



Release Notes for Cisco Customer Response Applications 3.5(4)

October 15, 2008

These release notes are for use with Cisco Customer Response Applications (Cisco CRA) Release 3.5(4) 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/en/US/products/sw/custcosw/ps1846/prod_release_notes_list.html

Effective with release 3.0, Cisco Customer Response Applications (CRA) has been renamed Cisco Customer Response Solutions (CRS), and the following product names have been changed:

- IP ICD (IP Integrated Contact Distribution) is now IPCC Express (IP Contact Center Express)
- IP ICD Standard is now IPCC Express Standard
- IP ICD Enhanced is now IPCC Express Enhanced
- IP ICD Enhanced with CTI Option is now IPCC Express Premium



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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

The Cisco website and packaging materials have been updated to reflect the new names, but the user interface, and therefore the documentation, have not.

Contents

- [What's New in Cisco CRA Release 3.5\(4\), page 3](#)
- [Late-Breaking Information, page 3](#)
- [Upgrade Notes, page 11](#)
- [Removal of off-board VOIP Monitoring server, page 11](#)
- [Obtaining Double-Byte Data in a Cisco CRA Script, page 14](#)
- [Unsupported and Supported Actions for Cisco ICD Agents, page 14](#)
 - [Unsupported Actions for Cisco IP ICD Agents, page 14](#)
 - [Supported Configurations for Agent Phones, page 15](#)
 - [Unsupported Configurations for Agent Phones, page 16](#)
- [Unsupported Features in Cisco CallManager, page 16](#)
- [Upgrading from Nuance Vocalizer 1.0 to Nuance Vocalizer 3.0, page 17](#)
- [Changing the IP Address of a Cisco CRA Server, page 19](#)
- [Entering a Datasource Name in Cisco CRA Administration, page 21](#)
- [Contact Dispositions in Cisco CRA Real-Time Reports and Historical Reports, page 22](#)
- [Cisco CRA Historical Reports Upgrades and Enhancements, page 23](#)
- [Sharing Cisco CRA Historical Reports on the Web, page 30](#)
- [Adding a 15-Minute Interval Length to a Cisco CRA Historical Report Filter Parameter, page 32](#)
- [Selecting Languages for ASR, page 34](#)
- [Using Cisco CRA Clients with Microsoft Windows XP-SP2, page 35](#)
- [Features Available with Each Product Package, page 40](#)
- [Related Documentation, page 42](#)
- [Caveats, page 43](#)

- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 49](#)

What's New in Cisco CRA Release 3.5(4)

- Support for Cisco CallManager version 4.2
- Resolved caveats, including those described in the [“Resolved Caveats” section on page 44](#)

Late-Breaking Information

This section provides important information that is not included in the Cisco CRA documentation.

- For current information about supported products for Cisco CRA, refer to *Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide*, which is available at this URL:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html

- If you are performing a new coresident installation of Cisco CRA (an installation in which Cisco CRA and Cisco CallManager reside on the same server), make sure to apply this hotfix:

OS_Hotfix_for_CCM4.x_co-res_CRS3.5.x.exe

This hotfix is available at this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/crs35>

If you do not apply this hotfix, the Cisco CallManager Administration application may not start or some Cisco CallManager or Cisco CRA services may not start.

- 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 3.5(4), you must upgrade the Cisco Agent Desktop and the Cisco Supervisor Desktop to release 4.5.7.4 after you upgrade Cisco CRA.
- When you install or upgrade Cisco CRA in a co-resident scenario (where Cisco CRA and Cisco CallManager reside on the same server), a dialog box will appear that asks you to continue in mixed mode. When you see this dialog box, click **Yes** to continue. In this way, Cisco CRS can connect to the SQL server database using SQL authentication.
- Cisco CRA 3.5(4) is compatible with McAfee VirusScan Enterprise 7.0.
- 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/en/US/products/sw/custcosw/ps1844/prod_bulletins_list.html
- **Policy Changes in New Zealand Daylight Savings Time**—To know about the policy changes in New Zealand daylight savings time and to understand the impact on Unified CCX, refer to the field notice FN - 62880 - New Zealand Daylight Savings Time Policy Changes Effective September 2007 - For Cisco Unified Contact Center Express (Unified CCX), which is available at this URL:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_field_notice09186a00808b40b7.shtml
- **Redirection to translation patterns not supported**—CRS does not support the use of consult transfer/redirect step from scripts to a translation pattern that maps back to a route point.
- 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**.
 - d. If you made any change to the CiscoCRAServletEngine service properties in Step b or to the Cisco CRA Engine service properties in Step c, restart the service to cause the changes to take effect.
- If you are using a proxy service in Internet Explorer on the CRA Historical Reports client system, scheduled historical reports might not run and you might see this message in the CiscoSch.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**.
The Use a Proxy Service check box will be checked if you are using a proxy server.
 - 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.
- If you create a custom report as described in *Creating Custom Reports for Cisco Customer Response Applications*, you must use Crystal Reports version 8.5 to create and save the report.

- 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/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html

- The JTAPI Client Update Tool synchronizes the Cisco CallManager Plugin with Cisco CRA and the Cisco Agent Desktop (CAD). You must run this tool from the Cisco CRA Server whenever you update Cisco CallManager. For detailed information about the JTAPI Client Update Tool, refer to *Cisco Customer Response Applications Administrator Guide*, which is available at this URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html#anchor1

- Cisco CRA does not support the use of child domains with Active Directory.
- 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.

- The only supported username for the Windows account on a server that is running Cisco CRS is Administrator. If you use another user name, the CRSAdminUtil.exe tool may not work properly.
- 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.
- An ICD Call Recording and Monitoring Server can support up to 32 simultaneous monitoring and recording sessions.
- An ICD Call Statistics, Recording, and Monitoring Server checks the maximum number of concurrent recordings. If it reaches the limit of 32, it will not allow any more recordings to be made.
- Attempting to generate a scheduled custom report fails with the error “Invalid name” when the showUserNameOnReport parameter is set to 1 in the Historical Reports hrcConfig.ini file. To work around this problem, add the label @\$UserName to the .rpt report file that you create with Crystal Reports. To determine where to place this attribute, look at the definition file for any of the Cisco-provided historical reports.
- If you are using Cisco CRS Historical Reports client software, it must be the same version as the version of Cisco CRS that you are running.
- To access the CRA User Options pages or the CRA Supervision pages, you must use Microsoft Internet Explorer 5.x or 6.x.
- To install the required patch for the Cisco Agent Desktop and the Cisco Supervisor Desktop, perform the following steps. This procedure installs a patch that fixes the problem identified by CSCsa74890. Perform this procedure on all computers on which the Cisco Agent Desktop or the Cisco Supervisor Desktop are installed.

**Note**

The patch applies to English versions of the Cisco Agent Desktop only. It cannot be deployed for other languages.

You cannot uninstall the patch after you install it. If you want to remove the patch, you must uninstall and then reinstall the Cisco Agent Desktop or the Cisco Supervisor Desktop.

Before you install the patch, make sure that you have installed Service Release 3 on the Cisco CRS server as explained earlier in this Readme file for that service release.

Procedure

- a. Exit the Cisco Agent Desktop or the Cisco Supervisor Desktop.
 - b. Choose **Start > Run**.
 - c. In the Run dialog box, type `\\appsserver\desktop_cfg\desktop` and click **OK** to open the share folder.
 - d. Double-click HotFix.exe.
 - e. Start the Cisco Agent Desktop or the Cisco Supervisor Desktop.
- BARS 4.0(9) is compatible with Cisco CRS 3.5(4). However, when BARS 4.0(9) starts, you see this message: The Version of CRS installed CRS 3.5(4) has not been verified to function with BAR 4.0.9000, you should upgrade the BARS software to ensure complete compatibility. You can ignore this message.
 - If there is a firewall between the Cisco CRA Server and the LDAP server, make sure that the firewall allows ICMP connectivity between these servers.
 - The following information applies to the information in the Cisco CRA SRND:

The Cisco CRS Installer requires ICMP access to the LDAP server. If ICMP is not configured between Cisco CRA and the LDAP server, the installation fails.
 - If you change the LDAP for your installation (for example, if you change from DC-Directory to Microsoft Active Directory), you must use Cisco CRA Application Administration to reconfigure your Cisco CRA data.
 - The Cisco CRS Installer uses the Internet Control Message Protocol (ICMP).

- In Cisco CRS 3.5, the ICD Call Recording and Monitoring server is optional. However, ICD Call Statistics, Recording, and Monitoring Server required for agents and supervisors to obtain statistics and reports and if you will upgrade to Cisco CRR 4.0(x).
- For information about updating the license count in Cisco CRA 3.5, refer to the document at this URL:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_tech_note09186a008027f7c2.shtml
- When setting up a system that supports automatic speech recognition (ASR), Voice Activity Detection (VAD) should not be enabled anywhere in the network in which voice traffic will be transmitted if that traffic is routed to a Cisco CRS server with ASR.
- Installing BARS 4.0(9) SR1 install is not supported on a Cisco CRS server that is configured as a BARS target.
- To migrate from DC Directory to Microsoft Active Directory, follow these general steps:
 - a. Follow the instructions at the following link to uninstall the Cisco Agent Desktop:
http://cco/en/US/products/sw/custcosw/ps1846/products_tech_note09186a008020880a.shtml
 - b. Reinstall Cisco CRS, which reinstalls the Cisco Agent Desktop with the correct LDAP information and populates the new LDAP with information that the Cisco Agent Desktop requires.
 - c. Uninstall and then reinstall all Cisco Agent Desktop applications.
- If you change the Windows Administrator Password, you must make the same change to the password of each Cisco CRS service that runs under the Windows Administrator account.
- The *CRS Installation Guide* states that, if Cisco CRS co-located with Cisco CallManager, you can configure a maximum of 256 CTI ports. This statement should instead say that you can configure a maximum of 10 CTI ports.
- The CRS Administrator guide states that, in the Directory Port Number field, the default port number of the Cisco IP telephony directory is 8480. This statement should instead say that the default is 8404.
- When performing general troubleshooting Cisco CRS, verify that there is network connectivity to the CRA server.

- When generating a historical report that includes Not Ready codes, be aware that not ready codes are system wide and cannot be configured to be hidden from certain agents.
- It is normal for the following CRA subsystems to be in Partial service if the subsystems are not configured. They will only be in service if you have configured the server to use them.
 - Database subsystem—In service only if you have configured an external database for something such as a database dip when a call come in.
 - MRCP ASR subsystem—In service only if you have configured an ASR system for use with CRA.
 - MRCP TTS subsystem—In service only if you have configured a TTS system for use with CRA.
 - VOIP Monitor subsystem—In service only if you have completely configured monitoring and recording on your server for monitoring and recording of agents.
- The following information applies when you use the Place Call Step as described in the “Working with Multiple Contacts” chapter in *Cisco Customer Response Applications Developer Guide*:
 If the RNA timeout in the script is longer than the CFNA timer of Cisco CallManager, the agent phone goes to Not Ready state after a ring-no-answer. To resolve this issue, change the timeout value in the script to a lower than the CFNA in Cisco CallManager.
- The following section should be added to the “CRS Administration Problems” section:

Callers hear a fast busy while calling the JTAPI triggers

Symptom: While calling the JTAPI triggers, callers hear a fast busy and the following message appears in the MIVR log:

```
%MIVR-SS_TEL-7-UNK:Call.rejected(TRIGGER_MAX_SESSION)
```

Recommended Action:

1. Delete and then add back the trigger
 2. Restart CRS node manager.
- The following note applies to the “The Add a New Prompt Hyperlink” section in the “The Tools Menu” chapter in *Cisco CRS Administrator Guide*:

If you receive the error “The page cannot be displayed” in Cisco CRA Administration when trying to upload a large prompt .wav file, manually move the file to the repository to resolve the issue.

- You can use a custom script or the Cisco CRA Administration to upload a prompt.
- The following information applies to the description of the Call Redirect Step in the “Designing an IP IVR Scrip” chapter:

Adding a 2 second delay is a best practice when you have a script that performs a a transfer or redirect to another script. Without the delay, there will be a timing issue. When a transfer or redirect occurs, a call leg is initiated. If the transfer or redirect completes and then another transfer or redirect occurs, the call leg from the second transfer or redirect can get stuck. In this case, the second transfer or redirect fails. Adding a delay ensures that the second transfer or redirect leg can complete before continuing through the script.

- Hyperthreading is not supported by Microsoft Windows 2000 and 2003 and is disabled by default in Cisco-provided operating systems.

Upgrade Notes

To upgrade from Cisco CRS 3.5(x) to 3.5(4), use the Cisco CRS 3.5(4) CD. Follow the on-screen instructions to perform the upgrade. For additional information, refer to *Getting Started with Cisco Customer Response Applications*.

Removal of off-board VOIP Monitoring server

Please perform the following steps to remove off-board VOIP monitoring server:

- If the off-board VOIP Monitoring server exists but you decide not to upgrade that server, uninstall the VOIP Monitoring component from that server by using "Add or Remove Programs" in the Windows Control Panel. Uninstall the "Desktop VOIP Server" entry followed by the "Desktop Base" entry.

- Navigate to the LDAP directory server and remove the off-board VOIP Monitoring server by browsing to ldapRoot-->o=cisco.com-->ou=CCN Apps-->ou= <server hostname>LCC --> servers. Delete the server entry that has the off-board VOIP Monitoring server installed on it.

**Note**

Please exercise caution when you are deleting information in the LDAP Directory.

Cisco CRS 3.5 Admin Password Utility

With Cisco CallManager 4.x releases, the Cisco CallManager database uses NT authentication instead of mixed mode authentication. With this change, any service that accesses the Cisco CallManager database must be a valid NT user on the Cisco CallManager server, with privileges set for accessing the Cisco CallManager database.

These Cisco CRA services run under the CCMSERVICE NT user account, which provides access to Cisco CallManager Database:

- Cisco Desktop Sync Server
- Cisco Desktop VoIP Monitor Server (installed with Cisco IP ICD enhanced license)

If the password for the Cisco CallManager CCMSERVICE NT account is changed using Cisco CallManager AdminUtility, the password change must be applied to the Cisco Desktop Sync Server and the Cisco Desktop VoIP Monitor Server services. Otherwise, they will not be able to access the Cisco CallManager database. The Cisco CRS CRSAdminUtil utility applies the password change to these services. This utility is stored in the C:\Program Files\Cisco\Bin directory on a server that is running Cisco CRA.

It is not necessary to use the CRSAdminUtil utility on a co-resident server (a server on which Cisco CRA and Cisco CallManager are installed on the same server). On a co-resident server, the Cisco CallManager AdminUtility changes the password of the CCMSERVICE account, applies the new password to the Cisco Desktop Sync Server service and to the Cisco Desktop VoIP Monitor Server service (if present), and restarts these services automatically.

In other deployments, when you use the Cisco CallManager AdminUtility, you should run the CRSAdminUtil utility as follows:

- In a standalone deployment (In which Cisco CRA and Cisco CallManager are installed on the separate servers), run the CRSAdminUtil utility on the Cisco CRS server. This process will restart the Cisco Desktop Sync Server and the Cisco Desktop VoIP Monitor Server services, if they are running.
- If your deployment includes a dedicated ICD Call Statistics, Recording, and Monitoring Server or ICD Call Recording and Monitoring Servers, run the CRSAdminUtil utility on each of these servers. This process will restart the Cisco Desktop VoIP Monitor Server service on the server, if the service is running.

To run the CRSAdminUtil utility, follow these steps:

Procedure

-
- Step 1** Open a command window.
- Step 2** In the command window, enter this command and then press **Enter**:
- ```
cd C:\Program Files\Cisco\Bin
```
- Step 3** Enter this command and then press **Enter**:
- ```
CRSAdminUtil -u CCMSERVICE -p password_phrase
```
- Replace *password_phrase* with the password phrase you entered when you used the Cisco CallManager AdminUtility to change Cisco CallManager NT accounts password.
- If you enter different a password phrase, the CRSAdminUtil utility will generate a password that does not match the password that was generated by the Cisco CallManager AdminUtil, and the Cisco Desktop Sync Server and the Cisco Desktop VoIP Monitor Server services will not be able to access the Cisco CallManager database. In this case, run the CRSAdminUtil utility again, making sure to enter the correct password phrase.
- Step 4** Enter the Windows system administrator password for the server on which you are running the CRSAdminUtil utility when prompted.
- Step 5** Enter y when prompted to confirm that you want to change the password phrase.

CRSAdminUtil utility generates a strong password using the password phrase that you entered, applies the password to the CCMSERVICE NT user account, and applies the password to the Cisco Desktop Sync Server and the Cisco Desktop VoIP Monitor Server services. If these services are running, the CRSAdminUtil restarts them.

Obtaining Double-Byte Data in 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.

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

Use of the following softkeys on a Cisco IP Phone is not supported:

- **Barge**
- **cBarge**

- **DirTrfr**
- **GPickup**
- **iDivert**
- **Join**
- **MeetMe**
- **Park**
- **Pickup**

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/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html

The following configurations are supported for agent phones:

- An ICD extension configured on a single device (but not on multiple devices).
- An ICD extension configured in a single device profile (but not in multiple device profiles).
- Multiple agents sharing the same ICD extension, which you can set up as follows:
 - a. Configure the ICD extension on a single phone (not in a device profile).
 - b. Associate that phone with each agent who will use that extension.
 - c. Select the appropriate directory number (DN) as the ICD extension for each agent.

In this configuration, only one agent at a time can be logged in.



Note

All agents that currently have the ICD extension to be shared must log out before you can configure additional agents to share that extension.

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.
- An ICD extension assigned to multiple devices.
- 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.)
- In the Cisco CallManager Administration Directory Number Configuration web page for each ICD line, setting Maximum Number of Calls to a value other than 2.
- In the Cisco CallManager Administration Directory Number Configuration web page for each ICD line, setting Busy Trigger to a value other than 1.
- Configuring a Cisco IP Phone with SRTP on.
- 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

The following Cisco CallManager features are not supported by Cisco CRA 3.5(4). These features are disabled by default and should not be enabled for Cisco CRA. For more information about these features, refer to the Cisco CallManager documentation.

- Block External to External Transfer.
- Drop Adhoc Conference When Creator Leaves.
- Multilevel precedence and preemption (MLPP).

- Q Signalling (QSIG) Path Replacement (PR).

This feature must be disabled when Cisco CRS is deployed. To disable this feature, set the Cisco CallManager service parameters Path Replacement Enabled and Path Replacement on Tromboned Calls to False.

- Forced Authorization Code and Client Matter Code.

Because these feature can be enabled per route pattern, they should be turned off for all route patterns in the Cisco CallManager cluster that Cisco CRS might use. Enabling these features for route patterns that Cisco CRS does not use will not affect Cisco CRS.

In addition, do not use Cisco CallManager Administration to configure shared lines for CTI ports and for CTI route points.

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 3.5*.

Step 3 Install Cisco CRA on the Cisco CRA Server.

For instructions, refer to *Getting Started with Cisco Customer Response Applications 3.5*.

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 3.5*.



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 in *Getting Started with Cisco Customer Response Applications 3.5*.

- Step 6** Install the Nuance Speech Server software on the Cisco CRA server using Cisco Customer Response Solutions CD-ROM 5.
- For instructions, refer to the “Installing Nuance ASR and TTS” in *Getting Started with Cisco Customer Response Applications 3.5*.
- 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*.
-

Changing the IP Address of a Cisco CRA Server

To change the IP address on the Cisco CRA server, perform the following steps. If you do not follow these steps when you change the IP address, the CRA Engine will not come into service.

Procedure

-
- Step 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.
- Step 2** Change the IP address on the Cisco CRA server to the new address.
- Step 3** Reinstall and configure Cisco CRA 3.5. (Do not uninstall Cisco CRA 3.5 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 3.5* for installation instructions.

- Step 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**.
- Step 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 4.5.5 (ICD) Service Information*.
- Step 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.
- Step 7** If you are using Cisco CRA Historical Reports:
- Stop the Cisco CRA Engine (see [Step 1](#)).
 - From the Cisco CRA Administration web page, choose **Tools > Historical Reporting**, click the **Database Server Configuration** hyperlink, and then click **Update**.
 - 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.
- Step 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.
- Step 9** On each client computer from which you run real-time reports, point the web browser to the new Cisco CRA server IP Address.
- Step 10** If you have installed Nuance ASR on one or more dedicated servers, follow these steps on each such dedicated server:
- Choose **Start > Programs > Administrative Tools > Data Sources (ODBC)**.
 - Click the **System DSN** tab.
 - Click **wfnuance** in the System Data Sources pane and click **Configure**.
 - In the Server field, type in the new IP address of the Cisco CRA server and then click **Next**.
 - 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**.
 - 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.

Step 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\.

Entering a Datasource Name in Cisco CRA Administration

If the datasource name in the Cisco CRA Administration Enterprise Database Subsystem Configuration web page does not match exactly the datasource name in the Windows ODBC DSN configuration window, the connection to the CRA database will fail and the message `PARTIAL SERVICE` appears for the database subsystem in the Cisco CRA Administration Engine Status web page.

To workaroud this problem, change the datasource name in the Cisco CRA Administration Enterprise Database Subsystem Configuration web page to match the Windows ODBC DSN name.

Contact Dispositions in Cisco CRA Real-Time Reports and Historical Reports

The following notes will help clarify information regarding contact dispositions on various Cisco CRA real-time reports and historical reports.

- Many real-time and historical reports show the disposition of a call. CSQ reports show the disposition as Handled, Abandoned, or Dequeued. Other reports show the disposition as Handled or Abandoned.
- A contact that is queued and answered by an agent will show as handled in real-time and in historical reports.
- A contact that is queued but abandoned before it is answered by an agent will be shown as handled in the Overall IP ICD Stats real-time report if a SetContactInfo step in the workflow marks the call as handled. The call will be shown as abandoned otherwise. The CSQ IP ICD Stats real-time report will show the call as abandoned in both cases because it does not consider the SetContactInfo step.
- The historical CSQ reports take into account whether a contact is marked as handled by the SetContactInfo step to determine if a contact is dequeued. The CSQ IP ICD Stats does not consider the SetContactInfo step. Therefore, if a call is queued, then marked as handled, and then disconnects, the historical CSQ reports will show the call as dequeued and the real-time CSQ IP ICD Stats report will show it as abandoned.
- If the Dequeue step is used, the CSQ historical reports will show a contact as dequeued for each CSQ that it was dequeued from, but only if the contact is marked as handled. If a call is dequeued (by the Dequeue step), and then disconnects without being marked handled, the CSQ historical reports will show the contact as abandoned.
- If a call is dequeued using the Dequeue step and the caller drops, the CSQ IP ICD Stats real-time report will show the call as dequeued. If a call is dequeued from CSQ1 and is eventually handled by CSQ2, the CSQ IP ICD Stats report will show the call as dequeued for CSQ1 and handled for CSQ2. If a call is queued on multiple CSQs and is eventually handled by CSQ1, the CSQ IP ICD Stats report will show the call as handled for CSQ1 and dequeued for all other CSQs.

Cisco CRA Historical Reports Upgrades and Enhancements

This section describes enhancements to Cisco CRA Historical Reports that are not yet documented in *Cisco CRA Historical Reports User Guide*. These enhancements were added in previous Cisco CRA 3.1 or 3.5 releases and are currently available in English only.

**Note**

This section describes only the changes that are applicable to the existing Cisco CRA Historical Reports User Guide, Release 3.0 available at the URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_user_guide_book09186a00800e68e8.html

This section includes the topics:

- [Abandoned Call Detail Activity Report, page 24](#)—Describes new fields in this report
- [Agent Detail Report, page 24](#)—Describes new fields in this report
- [Agent Login Logout Activity Report, page 24](#)—Describes new fields in this report
- [Agent State Summary Report \(by Agent\), page 24](#)—Describes new fields in this report
- [Agent State Summary Report \(by Interval\), page 25](#)—Describes new fields in this report
- [Call Custom Variables Report, page 25](#)—Describes new filter parameters in this report
- [Common Skill Contact Service Queue Activity Report \(by Interval\), page 26](#)—Describes this new report
- [Detailed Call by Call CDR Report, page 27](#)—Describes new filter parameters in this report
- [Detailed Call, CSQ, Agent Report, page 27](#)—Describes this new report

Abandoned Call Detail Activity Report

- This report displays up to three skills for the CSQ to which the call was routed. (This enhancement was added in Cisco CRA 3.1(1).)
- The Average Time to Abandon field has been added to this report.

Time to abandon is the duration from the time when the call comes to the system to the time when the call is abandoned. Average time to abandon is the average value for all calls abandoned during the report range. The format is hh:mm:ss.

Agent Detail Report

This report displays up to three skills for the CSQ to which the call was routed. (This enhancement was added in Cisco CRA 3.1(1).)

Agent Login Logout Activity Report

The following fields have been added to this report:

- Extension—Cisco ICD extension that the Cisco CallManager assigned to the agent.
- Logout Reason Code—Reason code that the agent enters when the agent logs out from the Cisco Agent Desktop. A value of –1 indicates that no logout reason code is configured or that the agent was unable to enter a reason code.
- Grand Total—Total logged-in duration for all agents during the report period.

Agent State Summary Report (by Agent)

The Grand Total field has been added to this report. If the report is generated with 30-minute or 60-minute intervals, the grand total displays the total for all agents for all intervals during the report period. If the report is generated with the entire report range, the grand total displays the same values as the summary line. The grand total includes total logged-in time, total and percentage not ready time, total and percentage ready time, total and percentage reserved time, total and percentage talk time, and total and percentage work time.

Agent State Summary Report (by Interval)

The Grand Total field has been added to this report. If the report is generated with 30-minute or 60-minute intervals, the grand total displays the total for all agents for all intervals during the report range. If the report is generated with the entire report range, the grand total displays the same values as the summary line. The grand total includes total logged-in time, total and percentage not ready time, total and percentage ready time, total and percentage reserved time, total and percentage talk time, and total and percentage work time.

Call Custom Variables Report

The following filter parameters have been added to this report:

- Original Called Number—Displays information for the specified original called number(s).
- Called Number—Displays information for the specified called number(s).
- Calling Number—Displays information for the specified calling number(s). Calling number is the same as Originator DN.
- Application Name—Displays information for the specified application name(s).
- Contact Type—Displays information for the specified contact type(s) (incoming, outgoing, or internal).
- Originator Type—Displays information for the specified originator type(s) (agent, device, or unknown).
- Destination Types—Displays information for the specified destination type(s) (agent, device, or unknown).
- Duration Greater Than or Equal to T seconds—Displays calls with duration greater than or equal to the number of seconds specified by T.
- Duration Less Than or Equal to T seconds—Displays calls with duration less than or equal to the number of seconds specified by T.
- Custom Variable 1—Enter a whole string or substring to search for. Separate multiple strings with commas. When this filter parameter is specified, the report displays calls for which Custom Variable 1 contains the string or any of the substrings entered.

- Custom Variable 2—Enter a whole string or substring to search for. Separate multiple strings with commas. When this filter parameter is specified, the report displays calls for which Custom Variable 2 contains the string or any of the substrings entered.
- Custom Variable 3—Enter a whole string or substring to search for. Separate multiple strings with commas. When this filter parameter is specified, the report displays calls for which Custom Variable 3 contains the string or any of the substrings entered.
- Custom Variable 4—Enter a whole string or substring to search for. Separate multiple strings with commas. When this filter parameter is specified, the report displays calls for which Custom Variable 4 contains the string or any of the substrings entered.
- Custom Variable 5:—Enter a whole string or substring to search for. Separate multiple strings with commas. When this filter parameter is specified, the report displays calls for which Custom Variable 5 contains the string or any of the substrings entered.
- Any Custom Variable—Enter a whole string or substring to search for. Separate multiple strings with commas. When this filter parameter is specified, the report displays calls with any of the five custom variables containing the string or any of the substrings entered.

Common Skill Contact Service Queue Activity Report (by Interval)

As of Cisco CRA 3.1(1), 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.

Detailed Call by Call CDR Report

The following filter parameters have been added to this report:

- Original Called Number—Displays information for the specified original called number(s).
- Called Number—Displays information for the specified called number(s).
- Calling Number—Displays information for the specified calling number(s). Calling number is the same as Originator DN.
- Application Name—Displays information for the specified application name(s).
- Contact Type—Displays information for the specified contact type(s) (incoming, outgoing, or internal).
- Originator Type—Displays information for the specified originator type(s) (agent, device, or unknown).
- Destination Type—Displays information for the specified destination type(s) (agent, device, or unknown).
- Duration Greater Than or Equal to T seconds—Displays calls with duration greater than or equal to the number of seconds specified by T.
- Duration Less Than or Equal to T seconds—Displays calls with duration less than or equal to the number of seconds specified by T.

Detailed Call, CSQ, Agent Report

This new report has been added.

The Detailed Call, CSQ, Agent Report includes this chart:

- Total Calls by Called Number—Displays the total number of calls to each called number.

The Detailed Call, CSQ, Agent Report includes these fields:

- Session ID - Sequence No.—Session ID is the unique session identification number that the system assigned to a call. Sequence No. is the session sequence number that the system assigned to each call leg. The session sequence number increases by 1 for each leg of a call.
- Call Start Time—Date and time that the call started.

- **Call End Time**—Date and time that the call was disconnected or transferred.
- **Contact Disposition**: Disposition of a call (abandoned or handled)—For an ICD call, the call is abandoned if the call disconnects before connecting to an agent. The call is handled when the call is connected to an agent. For an IVR call, the call is abandoned if it does not reach the workflow step that defines the call as handled. The call is handled when it reaches this step.
- **Orig. DN (Calling No.)**—Originator directory number. This number is the same as the calling number. If originator type is agent, this field shows the ICD extension of the agent. If originator type is device, this field shows the CTI port number. If originator type is unknown (through gateway), this field shows the telephone number of the caller.
- **Destination DN**—Destination directory number. If destination type is agent, this field shows the ICD extension of the agent. If destination type is device, this field shows the CTI port number. If destination type is unknown (through gateway), this field shows the telephone number called.
- **Called Number**—If the call was a transfer, this field shows the number that the call was transferred to. Otherwise, this field shows the number originally dialed by the caller. This number can be either a route point number or an agent extension.
- **Application Name**—Name of the Cisco ICD or IVR application associated with the route point.
- **CSQ Names**—Name(s) of the contact service queue (CSQ) or queues for which the call was queued. This field displays a maximum of three CSQs separated by comma. The CSQ that handled the call is marked with an asterisk (*). This field is blank if the call did not queue for any CSQ.
- **Queue Time**—Time that elapsed between the time a call entered the CSQ and the time the call was answered by an agent or disconnected. This field is blank if the call did not queue for any CSQ.
- **Agent Name**—Name of the agent who handled the call, name of the agent who participated in the conference call, or name of the supervisor who barged the call. This field is blank if the call was not presented to any agent.
- **Ring Time**—Time that elapsed between the time that a call rang at the Cisco Agent Desktop and the time that the call was answered by an agent, presented to another agent (if the first agent did not answer the call), or disconnected. This field is blank if the call was not presented to any agent.

- **Talk Time**—Time that elapsed between the time that an agent answered the call and when the call was disconnected or transferred, not including hold time.
- **Work Time**—Amount of time that an agent spent in Work State after the call. This field is blank if the call was not handled by any agent.

The Detailed Call, CSQ, Agent Report includes these sort criteria:

- **Session ID**—Displays the report in order of the unique session identification number that the system assigned to a call.
- **Call Start Time**—Displays the report in order of the date and time that the call started.
- **Called Number**—Displays the report in order of the number called.

The Detailed Call, CSQ, Agent Report includes these filter parameters:

- **Called Number**—Displays information for the specified called number(s).
- **Calling Number**—Displays information for the specified calling number(s). Calling number is the same as Originator DN.
- **Application Name**—Displays information for the specified application name(s).
- **Contact Type**—Displays information for the specified contact type(s): incoming, outgoing, or internal.
- **Originator Type**—Displays information for the specified originator type(s): agent, device, or unknown.
- **Destination Type**—Displays information for the specified destination type(s): agent, device, or unknown.
- **Agent Name**—Displays ICD calls handled by the specified agent(s), conference calls which were participated by the specified agent(s), and calls which were barged by the specified supervisor(s).
- **CSQ Name**—Displays calls which queued for any of the specified CSQs.
- **Duration Greater Than or Equal to T seconds**—Displays calls with duration greater than or equal to the number of seconds specified by T.
- **Duration Less Than or Equal to T seconds**—Displays calls with duration less than or equal to the number of seconds specified by T.

Sharing Cisco CRA Historical Reports on the Web

This section explains how you can make Cisco CRA Historical Reports available to users over the web. Because historical reports can contain proprietary information, you may want to make them available through your company intranet (rather than the public Internet) so that you can control access to them.

Before you make historical reports through the web, refer to the “Crystal Reports Developer Edition from Crystal Decisions” information in the “Licensing and Copyright Information” section in *Release Notes for Cisco Customer Response Applications 3.0(1)*. This material includes important usage information and restrictions of which you should be aware.

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_release_notes_list.html

In addition, refer to *Cisco CRA Historical Reports User Guide* for information about scheduling and exporting historical reports.

To provide web access to historical reports, perform the following procedure. This procedure creates a folder on the web server in which historical reports are stored. It also sets up the Cisco CRA Historical Reports client computer to export reports to the web server for sharing. The web server must be running the Windows 2000 Server operating system.



Note

Do not use the Cisco CRA server or a Remote Database Server as the web server to avoid affecting the performance of these servers.

Procedure

-
- Step 1** On the web server, make sure that the following services are running:
- IIS Admin service
 - World Wide Web Publisher service
- Step 2** On the web server, create a folder in which to store historical reports. For example, create a folder on the C:\ drive and name it Reports.
- Step 3** Locate and right-click the new folder you created and choose **Sharing**.
- Step 4** In the Properties dialog box, click the **Web Sharing** tab.

Step 5 In the Web Sharing area:

- a. Choose Default Web Site from the Share on drop-down list.
- b. Click the **Share this folder** radio button.
- c. Highlight the alias for the folder you created and click **Edit Properties**.

Step 6 In the Edit Alias dialog box:

- a. Check the **Read** check box.
- b. Check the **Directory browsing** check box.
- c. Uncheck any other check boxes if they are checked.
- d. Click the **None** radio button.
- e. Click **OK**.

Step 7 In the Properties dialog box, click **OK**.

The new folder you created can now be accessed by entering the following URL in a web browser, where *server* is the name or the IP address of the web server and *folder* is the alias of the new folder:

http://server/folder/

Step 8 On the Cisco CRA Historical Reports client computer, map a network drive to the folder on the web server that you set up for sharing historical reports.

Set up mapping to reconnect at logon.

For example, if you created a folder on the web server called Reports, map the network drive to the Reports folder on the web server.

Refer to your Windows documentation for information about mapping a network drive.

Step 9 When you schedule or export reports from the Cisco CRA Historical Reports client, use the drive letter from the mapping process when you specify the export location.

For example, if the drive letter from the mapping process is F and if you are exporting a report called myreport.pdf, specify F:\myreport.pdf as export location.

The report you export will be available at the following URL, where *server* is name or IP address of the web server, *folder* is the alias of the web server folder in which reports are stored, and *report* is the name of the report:

<http://server/folder/report.pdf>.

Adding a 15-Minute Interval Length to a Cisco CRA Historical Report Filter Parameter

The following Cisco CRA historical reports provide filter parameters that let you display information for 30-minute intervals or for 60 minute intervals within the report period.

- Contact Service Queue Activity Report (by CSQ)
- Contact Service Queue Activity Report (by Interval)
- Agent State Summary Report (by Agent)
- Agent State Summary Report (by Interval)
- Common Skill Contact Service Queue Activity Report (by Interval)

You can add a filter parameter that lets you display information for 15-minute intervals during the report period. To do so, follow these steps:

Procedure

- Step 1** Locate the report definition file for the report that you want to update and make a backup copy of this file.

Report definition files have descriptive names and are located in the following folder under the folder in which you installed the Cisco CRA Historical Report client system. (By default, the client system installs in the Program Files directory.)

Cisco CRS Historical Reports\ReportTemplates\Language

For example, the report definition file for the U.S. English version of the Contact Service Queue Activity Report (by Interval) report is named:

ICD_Contact_Service_Queue_Activity_by_Interval_en_us.xml

By default, this file is located in this directory:

C:\Program Files\Cisco CRS Historical Reports\ReportTemplates\EN_us

- Step 2** Use a Windows text editor to open the report definition file for the report that you want to update.

- Step 3** In the report definition file, locate this line:

```
<ListOption OptionSelected="True" OptionValue="0">Entire report range</ListOption>
```

- Step 4** Insert this line immediately after the line that you located:

```
<ListOption OptionSelected="False" OptionValue="15">Fifteen (15) minutes</ListOption>
```

Now there is a series of lines in the file that looks like this:

```
<ListOption OptionSelected="True" OptionValue="0">Entire report range</ListOption>
<ListOption OptionSelected="False" OptionValue="15">Fifteen (15) minutes</ListOption>
<ListOption OptionSelected="False" OptionValue="30">Thirty (30) minutes</ListOption>
<ListOption OptionSelected="False" OptionValue="60">Sixty (60) minutes</ListOption>
```

- Step 5

Save your changes and exit the text editor.

A new option for the Interval Length filter parameter is available for the report that you updated. The new option lets you designate a 15-minute interval for the report.

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 35](#)
- [Installing a Cisco Desktop Client on a PC on which Windows XP-SP2 is Already Running, page 38](#)
- [Unblocking Applications, page 39](#)

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 36](#)
- [Cisco Agent Desktop with Media Termination, page 36](#)
- [Cisco Desktop Administrator, page 37](#)

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 39](#).

- 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 39](#).

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 39](#).

- 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 39](#).



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 39](#).

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 39](#).

- 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 39](#).

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 39](#).

- 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 39](#).

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
 - **SpkView**—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 IVR ¹	IPCC Express Standard	IPCC Express Enhanced	IPCC Express Premium	Extended Services
Telephony Apps	X	X ²	X ²	X ²	
ICD ³		X	X	X	
Queue Manager	X				

Table 2 *Features Enabled by Each Product Package (continued)*

Feature	IP IVR¹	IPCC Express Standard	IPCC Express Enhanced	IPCC Express Premium	Extended Services
Extension Mobility	X ⁴			X ⁴	X
Auto Attendant	X ⁴			X ⁴	X
Multiple Language Support	X	X	X	X	
JTAPI ⁵	X	X	X	X	X
HTTP ⁶	X			X	
Email	X			X	
Database	X			X	
Cisco Media Termination	X	X	X	X	X
ASR ⁷	X ⁸		X ⁸	X ⁸	
TTS ⁹	X ⁸		X ⁸	X ⁸	
Voice Browser	X ¹⁰		X ¹⁰	X ¹⁰	
Real-Time Reporting	X	X	X	X	X
Historical Reporting	X ¹¹	X ¹²	X ¹³	X ¹³	
Editor	X ¹⁴	X ¹⁵	X ¹⁶	X ¹⁷	

1. IP IVR = Cisco IP Interactive Voice Response
2. Cisco Intelligent Contact Management (ICM) (Translation routes and Post-routes can not be configured)
3. ICD = Integrated Contact Distribution
4. Sample Scripts Included
5. JTAPI = Java Telephony Application Programming Interface
6. For Extended Services, the HTTP subsystem and the ability to configure HTTP triggers is included for use with Extension Mobility
7. ASR = Automatic Speech Recognition
8. Add-on Feature
9. TTS = Text-To-Speech

10. Only available if ASR option is purchased
11. Only IVR Reports
12. ICD Standard Historical Reporting Client can be purchased
13. ICD Enhanced Historical Reporting Client can be purchased
14. ICD Steps not included
15. Email, Http, DB, ICM and Java steps not included, and the Set Priority step is not included
16. Email, Http, DB, ICM and Java steps not included
17. ICM 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.



Note

If a Cisco CRA document is not updated from a previous release of Cisco CRA, that document remains valid for the current release.

Table 3 **Related Documentation**

Related Information and Software	Document or URL
Cisco CRA documentation overview	<i>Cisco Customer Response Applications 3.5 Resources Card</i> in your Cisco CRA product package
Cisco CRA documentation	http://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
<i>Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide</i>	http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html
Cisco voice products documentation	http://www.cisco.com/en/US/products/sw/voicesw/index.html
Operating system documentation	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_installation_guides_list.html

Table 3 *Related Documentation (continued)*

Related Information and Software	Document or URL
Virtual Network Computing (VNC) documentation	http://www.cisco.com/en/US/products/sw/netmgts/ps2255/index.html
Cisco MCS hardware specifications	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/products_data_sheets_list.html
Cisco CallManager documentation	http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Backup and restore documentation	http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
Service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Cisco CallManager Extended Services	http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Caveats

This section includes the following topics:

- [Resolved Caveats, page 44](#)—Severity 1, 2, and 3 defects that were resolved in this release of Cisco CRA
- [Closed Caveats, page 47](#)—Severity 1, 2, and 3 defects that were closed in this release of Cisco CRA
- [Open Caveats, page 48](#)—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 use Bug Toolkit, follow these steps:

Procedure

-
- Step 1** Go to this URL to access the Bug Toolkit:
<http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>
- Step 2** Log on with your Cisco.com user ID and password.

Step 3 To access Cisco CRS caveats, take either of these actions:

- To access a particular caveat when you know its identifier, enter the identifier in the Search for Bug ID field and click **Go**.
- To access all caveats, follow these steps:
 - a. From the Select Product Category list, choose **Voice and Unified Communications**.
 - b. From the Select Product list, choose **Cisco Unified Contact Center Express**.
 - c. From the Software Versions drop-down list, choose the desired Cisco CRS release.
 - d. Click the desired Advanced Options radio button
If you choose custom settings, enter appropriate custom information.
 - e. Click **Search**.

A list of caveats that match your search criteria appear. To see details about any caveat, click its Bug ID number or click its **Info** link.

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*.

Resolved Caveats

[Table 4](#) describes Severity 1, 2, and 3 defects that were resolved in this release of Cisco CRA.

Table 4 *Resolved Caveats for Cisco CRA 3.5(4)*

Identifier	Summary
CSCed41480	JRE incompatibility error, JRE too new
CSCee03176	Issue in AgentStateDetail table
CSCee47370	Refresh after adding CSQ adds another record of the same CSQ
CSCef04789	Cisco Agent Desktop shows lingering calls even after call has terminated

Table 4 *Resolved Caveats for Cisco CRA 3.5(4) (continued)*

Identifier	Summary
CSCef18373	SyncServer/VoIP server not started after password change using CRSAdminUtil
CSCef33922	Time of Day Cust. gives Time Ranges Overlap error for valid input
CSCef68013	DB Write step throws ArrayIndexOutOfBoundsException
CSCef73801	Real time reports show call stuck in queue after call RNAs to agent
CSCef80041	Agent and Supervisor desktops experience significant delay with SRST
CSCef86091	RTP input event lost under load test
CSCef86688	Issue in Historical Reporting Client Scheduler
CSCef88742	Enhance consult transfer to support off-net destinations
CSCef91600	Getdigitstring operated different prior to 3.1 for ASR channels
CSCef97357	SL: FCVoIPMonSvr.exe takes 100% after installing Cisco Security Agent
CSCeg01517	On intercept, the Cisco Supervisor Desktop shows Improper data
CSCeg13020	Misspelling on CRA 3.5(2) Installation Wizard
CSCeg14592	Install: Some install errors result in the Installer not aborting
CSCeg16848	CRA install continues with invalid license
CSCeg17883	CRA Engine shuts down when RMI port is in use
CSCeg18795	Install: Bad license does not cause install to abort
CSCeg18931	Agent State Summary by Name Report shows duplicate entree for Agent
CSCeg19155	Install: Installer needs to detect license error and not continue
CSCeg22737	IVR does not play -6.00 in Hebrew when passed as a string from ICM
CSCeg30311	French Ver. CAD viewer inconsistency
CSCeg30813	After multiple transfer failures, call not aborted
CSCeg42603	Danish and Malay in language ICD Configuration dropdown list
CSCeg43024	Installation error for Malay and Danish as a country
CSCeg48933	Install: Installer needs to detect license format and not continue
CSCeg49450	Cisco Agent Desktop stops responding if Help menu is selected during SRST
CSCeg51377	MTCAD is unable to drop the call after Publisher failover
CSCeg53384	Error message displays after installation of ASR/TTS

Table 4 *Resolved Caveats for Cisco CRA 3.5(4) (continued)*

Identifier	Summary
CSCeg54466	Cisco Agent Desktop freezes with SRST switchback or network failure
CSCeg57674	CRA Historical Report Issues with MaxWaitTime for Calls Abandoned
CSCeg58828	VoIP Monitor Subsystem in Partial_Service after network recovery
CSCeg59244	Editor: Get Digit step does not convert properly from CRA 3.1 to CRA 3.5
CSCeg60247	Supervisor cannot monitor remote agents after SRST switchback
CSCeg66013	Call stuck in Cisco Supervisor Desktop when monitoring/recording with SRST
CSCeg70235	The link to modify the keypad mapping is not visible on the Cisco CallManager pages
CSCeg72780	Calls in ContactRoutingDetail table with finalPriority = 0
CSCeg87574	Call stuck in priority queue on Cisco Supervisor Desktop, agent transfer call to route point via Cisco Unity
CSCeh05891	Database subsystem should account for null SQL state in some error cases
CSCsa62784	Prompt queue not cleared if call dropped during VB prompt play
CSCsa63780	Phantom Calls in real-time reports
CSCsa71189	NullPointerException displayed when Execute button clicked in DB write
CSCsa71190	Historical reporting error on specific date overflow of data
CSCsa71918	Call aborted if transferred to route point using task button on Cisco Agent Desktop
CSCsa72409	IP-IVR ports hang if caller drops right when transfer is completed
CSCsa74890	Cisco Agent Desktop Blind Xfer toolbar button not working
CSCsa74890	Cisco Agent Desktop Blind Transfer toolbar button not working
CSCsa75397	Agent Detail Report extra record with blank called number
CSCsa81870	LDAP queries cause AD DC to go to 100% - agents sometimes lose skills
CSCsa82502	Spanish Version historical reports client unable to print report
CSCsa83251	LDAP malfunction causes loss of skills
CSCsa89722	Call stuck in queue when transfer to agent fails
CSCsb02825	Reporting issue if supervised transferred call to queue is redirected.

Table 4 *Resolved Caveats for Cisco CRA 3.5(4) (continued)*

Identifier	Summary
CSCsb08113	Missing TransferEnd cause potential deadlock, Applications subsystem goes to partial service
CSCsb12608	RmCm subsystem stuck in Initializing while loading agents due to LDAP issues
CSCsb12709	Some of the agents lose skill assignments
CSCsb14303	The talk time shows blank after long talk period
CSCsb15581	Discrepancy between Agent State Summary and Agent Login/Logout Activity
CSCsb25111	Java Heap runs out of space restarting the CRA engine
CSCsb33770	ICD: Agent member of hunt group leaves agent stuck in Not Ready
CSCsb35043	Agent State Detail report fails with apostrophe in the name.
CSCsb50990	AD malfunction causes IPCC Express Agents to lose skills
CSCsb67718	License update utility header never changes
CSCsb76192	CRA Editor validates with undefined variable
CSCsb80533	Phantom Calls in Real-Time Reporting
CSCsk15778	Current CRS time in Real-Time Reporting is not changing for NZ DST

Closed Caveats

[Table 5](#) describes list of Severity 1, 2, and 3 defects that were closed in this release of Cisco CRA.

Table 5 *Closed Caveats for Cisco CRA 3.5(4)*

Identifier	Headline and Bug Toolkit Link
CSCea90780	SL: Supervisor cannot stop recording an agent's call-specific scenario
CSCed14055	Blank Agent start time field after consult calls (conf or xfers)
CSCed41480	JRE incompatibility error, JRE too new
CSCeg32653	ASR Server information removed from config after failover and update
CSCsd86588	CSQ SLA report chart bar has percentage greater than 100

Open Caveats

Table 6 describes Severity 1, 2, and 3 defects in this release of Cisco CRA.

Table 6 *Open Caveats for Cisco CRA 3.5(4)*

Identifier	Headline and Bug Toolkit Link
CSCdz59921	IP Phone agent shown in Talking state after logoff
CSCdz78378	SL: VoIP autorecovery message should mention specific VoIP server IP address
CSCdz89970	SL: CAD shows Calling Num Unavailable after answering a conference
CSCea03689	SL: Disabling Ent Data from CDA should disable it for IP Phone agent
CSCea04306	With TAI shutdown, ICD logs out one IP Phone agent but not the other
CSCea20537	SA password change after installation needs registry update for sync
CSCea28382	SL: ICD cant start/restart if Publisher is down
CSCea32551	SL: Agent cannot see chat messages during conference
CSCea33430	Agent cannot go Ready after login under certain conditions
CSCea61018	HR leaks CRDR for arbitrary transfer/conference scenarios
CSCea81865	OrigCalledNumber in CCDR is blank in redirect to agent scenario
CSCeb07043	CSD Italian client inst: no warning text shown on dialog box
CSCeb51726	Agent's Enterprise Data does not get updated for one scenario
CSCec04764	GetCallContactInfo step does not show the transferred arrival type
CSCec10743	CRA ICD Setup does not allow domain name for host in AD section
CSCed21649	Developers Guide for ICD is incorrect when ref ccdrVar usage
CSCed45771	Cannot log in an agent if another one is logged in using same extension
CSCee79930	DB steps cannot see all SQL tables if a table name contains slashes
CSCee85626	ICD call transferred from an agent to another ICD rout point fails when call RONAs
CSCee89415	Cisco CRA with Active Directory fails to upload Spoken Name Prompts
CSCee90735	Under rare circumstances, Real-Time Reports falsely shows a call stuck in queue
CSCee92368	Call Stuck in queue—agent stuck in reserved—multiple IDs share DN

Table 6 *Open Caveats for Cisco CRA 3.5(4) (continued)*

Identifier	Headline and Bug Toolkit Link
CSCee95240	Historical Reporting: missing a transfer call record in Detail Call, CSQ, Agent Report
CSCeg33850	Call transfer fails from desktop if initial attempt is not completed
CSCeg49502	Cisco Agent Desktop and Cisco Supervisor Desktops report incorrect call information after Barge
CSCeg62599	Supervisor can not barge/intercept H.450.2 call flow

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)