi89957	install	AIX - after install, orm / snmp in bad state
CSCsg64409	oamp	OAMP: CS SIP tab Static route no check on invalid IP address
CSCsi80513	oamp	Outbound proxy host is not listed on changing H323 Call Server to SIP
CSCsi84434	oamp	Graceful shutdown of Reporting server from OAMP fails
CSCsi91723	oamp	OAMP: secure connection from OAMP to GW fails
CSCsi95507	patch	can not restore DB storeProcedure if uninstall of patch failed.
CSCsi86264	snmp	AIX install: snmp agent still running on port 8161 after uninstall
CSCsi60011	ss_ivr	Data Type Etime does not take a value less then 10 for HH field
CSCsi80470	ss_ivr	Incorrect prompt played for GS micro app of Type Date
CSCsi83990	ss_ivr	No prompt played when the length of the text for tts exceeds 123 chars
CSCsi43950	ss_sip	After SingleStepTransfer, GD didn't work
CSCsi79546	vbrowse	Multicast Moh does not work after warm transfer to CVP
CSCsi92848	vxml_server	Error Code = 44 Returned Queuing to VXML Sever w/ HTTPS
CSCsi93028	vxml_server	Missing changeAppAdminPerm script in the latest VXML Server build

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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 comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Field Alerts and Field Notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into www.cisco.com; then access the tool at http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en.

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:

- 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 non emergencies.

- For Non emergencies—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 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 at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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 (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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 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 Cisco Systems technical user magazine for maximizing Internet and networking investments. 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 access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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 for networking professionals to 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

- 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