



Release Notes for Cisco Customer Response Applications 3.1(3)

August 31, 2005

These release notes are for use with Cisco Customer Response Applications (Cisco CRA) Release 3.1(3) and Cisco CallManager Extended Services.

These release notes may be updated occasionally with new information. For the latest version of these release notes, go to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_1/english/admn_app/relnote/index.htm



Note

Effective with release 3.0, Cisco Customer Response Applications (CRA) has been renamed Cisco Customer Response Solutions (CRS) and, effective with release 3.1, is marketed under the names IPCC Express and IP IVR. The Cisco website and packaging materials have been updated to reflect the new name, but the user interface, and therefore the documentation, have not.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Contents

- [Installing a Required Service Release, page 3](#)
- [Maintaining Reason Codes when Upgrading Cisco CRA, page 4](#)
- [What's New in Cisco CRA Release 3.1, page 4](#)
- [Late-Breaking Information, page 6](#)
- [Obtaining Double-Byte Data with a Cisco CRA Script, page 12](#)
- [Upgrading Cisco CRA on a Historical Reports Database Server, page 12](#)
- [Unsupported and Supported Actions for Cisco ICD Agents, page 13](#)
 - [Unsupported Actions for Cisco IP ICD Agents, page 13](#)
 - [Supported Configurations for Agent Phones, page 14](#)
 - [Unsupported Configurations for Agent Phones, page 14](#)
- [Unsupported Features in Cisco Callmanager 3.3\(4\), page 14](#)
- [Nuance Vocalizer 3.0, page 15](#)
 - [Installing Nuance Vocalizer 3.0, page 15](#)
 - [Upgrading from Nuance Vocalizer 1.0 to Nuance Vocalizer 3.0, page 16](#)
 - [Nuance Vocalizer 3.0 Notes, page 18](#)
- [Selecting Languages for ASR, page 19](#)
- [Using Cisco CRA Clients with Microsoft Windows XP-SP2, page 20](#)
- [Features Available with Each Product Package, page 25](#)
- [Related Documentation, page 27](#)
- [Resolved Caveats, page 28](#)
- [Closed Caveats, page 36](#)
- [Known Caveats, page 39](#)
 - [ASR Component, page 40](#)
 - [Cisco CRA Editor Component, page 40](#)
 - [Cisco CRA Installation Component, page 41](#)
 - [Cisco ICD Component, page 41](#)

- Documentation Component, page 54
 - TTS Component, page 59
- Obtaining Documentation, page 59
- Documentation Feedback, page 61
- Cisco Product Security Overview, page 61
- Obtaining Technical Assistance, page 63
- Obtaining Additional Publications and Information, page 65

Installing a Required Service Release

Cisco will occasionally make a new Service Release available for Cisco CRA 3.1(3). Service Releases provide important software updates. After you install Cisco CRA 3.1(3), you must download and install the latest available Service Release on your system. To do so, follow these steps:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Go to this URL:
http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml |
| Step 2 | Locate and double-click the Readme file for the latest Cisco CRA 3.1(3) Service Release and follow the prompts to download this file. The Readme file contains installation instructions and other information for the Service Release. |
| Step 3 | Go back to the URL shown in Step 1, locate and double-click the latest Cisco CRA 3.1(3) Service Release file, and follow the prompts to download this file. |
| Step 4 | Follow the instruction in the Readme file to install the Service Release. |
-

Maintaining Reason Codes when Upgrading Cisco CRA

When you upgrade from Cisco CRA 3.0(x) to Cisco 3.1(3), existing reason codes will be deleted. For more information, including a workaround, see defect number CSCeb17184 in the [“Cisco ICD Component” section on page 41](#).

What’s New in Cisco CRA Release 3.1

Cisco CRA Release 3.1(2) includes the following new features:

- MS SQL Server 2000 Support—You can install MS SQL Server 2000 on a Historical Reports Database Server. For more information, refer to *MS SQL Server 2000 for Historical Reports Database Server Resources Card*.
- Nuance Vocalizer 3.0 Support—Cisco CRA 3.1(1) supports Nuance Vocalizer 3.0 for TTS (Text to Speech). For more information, see the [“Nuance Vocalizer 3.0” section on page 15](#).

Cisco CRA Release 3.1(1) includes the following new features:

- Cisco CallManager 3.3 Support—Cisco CRA now supports Cisco CallManager release 3.3(3) and above.



Note

Cisco CallManager release 3.3(4) includes some features that are not supported by Cisco CRA 3.1. For more information, see the [“Unsupported Features in Cisco Callmanager 3.3\(4\)” section on page 14](#).

- Competency-Based Routing—Allows contacts to be routed to resources based on the resource skill proficiency level, when skills-based routing is configured. Specifically when a pool of resources is available and waiting for the system to route contacts to it, Competency-Based Routing will determine which resource to select on the basis of the skill proficiencies, instead of on the basis of other criteria such as longest available or most handled contacts. Competency-Based Routing provides the functionality to route calls to the most or to the least skilled resources.

- ICD agent line forwarding—When call forwarding for an ICD extension is turned on, non-ICD calls will be forwarded. ICD calls will be pulled back to the queue (not forwarded) and the agent will go to Not Ready state.
- Support for up to 150 ICD Agents—Cisco CRA now supports up to 150 Cisco ICD agents (requires using the appropriate dual-processor server). In addition, the Cisco CRA ICD Configuration web page has been enhanced to support the configuration of ICD agents.
- Support for up to 300 CTI ports —Cisco CRA now supports up to 300 CTI ports (requires using the appropriate dual-processor server).
- Historical Reports Database Server—You can install the Cisco CRA databases (with MSDE) on a separate, dedicated server for historical reporting. Alternatively, you can install the Cisco CRA databases (with MSDE) on the ICD Call Statistics, Recording, and Monitoring Server or the ICD Call Recording and Monitoring Server.
- ICD Call Statistics, Recording, and Monitoring Server—With Cisco ICD Enhanced, you can set up this dedicated server to maintain ICD call statistics and to provide for recording and call monitoring.
- ICD Call Recording and Monitoring Server—You can set up one or more of these servers to provide for call monitoring.
- G.729 codec Support—Cisco CRA now supports G.729 codec for outgoing and incoming voice streams. (Previous releases of Cisco CRA support G.711 codec, and this support continues.) When you use the G.729 codec, prompts are played using the ITU G.729(A) standard format, and recordings are stored in G.729(A) format.
- Support for Dual-CPU Servers—Cisco CRA now supports the MCS-7845H-2.4-CC1 and the Compaq DL 380-2400 G3 dual-processor servers.

Late-Breaking Information

This section provides information, including late-breaking changes, that is not included in the Cisco CRA 3.1 documentation.

Late-Breaking Information for Cisco CRA 3.1(3):

- If you set up a Dedicated ICD Call Monitoring server, there must also be one server that has the ICD Record/Statistics Server component installed on it. This server can be the CRA server or a dedicated server, but only one instance of the ICD Record/Statistics Server component can be installed on it.
- If you upgrade to Cisco CRA release 3.5, you must obtain Cisco CRA 3.5 product licenses. You cannot use product licenses from earlier versions of Cisco CRA.
- If you upgrade Cisco CRA to release 3.1(3), you must upgrade the Cisco Agent Desktop and the Cisco Supervisor Desktop to release 4.5.1.5 after you upgrade Cisco CRA.
- Adding third-party software to a Cisco CRA system may affect how Cisco CRA functions and may affect Cisco's support for Cisco CRA. Such third-party software includes Microsoft critical security updates, anti-virus software, and other non-required third-party software. For information about Cisco's policy regarding third-party software, refer to this URL:

http://www.cisco.com/application/pdf/en/us/guest/products/ps3651/c1037/ccmigration_09186a0080207fb9.pdf

- If you are using MSDE for the Cisco CRA databases, you should install the latest MSDE Service Pack and the Cumulative Patch for SQL 7.0 Server on the Cisco CRA server. If you have installed the CRA databases on a remote server, you should install the Service Pack and Cumulative Patch for SQL 7.0 Server on that server also.

If you are using MS SQL Server 2000 for the Cisco CRA databases on a Remote Database Server, you should install the latest MS SQL Server 2000 Service Pack and the Cumulative Patch for SQL 2000 Server on the remote server on which you have installed the CRA databases.

The Service Packs and Cumulative Patches are named as follows:

- MSDE Service Pack—SQL7-ServicePack4.1-0-2.exe
- MS SQL Server 2000 Service Pack—SQL2K-ServicePack3.1-0-4.exe.

- Cumulative Patch for SQL 7.0—SQL7-MS03-031.exe
- Cumulative Patch for SQL 2000 Server—SQL2K-MS03-031.exe

The Service Packs and Cumulative Patches are available at this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>



Note

Before you install either service pack, stop all services that are running on the server on which you are installing the service pack.

- If you create your own custom reports, Cisco recommends that you use Crystal Reports Developer Edition version 8.5. If you will integrate custom reports with the Cisco CRA Historical Reporting system, you must use Crystal Reports Developer Edition version 8.5 to create the reports.
- Running any of the following historical reports with the Interval Length filter parameter set to 30 or 60 minute intervals can consume significant CPU resources. The report may take a long time to complete.
 - Agent State Summary Report (by Agent)
 - Agent State Summary Report (by Interval)
 - Contact Service Queue Activity Report (by CSQ)
 - Contact Service Queue Activity Report (by Interval)

Cisco recommends that you run these reports at off-peak times.

- Cisco CRA 3.1(3) is compatible with Enterscept HIDS version 2.5.3 and with McAfee Netshield version 4.5.
- When you try to configure a network share for TTS, you may see this message when providing credentials for the network share: `Network share connection failed. [Bad username/pwd or Server unreachable]`. If you see this message, follow these steps:
 - a. Choose **Start > Programs > Administrative Tools > Services**. The Services window appears.
 - b. Right-click the CiscoCRAServletEngine service, choose **Properties**, and click the **Log On** tab. Make sure that the **This account** radio button is checked and that the account is set to Administrator. Click **OK**.

- c. Right-click the Cisco CRA Engine service, choose **Properties**, and click the **Log On** tab. Make sure that the **This account** radio button is checked and that the account is set to Administrator. Click **OK**.
- If you are using a proxy service in Internet Explorer on the CRA Historical Reports client system, scheduled historical reports may not run and you may see this message in the CiscoSch.log log file: [CRA_DATABASE] entry not found in the properties file followed by failed to validate user OR get MaxConnections of database value. If this situation occurs but you can run the report directly from the CRA Historical Reports client system, follow these steps:
 - a. From Internet Explorer on the Historical Reports client system, choose **Tools > Internet Options**.
 - b. Click **Connections**.
 - c. Click **LAN Settings**.
 - d. Click **Advanced**.
 - e. In the Do not use proxy server for addresses beginning with field, enter the IP address of the Cisco CRA server that the Historical Reports client system logs in to.
 - f. Click **OK** as needed to save your changes.
- If a large number of VRU scripts are configured for your system, the Add VRU Script operation and the Refresh Scripts operation can take a long time to complete. These tasks can also result in high CPU utilization.
- In Cisco CRA 2.x, the default setting for media steps is interruptible = NO. In Cisco 3.x, the default setting for these steps is interruptible = YES. However, scripts that are upgraded from Cisco CRA 2.x to Cisco CRA 3.x will retain the interruptible = NO setting. You should set media steps in Cisco CRA 3.1(3) queuing scripts that are upgraded from 2.x to 3.x to interruptible = YES. In this way, the IVR system will be able to properly transfer a call to an agent.
- Cisco CRA does not support the use of child domains with Active Directory
- Cisco supports the use of Active Directory 2003 as an LDAP server for storing and retrieving configuration and user data.
- On the Cisco CRA server, make sure to check the **Automatically adjust clock for daylight savings changes** check box in the Windows Date/Time Properties window Time Zone tab, if this check box is available.

- A script will only execute steps in the Failed branch of the Connect step if no agents are available for the call when the connect step goes to the Failed branch. Instead the call will immediately go from the Failed branch to the Select Resource step. In addition, if an agent becomes available while the Failed branch of the Connect step is executing, the steps in the Failed branch will immediately stop executing and the call will to the Select Resource step.
- Any server on which you install Cisco CRA must be a Cisco-approved server. For a list of approved servers, refer to *Cisco CallManager Compatibility Matrix*, which is available at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

- The use of dual network interface cards (NICs) is supported on a server that is running Nuance ASR if the NICs are used for traffic segregation and not for redundancy. If you install dual NICs on such a server, you must configure the Nuance ASR software to use the primary NIC. In addition, you should configure Nuance processes to refer to host servers using the IP addresses of the host server, not their host names.
- Cisco CRS does not support NIC teaming.
- If you are deploying an MCS-7835-I1, MCS-7845-I1, or IBM xSeries-346 server, refer to the field notice Some Cisco Media Convergence Server (MCS) Encounter Network Interface Card (NIC) Numbering Reversal, which is available at this URL:

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/products_field_notice09186a0080415411.shtml

- When you install the Windows 2000 Server operating system provided by Cisco on a server on which you will install Cisco CRS, but not Cisco CallManager, use the following Cisco CRS product key:

FVHD IAZA ROFJ DERJ

When you install the operating system on a server on which you will install Cisco CRS and Cisco CallManager, use a valid Cisco CallManager Manager product key instead of the Cisco CRS product key.

Late-Breaking Information for Cisco CRA 3.1(1):

- The following data writing intervals have been added: 5, 10, 15, 20, and 25. You can set the data writing intervals from Cisco CRA Administration by choosing **Tools > Real Time Snapshot Config** and then choosing the desired

value from the Data Writing drop-down list. These new data writing intervals are useful when wallboard data is required to be updated with a refresh interval of less than 30 seconds.

- The following historical reports now display up to three skills for the CSQ to which the call was routed:
 - Agent Detail Report
 - Abandoned Call Detail Report
- The Common Skill Contact Service Queue Activity Report (by Interval) has been added to Cisco CRA Historical Reports. This report provides the following summary information for each group of CSQs:
 - Calls Presented—Maximum number of calls offered to each individual CSQ within the group. The maximum number rather than the sum is shown because the same call can be presented to multiple CSQs within the same group.
 - Calls Handled—Sum of calls handled by each individual CSQ within the group. The sum is used because each call, if handled, is handled by only one CSQ .
 - Calls Abandoned—Maximum number of calls abandoned from the same group. The maximum number is shown because a call abandoned is considered to be abandoned from all the CSQs for which it was queued.
- You can use the “**tempdb**” option with the **runTruncateHistDBLogs** command to truncate the tempdb.ldf database transaction log file. The new syntax for this command is:

runTruncateHistDBLogs “dbUserName” “dbPassword” {“db_cra” | “db_cra_ccdr” | “db_cra_all” | “tempdb”} size

Refer to the “Truncating Database Transaction Log File” section in the “Managing the Cisco CRA HHistorical Report Databases” chapter in *Cisco Customer Response Applications Administrator Guide* for detailed information about this command.

- When installing the Nuance Speech Server software, this message may appear: Setup Initialization Error Insufficient memory available to run Setup. Close all other applications to make more memory available and try to run Setup again. This message is most likely to appear on a Cisco MCS-7845 when the virtual memory is set to a high number. If you see this message, click **OK**. The installation will continue successfully.

- If a Historical Reports Database Server is set up and you have restored backed-up data on the Cisco CRA server but not on the Historical Reports Database Server, MIVR logs show that historical records fail because of primary key conflicts. (Both servers should always be backed up at the same time.) To workaround this problem, restore the backed-up data to the Historical Reports Database Server manually. Alternatively, follow these steps:
 - a. Use a text editor to open this file: C:\program files\WFAVVID\wfengine.properties. (This file may be in another folder if you did not install Cisco CRA in the default folder.)
 - b. Add 1000 to the value of this property:
com.cisco.wfframework.engine.APPLICATION_TASKID_BLOCK
 - c. Save the wfengine.properties file.
 - d. Use a text editor to open this file: C:\program files\WFAVVID\application.properties. (This file may be in another folder if you did not install Cisco CRA in the default folder.)
 - e. Add 1000 to the value of this property: com.cisco.session.id.block
 - f. Save the application.properties file.
- During generation of an Agent Detail Report or an Abandoned Call Detail Activity Report, an error message may appear indicating that the connection with the database has been broken. This message may appear if the system is under a heavy load when either of these reports is generated. A heavy load can include tens of thousands of calls during the report period or the maximum number of skills configured in the system. To work around this problem, reduce the length of the report period or reconfigure CSQs so that there are more CSQs with fewer skills each.
- If you create a custom button in the Cisco Agent Desktop that changes the agent state to AgentWork, the button will allow an agent to go from Ready state to Work state. However, this state change is not supported. To work around this issue, remove the custom button and use the Work button on the Cisco Agent Desktop to go from Ready state to Work state.

Obtaining Double-Byte Data with a Cisco CRA Script

The following guidelines apply when you use a Cisco CRA script to obtain double-byte data from a database:

- The database table must be defined to return UTF-8.
- Load the data from the database into an Editor variable (for example, dbString) with UTF-8 bytes using the DB Read and DB Get steps.
- Write a custom Java Class that takes the Editor UTF-8 string from the variable returns a UTF-16 string
- Pass the returned string to the step in which it needs to be used. For example, the Set Enterprise Data step.

Upgrading Cisco CRA on a Historical Reports Database Server

If you upgrade Cisco CRA on a Historical Reports Database Server, the Cisco CRA installation program will not overwrite existing data files. As a result, you will not be able to update configuration information on the Cisco CRA Administration Historical Reporting Configuration web page.

To avoid this problem, upgrade Cisco CRA on a Historical Reports Database Server by performing the following general steps. For detailed instructions about installing Cisco CRA on a Historical Reports Database Server, refer to *Getting Started with Cisco Customer Response Applications*.



Caution

This procedure deletes existing data files. If you want to save these files, back them up before you perform this procedure.

Procedure

- Step 1** On the Historical Reports Database Server, delete all files in the c:\Program Files\Microsoft SQL Server\MSSQL\data folder.
- Step 2** On the Historical Reports Database Server, delete all files in the C:\MSSQL7\data folder.

- Step 3** On the Historical Reports Database Server, use the Windows Add/Remove Programs window to uninstall Cisco CRA RemoteDB.
- Step 4** On the Historical Reports Database Server, use the Windows Add/Remove Programs window to uninstall MSSQL Server.
- Step 5** On the Historical Reports Database Server, reinstall Cisco CRA.
During the installation, make sure to configure Cisco CRA as a Remote Database Server.
- Step 6** Make appropriate configurations on the Cisco CRA Administration Historical Reporting Configuration web page.

Unsupported and Supported Actions for Cisco ICD Agents

This section outlines the unsupported and supported actions for agents using the Cisco Agent Desktop or the Cisco IP Phone Agent Service. Agents can access similar information in the Cisco Agent Desktop online help.

Unsupported Actions for Cisco IP ICD Agents

The following actions are not supported:

- Arbitrary transfer or conference—Agent A receives a Cisco IP ICD call, places the call on hold, and initiates another call to another agent or user. Agent A then merges the two calls into a conference by making a new call and pressing the **Transfer** or the **Conference** button twice. Either of these actions will cause some information in certain historical reports to be inaccurate.

The agent can avoid this problem by initiating the transfer or conference using the appropriate feature button on the Cisco Agent Desktop or the Cisco IP Phone.

- Transferring a conference call—This action will cause some information in certain historical reports to be inaccurate.
- Using the **MeetMe**, **Pickup**, and **GPickup** soft keys.

Supported Configurations for Agent Phones

To determine the phone devices that supported by the Cisco Agent Desktop and for use by Cisco IP Phone Agents, refer to *Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide*, which is available at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/crscomtx.pdf

Unsupported Configurations for Agent Phones

The following configurations are not supported for agent phones:

- Two lines on an agent's phone that have the same extension but exist in different partitions.
- Configuring the same ICD extension in more than one device profile, or configuring the same ICD extension in any combination of device profiles and devices. (Configuring an ICD extension in a single device profile is supported.)
- Call waiting enabled on an ICD line.
- No Cisco Call Manager device can be forwarded to the ICD extension of an agent.
- The ICD extension of an agent cannot be configured to forward to a Cisco CRA route point.
- Use of characters other than the numerals 0 - 9 in the ICD extension of an agent.

Unsupported Features in Cisco Callmanager 3.3(4)

The following new features introduced with Cisco CallManager 3.3(4) are not supported by Cisco CRA 3.1. These features are disabled by default and should not be enabled for Cisco CRA.

- Forced Authorization Codes and Client Matter Codes (FAC/CMC)
- Block External to External Transfer

- Drop Adhoc Conference When Creator Leaves
- Q Signalling (QSIG)

For more information about these features, refer to *Release Notes for Cisco CallManager Release 3.3(4)* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/rel_note/334cmrn.htm

Nuance Vocalizer 3.0

Cisco CRA 3.1(3) supports Nuance Vocalizer 3.0 for TTS (Text to Speech). Vocalizer 3.0 offers enhanced voice quality.

This section includes the following topics:

- [Installing Nuance Vocalizer 3.0, page 15](#)
- [Upgrading from Nuance Vocalizer 1.0 to Nuance Vocalizer 3.0, page 16](#)
- [Nuance Vocalizer 3.0 Notes, page 18](#)

Installing Nuance Vocalizer 3.0

If you obtained the appropriate Vocalizer 3.0 license files and transferred them to the Cisco CRA server, Vocalizer 3.0 is installed when you install Nuance TTS. (For more information about license files and Nuance TTS installation, refer to *Getting Started with Cisco Customer Response Applications 3.1*.)

To install Vocalizer 3.0 for Cisco CRA 3.1(3), follow these steps after you install and configure Cisco CRA:

Procedure

-
- Step 1** Follow Steps 1 through 12 in the “Installing Nuance ASR and TTS” chapter in *Getting Started with Cisco Customer Response Applications 3.1*.
- Step 2** Follow the on-screen prompts to complete the installation of Vocalizer 3.0
- Always accept the default values in each dialog box that appears. Do not change these values.
- If you do not have the Java Runtime Environment (JRE) installed on your system, the JRE installation program may start during the Nuance installation. If the JRE installation program starts, follow the on-screen prompts and accept the default values in all dialog boxes while installing the JRE.
- When a release notes document appears during the installation, close that document to continue with the installation.
- When the installation is complete, a Structured Query Language (SQL) Password dialog box appears.
- Step 3** Enter a new SQL Administrator Password, or leave the field blank, and then click **OK**.
- Step 4** When you are prompted to reboot, click **Yes**.
-

Upgrading from Nuance Vocalizer 1.0 to Nuance Vocalizer 3.0



Upgrading from Nuance Vocalizer 1.0 to Nuance Vocalizer 3.0 requires new license files, so when you upgrade, you must also reinstall Cisco CRA. You also must reinstall the Nuance Speech Server software on each server on which it is currently installed.



Note

When you upgrade to Nuance Vocalizer 3.0, all existing TTS configuration information will be deleted and will need to be reconfigured.

Procedure

-
- Step 1** Remove the Vocalizer 1.0 license files from the Cisco CRA server.
- If the Nuance Speech Server software is installed on a dedicated server, remove the Vocalizer 1.0 license files from that server also.
- To determine if a license file is for Vocalizer 1.0, use a text editor to open the file and search for this string: CRA_NUANCETTSSW. If this string is found, the file is a Vocalizer 1.0 license file.
- Step 2** Copy the Vocalizer 3 license file or files to the Cisco CRA server.
- If you will install the Nuance Speech Server software on a dedicated server, copy the Vocalizer 3 license file or files to that server also.
- For information about copying license files, refer to the “Transferring License Files to the CRA Server” section in *Getting Started with Cisco Customer Response Applications*.
- Step 3** Install Cisco CRA on the Cisco CRA Server.
- For instructions, refer to *Getting Started with Cisco Customer Response Applications 3.1*.
- Make sure to select all appropriate components and languages during the installation.
-  **Note** The installation will not indicate the presence of ASR and TTS licenses. However, you can continue with the installation.
-
- Step 4** Set up Cisco CRA.
- Refer to the “Accessing the CRA Administration Web Interface” and the sections that follow in *Getting Started with Cisco Customer Response Applications 3.1*.
-  **Note** Do not configure TTS after completing this setup procedure. Instead, continue with this procedure.
-
- Step 5** Install the latest available Cisco CRA Service Release.
- For instructions, see the [“Installing a Required Service Release” section on page 3](#).

- Step 6** Install the Nuance Speech Server software on the Cisco CRA server using Cisco Customer Response Solutions CD-ROM 5.

For instructions, see [“Installing Nuance Vocalizer 3.0” section on page 15](#).

The installation program will indicate the presence of ASR and TTS license files. Make sure that the program indicates TTS3, which is for Vocalizer 3 license files.

The installation program will detect a previous installation of Vocalizer 1.0 and will prompt you to uninstall that version. Follow the prompts to uninstall Vocalizer 1.0 and re-run the Nuance Speech Server installation program.

- Step 7** Install the Nuance Speech Server software on a dedicated speech server, if appropriate.

- Step 8** Configure the speech server.

For instructions, refer to the “Provision the Nuance TTS Subsystem” section in *Cisco Customer Response Applications Administrator Guide*.

Nuance Vocalizer 3.0 Notes

- If you upgrade from Vocalizer 1.0 to Vocalizer 3.0 or downgrade from Vocalizer 3.0 to Vocalizer 1.0, TTS configuration will be lost. Before you upgrade or downgrade, make a note of existing configuration values. You can reenter these values manually.
- You can install either Vocalizer 1.0 or Vocalizer 3.0, but not both, in the same Cisco CRA system.
- You can install up to two languages for Vocalizer 3.0.
- You may install Cisco CRA, ASR, and Vocalizer 3.0 for one language on the same server, but that server must be a Cisco MCS-7845.
- Do not install ASR and Vocalizer 3.0 on the same server if Cisco CRA is installed on another server. In this case, ASR and Vocalizer 3.0 TTS must be installed on two separate servers.
- You cannot change the speed of speech for Vocalizer 3.0. The default speed of 50 will be used for all language-gender combinations.

- Each Vocalizer 3.0 process is configured to support a maximum of up to 60 requests simultaneously. If you wish to use more than 60 simultaneous requests, configure additional Vocalizer 3.0 processes to support more requests. For example, to support 130 TTS requests, then you must configure three Vocalizer 3.0 processes. (Configuring only two Vocalizer 3.0 processes would allow you to use up to 120 TTS requests.)
- You can specify text replacement filters for Vocalizer 3.0. These filters modify how specific text input is rendered by the TTS system. To specify replacement filters, follow these steps:
 - a. Use a text editor to open the file `c:\program files\wfavvid\TTS.properties`. (This file may be in another folder if you did not install Cisco CRA in the default folder.)
 - b. Change the value of the `isFilterEnabled` key to `true`. This key should then appear as `isFilterEnabled=true`.
 - c. Specify the names of the filters for the appropriate languages. Separate multiple filters with commas and do not include spaces. For example, if you want to use `filter1` and `filter2` for the US English language, specify `filter_USEnglish=filter1,filter2`
 - d. Save and Close the `TTS.properties` file.
 - e. Stop and then restart the Cisco CRA Engine service.
- For detailed information about Vocalizer 3.0 features, including the text replacement feature, refer to the Nuance documentation. To access this documentation from the Cisco CRA server, choose **Start > Programs > Nuance > Nuance Vocalizer 3.0 for Nuance 7 > Documentation**.

Selecting Languages for ASR

If you will install Nuance ASR, you must select the appropriate country-specific language or languages for use with ASR when you install Cisco CRA. [Table 1](#) shows the Cisco CRA country-specific languages that correspond to the ASR languages. When you install Cisco CRA, make sure to select the appropriate country-specific languages for the ASR languages that you will install.

Table 1 *CRA Country-Specific Languages and ASR Languages*

Cisco CRA Country-Specific Language	Corresponding ASR Language
en_US or en_CA	en_US
en_GB	en_GB
es_MX or es_US	es_MX
es_CO	es_CO
es_ES	es_ES
fr_FR	fr_FR
fr_CA	fr_CA
it_IT	it_IT
ja_JP	ja_JP
de_DE	de_DE

Using Cisco CRA Clients with Microsoft Windows XP-SP2

This section describes the steps you must take to allow the following Cisco CRA client applications to function on a PC that is running Microsoft Windows XP-Service Pack 2 (Windows XP-SP2) and on which the Windows Firewall is operating:

- Cisco Agent Desktop
- Cisco Agent Desktop with Media Termination
- Cisco Supervisor Desktop
- Cisco Desktop Administrator

The procedures in this section are not required for the Cisco CRA Editor or for the Cisco CRA Historical Reporting client.

This section includes these topics:

- [Upgrading a PC on which a Cisco CRA Client is Already Running to Windows XP-SP2, page 21](#)
- [Installing a Cisco Desktop Client on a PC on which Windows XP-SP2 is Already Running, page 23](#)
- [Unblocking Applications, page 25](#)

Upgrading a PC on which a Cisco CRA Client is Already Running to Windows XP-SP2

The following sections explain the steps you must take when you install Windows XP-SP2 on a PC on which a Cisco CRA Client is already installed:

- [Cisco Agent Desktop and Cisco Supervisor Desktop, page 21](#)
- [Cisco Agent Desktop with Media Termination, page 22](#)
- [Cisco Desktop Administrator, page 23](#)

Cisco Agent Desktop and Cisco Supervisor Desktop

After you upgrade a PC to Windows XP-SP2, an agent or supervisor will see a Windows Security Alert when attempting to log in to Cisco Agent Desktop for the first time or when selecting a team using the Cisco Supervisor Desktop.

- If the agent or supervisor is logged in to Windows without administrator privileges, the alert prompts: To help protect your computer, Windows Firewall has blocked some features of this program. Your computer administrator can unblock this program for you.

In this case, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

- If the agent or supervisor is logged in to Windows with administrator privileges, the alert prompts: To help protect your computer, Windows has blocked some features on this program. Do you want to keep blocking this program?

In this case, the agent or supervisor should click the **Unblock** button to continue. If the agent or supervisor clicks the **Keep Blocking** button or the **Ask Me Later** button, various features in the Cisco Agent Desktop or

Cisco Supervisor Desktop will not work properly. To correct this problem, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

Cisco Agent Desktop with Media Termination

After you upgrade a PC to Windows XP-SP2, an agent or supervisor will see a Windows Security Alert when attempting log in to the Cisco Agent Desktop with Media Termination for the first time.

- If the agent or supervisor is logged in to Windows without administrator privileges, the alert prints: To help protect your computer, Windows Firewall has blocked some features of this program. Your computer administrator can unblock this program for you.

In this case, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

- If the agent or supervisor is logged in to Windows with administrator privileges, this alert prompts: To help protect your computer, Windows has blocked some features on this program. Do you want to keep blocking this program?

In this case, the agent or supervisor should click the **Unblock** button to continue. If the agent or supervisor clicks the **Keep Blocking** button or the **Ask Me Later** button, various features in the Cisco Agent Desktop or Cisco Supervisor Desktop will not work properly. In addition, the agent or supervisor will be unable to hear callers. To correct this problem, perform the procedure described in the [“Unblocking Applications” section on page 25](#).



Note

If you have unblocked the Cisco Agent Desktop but not the Media Termination module, an agent or supervisor will see a Windows Security Alert for the Media Termination module the first time a call is presented. In this case, the agent or supervisor should click the **Unblock** button to continue. If the agent or supervisor clicks the **Keep Blocking** button or the **Ask Me Later** button, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

Cisco Desktop Administrator

After you upgrade a PC to Windows XP-SP2, an agent or supervisor will see a Windows Security Alert when attempting access the Cisco Desktop Administrator for the first time.

- If the agent or supervisor is logged in to Windows without administrator privileges, the alert prints: To help protect your computer, Windows Firewall has blocked some features of this program. Your computer administrator can unblock this program for you.

In this case, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

- If the agent or supervisor is logged in to Windows with administrator privileges, this alert prompts: To help protect your computer, Windows has blocked some features on this program. Do you want to keep blocking this program?

In this case, the agent or supervisor should click the **Unblock** button to continue. If the agent or supervisor clicks the **Keep Blocking** button or the **Ask Me Later** button, the Logical Call Center and other data will not appear in the Cisco Desktop Administrator. To correct this problem, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

Installing a Cisco Desktop Client on a PC on which Windows XP-SP2 is Already Running

When you install the Cisco Agent Desktop (with or without Media Termination), the Cisco Supervisor Desktop, or the Cisco Desktop Administrator on a PC on which Windows XP-SP2 is already installed, the following message will appear:

Security Warning message. The publisher could not be verified. Are you sure you want to run this software?

When you see this message, click **Yes** to continue.

After you upgrade a PC to Windows XP-SP2, an agent or supervisor will see a Windows Security Alert in the following situations:

- When attempting to log in to the Cisco Agent Desktop for the first time
- When selecting a team using the Cisco Supervisor Desktop

- When performing these actions in the Cisco Desktop Administrator:
 - Launching Cisco Desktop Administrator (for the application Administrator.exe)
 - Clicking **Enterprise Data Configuration/Enterprise Data** for the application TSSPAdm
 - Attempting to save a Reason Code that you added under the Desktop Configuration\Reason Codes node (for the application SplkView)

The Windows Security Alert varies depending on how the agent or supervisor is logged in.

- If the agent or supervisor is logged in to Windows without administrator privileges, this alert prompts: To help protect your computer, Windows Firewall has blocked some features of this program. Your computer administrator can unblock this program for you.

In this case, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

- If the agent or supervisor is logged in to Windows with administrator privileges, this alert prompts: To help protect your computer, Windows has blocked some features on this program. Do you want to keep blocking this program?

In this case, the agent or supervisor should click the **Unblock** button to continue. If the agent or supervisor clicks the **Keep Blocking** button or the **Ask Me Later** button, various features in the Cisco Agent Desktop or Cisco Supervisor Desktop will not work properly. In addition, an agent or supervisor will be unable to hear callers if using Media Termination, and the Logical Call Center and other data will not appear in the Cisco Desktop Administrator. To correct these problems, perform the procedure described in the [“Unblocking Applications” section on page 25](#).

Unblocking Applications

Procedure

-
- Step 1** Log into the PC as the Windows administrator.
- Step 2** Choose **Start > Settings > Control Panel > Security Center > Windows Firewall**.
- Step 3** Click the **Exceptions** tab.
- Step 4** Check one or more of the following check boxes in the Program and Services window, as appropriate.
- If an appropriate application does not appear, click **Add Programs**, and then browse to C:\Program Files\Cisco\Desktop\Bin and select the program.
- **CallChat**—In all cases
 - **Cisco Agent Desktop**—In all cases
 - **MediaClient Module**—In all cases
 - **Cisco Supervisor**—If the Cisco Supervisor Desktop is running on the PC
 - **Supervisor Log Viewer**—If the Cisco Supervisor Desktop is running on the PC
 - **Cisco Desktop Administrator**—If the Cisco Desktop Administrator is running on the PC
 - **SplkView**—If the Cisco Desktop Administrator is running on the PC
 - **TSSPAdm**—If the Cisco Desktop Administrator is running on the PC
- Step 5** Click **OK**.
-

Features Available with Each Product Package

[Table 2](#) lists the Cisco CRA features that are available with each Cisco CRA product Package.

Table 2 Features Enabled by Each Product Package

Feature	IP IVR¹	IP ICD² Standard	IP ICD Enhanced	IP ICD Enhanced/ CTI³ Option	IP-QM⁴	Extended Services
Telephony Apps	X	X ⁵	X ⁵	X ⁵	X ⁶	
ICD ⁷		X	X	X		
Queue Manager	X				X	
Extension Mobility	X ⁸			X ⁸		X
Auto Attendant	X ⁸			X ⁸		X
Multiple Language Support	X	X	X	X	X	
JTAPI ⁹	X	X	X	X	X	X
HTTP ¹⁰	X			X		
Email	X			X		
Database	X			X		
Cisco Media Termination	X	X	X	X	X	X
ASR ¹¹	X ¹²		X ¹²	X ¹²	X ¹²	
TTS ¹³	X ¹²		X ¹²	X ¹²	X ¹²	
Voice Browser	X ¹⁴		X ¹⁴	X ¹⁴	X ¹⁴	
Real-Time Reporting	X	X	X	X	X	X
Historical Reporting	X ¹⁵	X ¹⁶	X ¹⁷	X ¹⁷	X ¹⁵	
Editor	X ¹⁸	X ¹⁹	X ²⁰	X ²¹	X ²²	

1. IP IVR = Cisco IP Interactive Voice Response

2. IP ICD = Cisco IP Integrated Contact Distribution

3. CTI = Computer Telephony Interface

4. IP-QM = IP Queue Manager

5. Cisco Intelligent Contact Management (ICM) (Translation routes and Post-routes can not be configured)

6. Only ICM (Translation routes and Post-routes), Busy, and Ring-No-Answer (RNA) applications can be configured
7. ICD = Integrated Contact Distribution
8. Sample Scripts Included
9. JTAPI = Java Telephony Application Programming Interface
10. For Extended Services, the HTTP subsystem and the ability to configure HTTP triggers is included for use with Extension Mobility.
11. ASR = Automatic Speech Recognition
12. Add-on Feature
13. TTS = Text-To-Speech
14. Only available if ASR option is purchased
15. Only IVR Reports
16. ICD Standard Historical Reporting Client can be purchased
17. ICD Enhanced Historical Reporting Client can be purchased
18. ICD Steps not included
19. Email, Http, DB, ICM and Java steps not included, and the Set Priority step is not included
20. Email, Http, DB, ICM and Java steps not included
21. ICM Steps not included
22. Email, Http, DB, User and ICD steps not included

Related Documentation

[Table 3](#) provides references to related documentation. In addition, you can obtain online help from the Cisco CRA Administration web pages, the Cisco CRA Editor, the Cisco Agent Desktop, the Cisco Supervisor Desktop, the Cisco Desktop Administrator, and the Cisco CRA Historical Reports client interface.

Table 3 **Related Documentation**

Related Information and Software	Document or URL
Cisco CRA 3.1 documentation overview	<i>Cisco Customer Response Applications 3.1 Resources Card</i> in your Cisco CRA product package
Cisco CRA 3.1 documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_1/index.htm
<i>Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/crscomtx.pdf

Table 3 *Related Documentation (continued)*

Related Information and Software	Document or URL
Cisco voice products documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
Operating system documentation and Virtual Network Computing (VNC) documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Cisco MCS hardware specifications	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/products_data_sheets_list.html
<i>Cisco CallManager Compatibility Matrix</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/cemcomp.htm
Cisco CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
Cisco CallManager Extended Services	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/extendsv/index.htm
Cisco ICM Software and Cisco IPCC documentation	http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm

Resolved Caveats

This section contains a list of Severity 1, 2, and 3 and some Severity 4 and 6 defects that were resolved in this release of Cisco CRA.

Defect Number: CSCeb78798

Severity Level: 2

Headline: Ghost Calls in Real-Time Reporting

Defect Number: CSCec20826

Severity Level: 2

Headline: Unable to view overall ICD stats for conf to AA then redirect to ICD

Defect Number: CSCec48677

Severity Level: 2

Headline: ASR Name to User step fails to return extension numbers from LDAP

Defect Number: CSCec61496

Severity Level: 2

Headline: 100% CPU if script uses OnExceptionGoTo to catch AppsException

Defect Number: CSCeb21720

Severity Level: 3

Headline: Historical Reporting Client discrepancy

Defect Number: CSCeb34844

Severity Level: 3

Headline: Call Is Aborted When Agent Conference The Caller To ICD route point

Defect Number: CSCeb81634

Severity Level: 3

Headline: CSQ Activity report shows incorrect abandons

Defect Number: CSCeb86177

Severity Level: 3

Headline: Small Int Variable Reporting Snafu

Defect Number: CSCec11412

Severity Level: 3

Headline: Update fails in Purge config page

Defect Number: CSCec12951

Severity Level: 3

Headline: CRA 3.1 Does Not Search OUs below the OU specified in AD for U ACC

Defect Number: CSCec14885

Severity Level: 3

Headline: Failure in answering a consult for conference is mistaken as blind transfer

Defect Number: CSCec16219

Severity Level: 3

Headline: Agent not able to log in after moving stations

Defect Number: CSCec21693

Severity Level: 3

Headline: Talk time numbers do not match

Defect Number: CSCec39349

Severity Level: 3

Headline: Cannot conference using Cisco Agent Desktop (CAD) conference button

Defect Number: CSCec44681

Severity Level: 3

Headline: Empty DB when running historical report for Agent State Summary

Defect Number: CSCec47038

Severity Level: 3

Headline: Agent State left in Reserved after un-hold of ICD call

Defect Number: CSCec50915

Severity Level: 3

Headline: Inaccurate Agent Login Data

Defect Number: CSCec52258

Severity Level: 3

Headline: Agent stuck in Talking state

Defect Number: CSCec56602

Severity Level: 3

Headline: Agent Stuck in Reserved when going offhook right before selected

Defect Number: CSCec57333

Severity Level: 3

Headline: Cannot display agent first/last names in Resources page

Defect Number: CSCec68399

Severity Level: 3

Headline: Searching for users in User Maintenance does not always shows desired users

Defect Number: CSCec86964

Severity Level: 3

Headline: CRA does not update the Resource ID

Defect Number: CSCed04459

Severity Level: 3

Headline: ASR returning all PAB entries, which should be filtered

Defect Number: CSCed05867

Severity Level: 3

Headline: ICD: Agent goes off hook when RNA pulls call back, left in Reserved

Defect Number: CSCed07235

Severity Level: 3

Headline: Calls transferred from Unity AA to CRA show Unity DN as ANI

Defect Number: CSCed12005

Severity Level: 3

Headline: Keep Request controls in context in new ldap ctx due to comm excep

Defect Number: CSCed20826

Severity Level: 3

Headline: Script conversion from 2.x blanks out Get Call Contact Info step

Defect Number: CSCed21720

Severity Level: 3

Headline: Real-time report incorrect after call is dequeued and redirected

Defect Number: CSCed25174

Severity Level: 3

Headline: Cannot bring up Applications Administration page after installation

Defect Number: CSCed26787

Severity Level: 3

Headline: Historical Report shows call Dequeued but Real-Time Report does not

Defect Number: CSCed35106

Severity Level: 3

Headline: Wrong Caller ID after agent performs conference

Defect Number: CSCed37033

Severity Level: 3

Headline: Sessions hung and CRA Engine failed to stop after SQL down

Defect Number: CSCed42650

Severity Level: 3

Headline: Deleting AD user does not remove ID in Applications Administration Resource page

Defect Number: CSCed58672

Severity Level: 3

Headline: Real-Time Report does not update changes to User/Resource name

Defect Number: CSCed63915

Severity Level: 3

Headline: Agent stuck in Talking after transfer call-specific scenario

Defect Number: CSCed72559

Severity Level: 3

Headline: Nullpointer exception with AudioFormat

Defect Number: CSCed76654

Severity Level: 3

Headline: ICD caller intermittently stuck in queue when RNA=False

Defect Number: CSCed80292

Severity Level: 3

Headline: SQL2K License mode should be set to PERPROC

Defect Number: CSCed81927

Severity Level: 3

Headline: Agent desktop locks when LDAP lookup fails

Defect Number: CSCed93008

Severity Level: 3

Headline: Outbound calls are not being reported as outbound

Defect Number: CSCin61367

Severity Level: 3

Headline: AppAdmin Not listing CM users - Netscape Directory Configuration

Defect Number: CSCma24256

Severity Level: 3

Headline: The average and maximum talk times are reported incorrectly in the Cisco Supervisor Desktop

Closed Caveats

This section contains a list of Severity 1, 2, and 3 defects that were closed for this release of Cisco CRA.

If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release.

To access the Bug Toolkit, perform either of these actions:

- Go to this URL:
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
 - Log in to Cisco.com, click **Technical Support**, then click **Tools & Utilities**, then click **Software Bug Toolkit** under Troubleshooting Tools
-

Defect Number: CSCdv83022

Severity Level: 3

Component: Cisco CRA Historical Reports

Headline: The Scheduler icon does not appear in the Windows status bar under a terminal service session.

Symptom: The Scheduler icon does not appear.

Condition: You are running the Cisco CRA Historical Reports client under a terminal service session.

Workaround: This situation is normal. If you need to access features from the Scheduler icon, you must do so from the computer on which the Scheduler is installed.

Defect Number: CSCdv83312

Severity Level: 3

Component: Cisco CRA Historical Reports

Headline: When printing a historical report on a computer running Windows 98, the Print dialog box displays an incorrect printer.

Symptom: The Windows Print dialog displays an incorrect printer on the Cisco CRA Historical Reports client computer.

Condition: On a computer running the Windows 98 operating system, you have changed the default printer while Cisco CRA Historical Reports is running but you have not exited and restarted Cisco CRA Historical Reports.

Workaround: Exit and restart Cisco CRA Historical Reports.

Defect Number: CSCdx90332

Severity Level: 3

Component: Cisco ICD

Headline: Updating a network interface card driver disables silent monitoring and recording.

Symptom: The Cisco Agent Desktop and the Cisco Supervisor Desktop Silent Monitoring and Recording features do not work.

Condition: You have updated a network interface card driver on the server on which you checked the **VoIP Monitor Server** check box during installation of Cisco CRA.

Workaround: Reinstall Cisco CRA. (Make sure to check the **VoIP Monitor Server** check box in the Component Distribution pane.)

Defect Number: CSCdy35520

Severity Level: 3

Component: Cisco ICD

Headline: The Silent Monitoring and Recording features do not work when an agent is using a Cisco IP Softphone.

Symptom: The Cisco Agent Desktop and Cisco Supervisor Desktop Silent Monitoring and Recording features do not work for an agent.

Condition: The agent is using a Cisco IP Softphone as the agent device

Workaround: In the Cisco CallManager Administration web page for the Softphone CTI port, configure the CTI port Device Name to be “SEP” followed by the MAC address of the Softphone PC. Letters in the MAC address must be capitalized.

Defect Number: CSCea24470

Severity Level: 3

Component: Cisco CRA Real-Time Reports

Headline: Real-Time Reports client can not run from a server with a Cisco CallManager installed.

Symptom: The following message appears when you run a real-time report from Cisco CRA Administration: You are using JRE 1.4.0xx. Please exit, uninstall .4.0xx and install JRE 1.3.1

Condition: You are attempting to run the report on a server on which Cisco CallManager is installed.

Workaround: Run the report on a server on which Cisco CallManager is not installed.

Defect Number: CSCea41829

Severity Level: 3

Component: Cisco CRA Real-Time Reports

Headline: JRE causes IE exception while running RTR, freezes Windows 98SE,

Symptom: The message `DDHELP caused an invalid page fault in module <unknown> at . . .` appears after a real-time report has been running for a while, and the computer hangs.

Condition: A real-time report has been running for a long time on a computer running the Windows 98 SE operating system, JRE 1.3.1 or 1.4.1, and Internet Explorer 5.0 SP2.

Workaround: Upgrade Internet Explorer to version 5.5 SP2. If the problem persists, open Java Plug-in panel from the Windows Control Panel and add **-Dsun.java2d.noddraw=true** as a parameter.

Defect Number: CSCea44050

Severity Level: 3

Component: Cisco CRA Real-Time Reports

Headline: JRE failed to installed on servers with 4GB RAM

Symptom: The following message appears when you run the JRE 1.3.1 installer:
Insufficient memory available to run Setup. Error 111.

Condition: You are installing on a computer with more than 4 GB of RAM.

Workaround: Take one of these actions:

- Remove RAM temporarily when installing JRE 1.3.1.
- Run instances of a memory-intensive application to make available RAM less than 2 GB. For example, run several sessions of the My Leaky App application, which is available in the Windows 2000 Resource Kit. (Make sure to disable or delete the application after JRE is installed.)

Known Caveats

Known caveats are unexpected behaviors or defects in Cisco software releases. They are graded according to severity level. This section contains information for known severity 1, 2, and 3 defects in this release of Cisco CRA.

If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release.

To access the Bug Toolkit, perform either of these actions:

- Go to this URL:
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
- Log in to Cisco.com, click **Technical Support**, then click **Tools & Utilities**, then click **Software Bug Toolkit** under Troubleshooting Tools

For information about issues relating to VoiceXML implementation, refer to the “VoiceXML Implementation for Cisco Voice Browser” appendix in *Cisco Customer Response Applications Developer Guide*.

Known caveats are listed under these components:

- [ASR Component, page 40](#)
- [Cisco CRA Editor Component, page 40](#)
- [Cisco CRA Installation Component, page 41](#)
- [Cisco ICD Component, page 41](#)

- [Documentation Component, page 54](#)
- [TTS Component, page 59](#)

ASR Component

Defect Number: CSCdy35922

Severity Level: 3

Component: ASR

Headline: Creating more ASR channels than licensed does not work.

Symptom: If you attempt to configure more ASR channels in one or more Nuance Dialog Control Groups than the number of licensed ASR channels on your system, the system will not create the ASR channels that exceed the number specified in the license. The system will create the ASR channels, up to the licensed limit, based on the order in which the system creates the Nuance Dialog Control Groups. The system will not notify you that the excess ASR channels were not created.

Condition: You attempt to configure more ASR channels in one or more Nuance Dialog Control Groups than the number of licensed ASR channels on your system

Workaround: Ensure that the total number of ASR channels that you create across all Nuance Dialog Control Groups does not exceed the number of ASR channels than are licensed.

Cisco CRA Editor Component

Defect Number: CSCdx71057

Severity Level: 3

Component: Cisco CRA Editor

Headline: A new help web page does not appear when a help page is open.

Symptom: You choose **Help** from a step's Properties window and the newly-selected help web page does not appear.

Condition: A help web page is already open.

Workaround: Close the existing help web page before opening a new one.

Cisco CRA Installation Component

Defect Number: CSCdz24819

Severity Level: 3

Component: Cisco CRA Installation

Headline: The installation program fails.

Symptom: The CRA installation program fails and the following InstallShield message appears when you exit the installation program: Please insert disk 0 that contains the file data3.cab.

Condition: A CD-ROM is corrupted or various files exist in the Windows temporary directory (%temp%).

Workaround: Make sure that you are using clean, unscratched CD-ROMs. Also, delete any files in the Windows temporary directory. Then run the installation program again.

Cisco ICD Component

Defect Number: CSCdz59921

Severity Level: 3

Component: Cisco ICD

Headline: IP Phone agent shown in Talking state after logoff.

Symptom: An IP Phone agent remains in Talking state after logging out of the IP phone while on a call. An active remote monitoring session for that agent will continue until the call ends. (In contrast, when an agent logs out of the Cisco Agent Desktop while on a call, the agent will be go to Logged-off state immediately and an active remote monitoring session will end immediately.)

Condition: Two or more IP phone agent are logged in when one of the agents logs out while on a call.

Workaround: None

Defect Number: CSCdz78378

Severity Level: 3

Component: Cisco ICD

Headline: VoIP autorecovery message should mention specific VoIP server IP address.

Symptom: When the Cisco Desktop VoIP Monitor Server service stops on one or more computers in an installation where this service is running on more than one computer, the computer on which this service stopped is not specified.

Condition: The Cisco Desktop VoIP Monitor Server service stops on one or more computers (because, for example, the computer resets or is rebooted).

Workaround: Use the Windows Services window to check the status of the Cisco Desktop VoIP Monitor Server service on each computer on which this service should be running.

Defect Number: CSCdz89970

Severity Level: 3

Component: Cisco ICD

Headline: Cisco Agent Desktop shows calling number unavailable after answering a conference.

Symptom: The Calling and the Called number fields in the Cisco Agent Desktop may not show the parties on the call.

Condition: The Cisco Agent Desktop does not currently track all call events and therefore at times is unable to display all of a call's information.

Workaround: None.

Defect Number: CSCea03689

Severity Level: 3

Component: Cisco ICD

Headline: Disabling Enterprise Data from the Cisco Agent Desktop Administrator should disable it for IP phone agent.

Symptom: Disabling Enterprise Data from the Cisco Agent Desktop Administrator does not disable enterprise data on an agent's IP phone screen.

Condition: Disabling Enterprise Data for agents from the Cisco Desktop Administrator

Workaround: Follow these steps:

1. Use a text editor to open this file:
C:\Program Files\Cisco\Desktop\IP Phone Agent Interface\config\AgtStateSvr.cfg
 2. Change the value of the Enterprise Data Pop parameter to 0.
 3. Save the file and exit the text editor.
 4. Stop and restart the Cisco Desktop TAI Server service.
-

Defect Number: CSCea04306

Severity Level: 3

Component: Cisco ICD

Headline: With TAI shutdown, ICD logs out one IP phone agent but not the other.

Symptom: IP phone agents continue to receive ICD calls but cannot change their agent states through the IP Phone Agent service.

Condition: Two or more IP phone agent are logged in to ICD. The Cisco Desktop Telephony Agent Interface (TAI) Server service has failed. (When the system detects this problem, it logs out the IP phone agent who logged in most recently

but does not log out other IP phone agents. If the agents who remain logged in have Auto-available enabled, they will continue to go to Ready state after ICD calls end and therefore continue to receive other ICD calls.)

Workaround: None.

Defect Number: CSCea20537

Severity Level: 3

Component: Cisco ICD

Headline: SA password change after installation needs registry update for sync.

Symptom: Agents who are added in Cisco CallManager after Cisco CRA is installed cannot log in to the Cisco Agent Desktop. These agents see the message `ID not found` when trying to log in.

Condition: You have manually changed the password for the database user ID “sa” after installing Cisco CRA and rebooting the CRA server.

Workaround: Reinstall Cisco CRA. If you want to change the sa account password, you can do so when the CRA installation prompts for a new sa account password.

Defect Number: CSCea28382

Severity Level: 3

Component: Cisco ICD

Headline: ICD cannot start or restart if Publisher is down.

Symptom: The Cisco Agent Desktop Server services will not start on the Cisco CRA server.

Condition: The primary LDAP is down. (The Cisco Agent Desktop Server services will not be able to start because they will not be able to write their connection information to LDAP.)

Workaround: Restart the primary LDAP.

Defect Number: CSCea32551

Severity Level: 3

Component: Cisco ICD

Headline: Agent cannot see chat messages during conference.

Symptom: The Chat window in the Cisco Agent Desktop does not display the latest message.

Condition: This problem can occur in these situations:

- The chat message area is too small to display messages.
- The agent is scrolling through a previous message.

Workaround:

- Make sure that the Chat window is large enough to display messages.
 - When finished reading a message, scroll to the bottom of the Chat window to view the most recent message.
-

Defect Number: CSCea33430

Severity Level: 3

Component: Cisco ICD

Headline: Agent can't go Ready after login under certain conditions.

Symptom: After logging in to the Cisco Agent Desktop, an agent receives the message `State change request failed` when trying to change to Ready state.

Condition: Occurs intermittently when the agent's phone goes out of service while agent is logging in. The agent may see the message reading `Init Successful` after logging in, but the status bar of the Cisco Agent Desktop would show `No Agent logged in` and `Not Ready` as the current state.

Workaround: Exit the Cisco Agent Desktop, restart it, and log in again.

Defect Number: CSCea33056

Severity Level: 3

Component: Cisco ICD

Headline: Monitoring an agent after LDAP failover takes long.

Symptom: When silently monitoring an agent, the voice stream takes long to start.

Condition:

- You have set up more than one ICD Call Monitoring Server and you have not explicitly assigned the agent extension to a particular monitoring server using VoIP Monitor Server Admin in the Cisco Desktop Administrator.
- The Primary LDAP server is inaccessible on the network.

Workaround: Assign each agent extension to an ICD Call Monitoring Server by choosing **Enterprise Data Configuration > VoIP Monitor** under the Logical Contact Center in Cisco Desktop Administrator. Establish a connection to the Primary LDAP server.

Defect Number: CSCea61018

Severity Level: 3

Component: Cisco ICD

Headline: Historical Reports leaks CRDR for Arbitrary Transfer/Conference scenarios.

Symptom: In some Arbitrary Transfer/Conference scenarios, a Call Routing Detail Record (CRDR) is not written.

Condition: This problem occurs under certain Arbitrary Transfer/Conference scenarios when an agent puts a call received on hold, places an independent call (to another route point, for example), goes back to the original call, and then presses the **Transfer** key twice to complete the transfer.

Workaround: Arbitrary Transfer/Conference is not supported in Cisco CRA 3.1.

Defect Number: CSCea66516

Severity Level: 3

Component: Cisco ICD

Headline: Session changes in middle of call even without the workflow doing so.

Symptom: Call data associated with a consult call initiated by an agent is not merged into call data associated with the original call connected to the agent.

Condition: An agent is on an ICD call that was routed to the agent and then the agent initiates a consult call. (In this case, the consult call does not have access to the data variables stored in the workflow Session object associated with the ICD call, although it should. If the agent calls a route point that sets data for this consult call and then completes a transfer or a conference, the data set for the consult call will not be merged into the final call and will be lost.)

Workaround: None.

Defect Number: CSCea80191

Severity Level: 3

Component: Cisco ICD

Headline: Japanese localization corruption on various screens.

Symptom: Double-byte characters do not appear correctly on the Cisco Desktop Administrator on a computer that is running the Windows NT or the Windows XP operating system.

Condition: Japanese characters have been entered using the Windows Input Method Editor (IME) on a computer that is running a Japanese or a Chinese version of the operating system. In this case, the characters will not appear correctly on the Cisco Agent Desktop Administrator. If these characters are stored in configuration file on the shared drive, they will also appear corrupted on the Cisco Agent Desktop.

Workaround: If text for the Cisco Agent Desktop Administrator needs to be modified, modify the text using Notepad, then copy the text from Notepad to the Cisco Agent Desktop Administrator.

Defect Number: CSCea81865

Severity Level: 3

Component: Cisco ICD

Headline: OrigCalledNumber in CCCR is blank in redirect to agent scenario.

Symptom: The origCalledNumber field in the ContactCallDetail record for a call is blank.

This problem will only affect Historical Reports that refer to the origCalledNumber field. It will not affect standard historical reports or other CTI clients such as screen pop applications that uses the origCalledNumber.

Condition: A call is made to an application that includes a Redirect step that redirects the call to a logged-in ICD agent. In this case, the ContactCallDetail record for the second leg of the call will contain a blank origCalledNumber field.

Workaround: None.

Defect Number: CSCea90780

Severity Level: 3

Component: Cisco ICD

Headline: Supervisor cannot stop recording an agent's call.

Symptom: An agent who initiates a recording cannot stop the recording

Condition: Agents A and B are on the same team and are on the same conference call. Then,

1. Supervisor Z, who is associated with the same team, starts recording Agent B.
2. Agent A also starts recording the call.
3. Supervisor Z selects Agent A and stops Agent A's recording.

Supervisor Z's Cisco Supervisor Desktop will then show Agent B as being recorded. However, the Cisco Supervisor Desktop icons will show Start Record as enabled and Stop Record as disabled.

Workaround: None. Agent B's recording will stop when the call ends.

Defect Number: CSCeb07043

Severity Level: 3

Component: Cisco ICD

Headline: Cisco Supervisor Desktop Italian client installation: no warning text shown on dialog box.

Symptom: No warning message appears in a dialog box when you install an Italian version of the Cisco Supervisor Desktop.

Condition: Installing an Italian version of the Cisco Supervisor Desktop on a computer on which the Cisco Agent Desktop has already been installed.

(If you are installing an English version of the Cisco Supervisor Desktop, you will see a dialog box with the message Install Manager has detected that the same version of software is already installed on this computer. Therefore, no software or configuration changes will be made. If you wish to make changes, remove Cisco Agent Desktop prior to running the installation. Do you wish to continue?. However, if you are installing an Italian version, the dialog box appears without the message—only the **Si** and **No** buttons appear.)

Workaround: Click **Si** and the installation will continue normally.

Defect Number: CSCeb17184

Severity Level: 3

Component: Cisco ICD

Headline: Reason codes deleted during upgrade.

Symptom: Installation of Cisco CRA 3.1 deletes existing reason codes.

Condition: Upgrading from Cisco CRA 3.0(x) to Cisco CRA 3.1.

Workaround: Before upgrading to Cisco CRA 3.1, run the Cisco Agent Desktop Administrator and write down the reason codes that are currently configured. After installing Cisco CRA 3.1, reenter these reason codes in the Cisco Agent Desktop Administrator.

Defect Number: CSCeb28769

Severity Level: 3

Component: Cisco ICD

Headline: Sync server DSN requires update after CRA IP address change

Symptom: Agents do not receive enterprise data after the Cisco CRA server IP address is changed.

Condition: You have changed the Cisco CRA server IP address and followed the steps in the workaround for defect number CSCdy82034 in the [“Documentation Component” section on page 54](#).

Workaround: Follow these steps:

1. On the Cisco CRA server, choose **Start > Programs > Administrative Tools > Data Sources (ODBC)**.
 2. Click the **System DSN** tab.
 3. Click **SYNC_SERVER_A** in the System Data Sources pane and click **Configure**.
 4. In the Server field, type in the new IP address of the Cisco CRA server and then click **Next**.
 5. In the Microsoft SQL Server DSN Configuration dialog box, enter the SQL user ID (which is sa) and the SQL password and then click **Next**.
 6. Click **Next** on the next dialog box that appears.
 7. Click **Finish** on the next dialog box that appears.
 8. In the ODBC Microsoft SQL Server Setup dialog box, click **Test Data Source** and verify that the operation completes successfully.
 9. Click **OK**.
 10. Stop and restart the Cisco Desktop Enterprise Server service and the Cisco Desktop Sync Server service from the Windows Services window.
-

Defect Number: CSCeb35499

Severity Level: 3

Component: Cisco ICD

Headline: Call is aborted when agent conferences gateway caller to route point (answer got exception).

Symptom: An agent conferences a gateway caller to the CRA ICD route point, the ICD application plays the system default prompt, and then it aborts the call. The debug trace shows that the CRA application received a PlatformException from the answer request.

Condition: Occurs intermittently when an agent is talking to a gateway caller.

Workaround: None.

Defect Number: CSCec04764

Severity Level: 3

Component: Cisco ICD

Headline: GetCallContactInfo step does not show the transferred arrival type.

Symptom: The Arrival Type for a call that is transferred to a trigger appears as Direct instead of as Transferred.

Condition: The workflow includes the Get Call Contact Info step.

Workaround: If the workflow has logic that takes action based on the arrival type, use different triggers for direct calls and transferred calls.

Defect Number: CSCec10743

Severity Level: 3

Component: Cisco ICD

Headline: CRA ICD Setup does not allow domain name for host in AD section.

Symptom: Cannot enter domain name during the installation of Cisco CRA when integrating with Active Directory.

Condition: Cisco CRA integrated with Active Directory.

Workaround: Follow these steps:

1. Install Cisco CRA with Active Directory. During the installation, enter a single IP address in the LDAP Host field in the ICD Directory Server Configuration Pane.



Note Perform the rest of this procedure before installing the Cisco Agent Desktop or the Cisco Supervisor Desktop.

2. Update the InstallManager.cfg and AdvancedManager.cfg files as follows:
 - a. Use a text editor to open each file. The files are in the folder `c:\program files\cisco\Desktop_config\Desktop\`.
 - b. In each file, set LDAP SERVER A to the Active Directory domain name.
 - c. In each file, set LDAP SERVER A Type to **HostName**.
 - d. Save each file.
 3. Open a DOS command window (choose **Start > Run**, type **cmd**, and click **OK**) and follow these steps:
 - a. Type **c:** and press Enter.
 - b. Type **cd \program files\cisco\desktop_config\util** and press Enter.
 - c. Type **dsbrowser /editable** and press Enter.
 - d. Enter the Directory Administrator username and password.
 - e. Expand **Server Data**.
 - f. Expand **CRA Server Name LCC**.
 - g. Expand **App Data**.
 - h. Select **LDAP list**.
 - i. Double-click **LDAP Host**.
 - j. Enter the Active Directory domain name and click **OK**.
-

Defect Number: CSCec14797

Severity Level: 3

Component: ICD

Headline: Cisco Agent Desktop cannot log in to Call/Chat server.

Symptom: An agent receives the message `Call Chat server is down and trying to recover`. The agent sees a blank Call / Chat window. In addition, supervisors cannot see the agent on the Cisco Supervisor Desktop and so cannot perform supervisor functions such as barge, intercept, recording, and monitoring. If this agent is also logged in as a Supervisor using the Cisco Supervisor Desktop, this supervisor can not barge or intercept any other agent's calls.

Condition: An IPCC Express agent logs in using Media Terminated Cisco Agent Desktop on a computer running the Windows 2000 Professional operating system.

Workaround: None.

Defect Number: CSCec16672

Severity Level: 3

Component: ICD

Headline: Enterprise data not seen after CRA IP address change.

Symptom: Agents do not receive enterprise data after the Cisco CRA server IP address is changed.

Condition: You have changed the Cisco CRA server IP address and followed the steps in the workaround for defect number CSCdy82034. (See the [“Documentation Component” section on page 54](#) for that workaround.)

Workaround: Follow these steps on the Cisco CRA Server:

1. Choose **Start > Programs > Administrative Tools > Data Sources (ODBC)**.
 2. Click the **System DSN** tab.
 3. Click **SYNC_SERVER_A** in the System Data Sources pane and click **Configure**.
 4. In the Server field, type in the new IP address of the Cisco CRA server and click **Next**.
 5. In the Microsoft SQL Server DSN Configuration dialog box, enter the SQL user ID (which is sa) and the SQL password and click **Next**.
 6. Click **Next** in the next dialog box that appears.
 7. Click **Finish** in the next dialog box that appears.
 8. In the ODBC Microsoft SQL Server Setup dialog box, click **Test Data Source** and verify that the operation completes successfully.
 9. Click **OK**.
 10. Stop and restart the Cisco Desktop Enterprise Server service and the Cisco Desktop Sync Server service from the Windows Services window.
-

Defect Number: CSCec25235

Severity Level: 3

Component: ICD

Headline: Call drops on trying to intercept after dropout of barge-in.

Symptom: When a supervisor tries to intercept a call, the is dropped.

Condition: An IPCC Express supervisor barges an IPCC Express agent's call. After talking to the agent and the caller, the Supervisor drops out of the call. The supervisor then intercepts the same call from the agent.

Workaround: Have the agent transfer the call to the supervisor after the supervisor drops out of the call.

Documentation Component

Defect Number: CSCdv26511

Severity Level: 3

Component: Documentation

Headline: Configuration procedure for Sybase Database should be Documented.

Symptom: The connection to the CRA database fails and the PARTIAL SERVICE appears for the database subsystem in the CRA Administration Engine Status web page.

Condition: The Sybase datasource name in the CRA Administration Enterprise Database Subsystem Configuration web page does not match exactly the datasource name in the Windows ODBC DSN configuration window.

Workaround: Change the datasource name in the CRA Administration Enterprise Database Subsystem Configuration web page to match the Windows ODBC DSN name.

Defect Number: CSCdy82034

Severity Level: 3

Component: Documentation

Headline: Document procedure to change IP address of CRA server.

Symptom: The CRA Engine will not come into service.

Condition: The IP address has been changed on the Cisco CRA server.

Workaround: To change the IP address on the Cisco CRA server, follow these steps:

1. From the Cisco CRA Administration web page, choose **System > Engine**, click **Stop Engine** in the Engine web page, and then exit Cisco CRA Administration.
2. Change the IP address on the Cisco CRA server to the new address.
3. Reinstall and configure Cisco CRA 3.1. (Do not uninstall Cisco CRA 3.1 before reinstalling it.) Make sure to also install the latest Service release. Do not reinstall the Speech Server now.

Refer to *Getting Started with Cisco Customer Response Applications 3.1* for installation instructions. Also see the [“Installing a Required Service Release” section on page 3](#) in these release notes.

4. From the Cisco CRA Administration web page, choose **System > Engine**, click the **Engine Configuration** hyperlink, enter the new Cisco CRA server IP address in the Application Engine Hostname field, and then click **Update**.
5. If you are using Cisco ICD, follow the procedure described in the “Updating the CAD Servers’ IP Address” section in *Cisco Desktop Product Suite 4.5 (ICD) Service Information*.
6. If you are using the Cisco IP Phone Agent service on Cisco CallManager, update the information in the Service URL field in the Cisco CallManager Administration Cisco IP Phone Services Configuration page with the new Cisco CRA server IP address.

7. If you are using Cisco CRA Historical Reports:
 - a. Stop the Cisco CRA Engine (see Step 1).
 - b. From the Cisco CRA Administration web page, choose **Tools > Historical Reporting**, click the **Database Server Configuration** hyperlink, and then click **Update**.
 - c. Start the Historical Reports Client, click **Server** in the Login dialog box, and change the server IP address to the new Cisco CRA server IP address.
8. If you are using the ICM subsystem on the Cisco CRA server, change the VRU PIM configuration to point to the new Cisco CRA server IP Address.
9. On each client computer from which you run real-time reports, point the web browser to the new Cisco CRA server IP Address.
10. If you have installed Nuance ASR on one or more dedicated servers, follow these steps on each such dedicated server:
 - a. Choose **Start > Programs > Administrative Tools > Data Sources (ODBC)**.
 - b. Click the **System DSN** tab.
 - c. Click **wfnuance** in the System Data Sources pane and click **Configure**.
 - d. In the Server field, type in the new IP address of the Cisco CRA server and then click **Next**.
 - e. In the Microsoft SQL Server DSN Configuration dialog box, make sure that this radio button is selected: **With SQL Server authentication using a login ID and password entered by the user**.
 - f. Also in the Microsoft SQL Server DSN Configuration dialog box, enter **nuance** in the password field and then click **Next**.
 - g. Click **Next** on the next dialog box that appears.
 - h. Click **Finish** on the next dialog box that appears.
 - i. In the ODBC Microsoft SQL Server Setup dialog box, click **Test Data Source** and verify that the operation completes successfully.
 - j. Click **OK**.

**Note**

You do not need to take any action for Nuance TTS.

11. Reboot the Cisco CRA server.

**Note**

Before logging in to the Cisco Agent Desktop or in to the Cisco Supervisor Desktop, choose **Start > Run** on the computer on which you are running either of these programs and enter the following command, where *new_ip* is the new IP address of the Cisco CRA server: \\new_ip\DESKTOP_CFG\desktop\.

Defect Number: CSCeb04994

Severity Level: 3

Component: Documentation

Headline: Help for Extended Get Digit String and Extended Play Prompt string are swapped.

Symptom: In the CRA Step Editor online Help, clicking on the Extended Get Digit string or Extended Play Prompt string brings up the help topic for the other.

Condition: Cisco CRA 3.0 and 3.1.

Workaround: For the Extended Get Digit string, see the Help topic for the Extended Play Prompt string. For the Extended Play Prompt string, see the help topic for the Extended Get Digit String.

Defect Number: CSCeb09612

Severity Level: 3

Component: Documentation

Headline: Share access may be denied if the Cisco CRA server is infected with a virus.

Symptom: Access to the desktop_cfg share folder on the Cisco CRA server is denied from client computers that are running the Cisco Agent Desktop or the Cisco Supervisor Desktop.

Condition: The Cisco CRA server is infected with virus and Netshield is set to respond as follows when a virus is detected: Disconnect remote users and deny access to network share. (This setting is the default setting and causes access to share to be removed when a virus is detected.)

Workaround: Follow these steps:

1. On the Cisco CRA server, right-click the desktop_config folder.
 2. Choose **Sharing**.
 3. In the Properties window, click **Permissions**.
 4. In the Permissions, window, click Administrator in the Name area.
 5. Click **Remove**.
 6. Click **OK**.
-

Defect Number: CSCeb30665

Severity Level: 3

Component: Documentation

Headline: No documentation for how grammar is selected in multi grammar file.

Symptom: There is no documentation for VXML Scripts using grammar files with more than one rule, so you do not know which rule is used to start the recognition.

Condition: Cisco CRA 3.1

Workaround: In a grammar file that has more than one rule, recognition starts at the last rule in the file. Make sure the starting rule is at the end of the file.

Defect Number: CSCeb59540

Severity Level: 3

Component: Documentation

Headline: Set Session Info with ccdrVar is not documented correctly.

Symptom: You are not able to write custom variables into ContactCallDetailRecord using the Set Session Info step.

Condition: Cisco CRA 3.1

Workaround: An attribute name should be begin with one underscore, not two underscores. Attribute names are _ccdrVar1 through _ccdrVar5.

TTS Component

Defect Number: CSCeb60021

Severity Level: 3

Component: TTS

Headline: Vocalizer 3.0 - read time out exception.

Symptom: When using Nuance Vocalizer 3.0, the CiscoMIVRn.log file contains the exception `Read timed out with the message PROMPT_STREAM_ERROR_IGNORED`. The TTS prompt that encounters this error is skipped and the next step in the workflow is executed.

Condition: The Vocalizer 3.0 engine did not respond to a TTS request within the configurable time out period (the default timeout period is 5 seconds).

Workaround: Take one of these actions:

- Set the Continue on Prompt Errors step to Yes in the workflow. In this case, if the TTS prompt encounters an error, the error is logged but ignored, and the workflow continues with the next step.
 - Set Continue on Prompt Errors to No in the workflow and configure the workflow to play a prompt if the TTS prompt encounters an error.
 - Edit the TTS.properties file (located by default in the C:\Program Files\wfvavvid folder) and increase the value for the TTSTimeoutMs key. Make sure to enter a value that will not seem excessively long to callers.
-

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, 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 send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments 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.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — 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.

- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.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.

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)—Your 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 operation 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 your network is impaired, but 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.

- 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>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.