



Release Notes for Cisco Agent Desktop 7.2(1)

Revised: August 12, 2009

Contents

These release notes discuss the following topics:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 2](#)
- [Open Caveats, page 3](#)
- [Resolved Caveats, page 4](#)
- [Documentation Updates, page 4](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 11](#)

Introduction

These release notes describe the new features for Cisco Agent Desktop version 7.2(1). These release notes also provide information that was unavailable at the time of release, including documentation changes, a resolved caveat that was previously reported as open, and an additional open caveat found after the release in July 2007.

Use these release notes in conjunction with the Cisco Agent Desktop 7.2 documentation provided on the installation CD.



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

© 2008, 2009 Cisco Systems, Inc. All rights reserved.
© 2008, 2009 Calabrio, Inc. All rights reserved.

System Requirements

Cisco Agent Desktop 7.2(1) is compatible with Cisco Unified Contact Center Enterprise and Hosted Edition, Release 7.2(1).

New and Changed Information

General

- Localized in Russian and Traditional Chinese
- Support for Windows MUI language packs
- Improved legibility of Graphical User Interface (GUI)
- Support for Windows 2003 Server R2
- Support for Windows Vista

**Note**

Automated updates are not supported on Windows Vista in this release.

Cisco Agent Desktop—Browser Edition

- Login and password encryption

Cisco Unified IP Phone Agent

- Login and password encryption

Cisco Supervisor Desktop

- Support for Cisco Unified CallManager-based agent call silent monitoring via an IP phone

Cisco Desktop Administrator

- Streamlined configuration setup during installation
- Integration of CAD Services LDAP and Recording and Statistics Service Database configuration
- Support for Microsoft Simple Network Management Protocol (SNMP)
- Improved serviceability with enhanced logging message content
- Support for exporting and importing workflow actions

Limitations and Workarounds

Supervisor Experiences Inconsistent Behavior When Trying to Monitor/Record An Agent

Symptom: Supervisor can sometimes monitor/record an agent, at other times the supervisor cannot monitor/record an agent.

Description: The agent's phone is using G.722 codec.

Workaround: Disable "Advertise G 722 Codec" on the Agent phone. CAD does not support G.722 codec.

Open Caveats

The following issues are open in Cisco Agent Desktop 7.2(1).



Note

You can view more information and track individual CAD defects using the Cisco Bug Toolkit located at: <http://tools.cisco.com/Support/BugToolKit>.

Table 1 Open caveats in release 7.2(1)

Identifier	Severity	Headline
CSCsg45013	2	Japanese IPPA screens are garbled in SIP phones.
CSCsg72033	3	CAD-BE agents in work states never get logged out if they close browser.
CSCsg72037	3	Reason code strings do not appear when viewing agent state logs in CSD.
CSCsg72048	3	Voice contact workflow rules are disabled after restoring backup data.
CSCsg72063	3	Restore from backup does not restore extended life recordings.
CSCsg72076	3	Restore from backup does not restore supervisor report preferences.
CSCsg72084	3	Occasionally unable to enter text in CAD-BE dialogs on Linux.
CSCsg72093	3	The CAD-BE login dialog does not appear in the task bar.
CSCsg72103	3	Restore from backup allows you to restore a backup from a different system.
CSCsg72106	3	Some multi-byte language input does not work in Desktop Administrator.
CSCsg73738	3	CAD-BE main window displays error after login.
CSCsg76689	3	Restore from backup does not restore new enterprise data fields.
CSCsg76697	3	Restore from backup does not restore new enterprise layouts.
CSCsi84699	3	The CAD SMC shows that SQL Agent is down when it is not.
CSCsi86360	3	Restore/Upgrade does not preserve reason codes and wrapup.
CSCsj09376	3	In some cases, Rec and Stats Database replication setup does not work.
CSCsj09392	3	Backup of Recording and Statistics Service database is blocked by CSA.
CSCsj18349	3	Task Button/Alt key issue

Resolved Caveats

The following issues have been resolved in Cisco Agent Desktop 7.2(1).



Note

You can view more information and track individual CAD defects using the Cisco Bug Toolkit located at: <http://tools.cisco.com/Support/BugToolKit>.

Table 2 Caveats resolved in release 7.2(1)

Identifier	Severity	Headline
CSCsg45022	3	Japanese email action sends mail in Shift JIS.
CSCsg72000	3	In multi-byte languages, some strings are garbled when running an MUI.
CSCsg72014	3	Multiple supervisors can not monitor a single CAD-BE mobile agent.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Agent Desktop release 7.2 documentation suite was released.

The following table lists the documents that are affected, the page(s) of the document on which the change appears, and the revision date.

Document name	Page	Change type	Revision date
<i>Cisco CAD Installation Guide</i>	77	correction	19 Dec 2008
	84	correction	19 Dec 2008
	42	omission	9 June 2008
	94	correction	5 May 2007
	18	correction	3 Dec 2007
	30	omission	12 Nov 2007
	70	omission	2 Aug 2007
<i>Cisco CAD Service Information Manual</i>	225	update	12 Aug 2009
	246	addition	6 Jul 2009
	25	correction	3 Dec 2007
	235	update	3 Dec 2007
	246	omission	12 Nov 2007
<i>Cisco IP Phone Agent User Guide</i>	14, 16	omission	26 Sep 2007

Cisco CAD Installation Guide

This section contains information about [NAT and VPN Requirements](#) and [Using Automated Package Distribution Tools](#) that the *Cisco CAD Installation Guide* does not provide. This section also contains corrected information about the following topics:

- upgrading from CAD 6.0 to CAD 7.2
- parameters for the BackupDB utility
- requirements when installing CAD 7.2

- changing the default URL authentication parameter
- the features that are available in the Standard CAD package

Upgrading from CAD 6.0 to CAD 7.2

The *Cisco CAD Installation Guide* contains the following instructions for upgrading from CAD 6.0 to CAD 7.0 on page 77.

If you are upgrading a single server:

- Complete steps 1-5 only in the following procedure.

If you are upgrading a replicated system:

- Shut down replication on both servers before beginning the following procedure. For instructions, see "Shutting Down Replication (CAD 7.1 and before)" on page 90.
- Complete steps 1-5 on the primary server and the remaining steps on the secondary server.



Note If you do not shut down replication before beginning the procedure, your CAD Services LDAP database may become corrupted.

This information is incorrect. Replication does not need to be shut down before beginning the procedure. The correct instructions for upgrading from CAD 6.0 to CAD 7.2 are as follows.

If you are upgrading a single server:

- Complete steps 1-5 only in the following procedure.

If you are upgrading a replicated system:

- Complete steps 1-5 on the primary server and the remaining steps on the secondary server.

BackupDB Utility

The *Cisco CAD Installation Guide* documents the parameters for the BackupDB utility on page 84 as follows.

```
BackupDB "<dbUser>" "<dbPassword>" "<server>" "<dir>"
```

where:

<dbUser> is the user ID for the old database. The default is **sa**.

<dbPassword> is the password for the old database. The default is **sa**.



Note If the user ID and password are not the default values and you have forgotten what they are, contact technical support for assistance.

<server> is the hostname of the server on which the database is located, or the local loopback IP address of 127.0.0.1.

<dir> is the directory in which the backup file is to be saved. <dir> must be a local drive.

This information is incorrect. The correct description of the parameters is as follows.

```
BackupDB <dbUser> <dbPassword> <server> "<dir>"
```

Use the following values.

<dbUser> Any value may be used.

<dbPassword> Any value may be used.

<server> The hostname of the server on which the database is located, or the local loopback IP address of 127.0.0.1.

<dir> The absolute path for the directory in which the backup file is to be saved. <dir> must be a local drive. The quotation marks are necessary only if the path has spaces in it.



Note The directory must exist before you run this command or it will fail.

Installing CAD Services

The existing *Cisco CAD Installation Guide* contains the following note on page 42.



Note

You must install CAD Services as a local administrator. If you install CAD Services as a domain administrator, Recording and Statistics replication jobs will fail.

This information is incomplete. The complete version of this note is as follows.



Note

When you install the CAD services, you must be logged in as a local administrator. If you install CAD services as a domain administrator, Recording and Statistics replication jobs will fail. If the Administrator account does not exist, you must create an administrator user before you begin installation. This user can be removed after you have installed the CAD services and completed CAD Configuration Setup (postinstall.exe).

Changing the Default Authentication URL

The default URL used for authentication is the best setting for most contact centers. If your contact center needs IP Phone Agent screens to be refreshed more quickly, changing the default URL to the IP Phone Agent authentication URL on the CAD server might provide better performance with IP Phone Agent. Note that improved performance is not guaranteed, however, and other applications that use this URL for authentication might even slow down.



Note

If either the CAD server is down or the Tomcat service (which runs on the CAD server) is down, authentication will fail.

You can change the URL used for authentication either for all IP phones as a group or for one or more IP phones individually. The advantage to changing the URL for all IP phones is that you only need to make the change once. Note that a global change will affect every IP phone and application that requires authentication. The advantage to changing the URL for one or more IP phones individually is that you can choose the specific phones you want to configure. Note that you must repeat the configuration process for every IP phone separately, however.

Changing the Default Authentication URL for All IP Phones as a Group

To change the authentication URL for all IP phones as a group, complete the following steps.

Step 1 Log into Unified CM Administration.

Step 2 Choose System > Enterprise Parameters. The Enterprise Parameters Configuration window appears.

Step 3 In the Phone URL Parameters section, change the value of the URL Authentication parameter to the following, where <Tomcat> is the IP address of the CAD server on which Tomcat is running.

`http://<Tomcat>:8088/ipphone/jsp/sciphonexml/IPAgentAuthenticate.jsp`



Note This URL is case sensitive.

Step 4 Click Save. A dialog box appears, telling you to click on the Reset Phone button to have the changes take effect.

Step 5 Click OK. The dialog box closes.

Step 6 Click Reset. The Device Reset window appears.

Step 7 To restart the device without shutting it down, click Restart. To shut down the device and bring it back up, click Reset.

Changing the Default Authentication URL for an Individual IP Phone

To change the authentication URL for an individual IP phone, complete the following steps.

Step 1 Log into Unified CM Administration.

Step 2 Choose Device > Phone. The Find and List Phones page appears.

Step 3 Click the Device Name of the phone that you want to configure. The Phone Configuration page appears.

Step 4 In the External Data Locations Information section, change the value of the Authentication Server parameter to the following, where <Tomcat> is the IP address of the CAD server on which Tomcat is running.

`http://<Tomcat>:8088/ipphone/jsp/sciphonexml/IPAgentAuthenticate.jsp`



Note This URL is case sensitive.

Step 5 Click Save. A dialog box appears, telling you to click on the Reset Phone button to have the changes take effect.

Step 6 Click OK. The dialog box closes.

Step 7 Click Reset. The Device Reset window appears.

Step 8 To restart the device without shutting it down, click Restart. To shut down the device and bring it back up, click Reset.

CAD 7.2 Feature Levels

The table on page 18 of the *Cisco CAD Installation Guide* lists event-triggered workflows as a feature in Cisco Agent Desktop and Cisco Agent Desktop–Browser Edition in the Standard CAD package. This is incorrect. The event-triggered workflows feature is only available in the Enhanced and Premium CAD packages.

NAT and VPN Requirements

Using network address translation (NAT) with firewalls or routers is supported for Cisco IP Phone Agent and for client desktops, including Cisco Supervisor Desktop and Cisco Agent Desktop. NAT is not supported for servers on which the CAD services run. SPAN-based monitoring and recording is not supported with NAT.

Using NAT with IP Phone Agent requires that you use static IP addresses for the IP Phone Agent phones as well as Static NAT. Dynamic NAT and address overloading are not supported. You can find more information about NAT at this URL:

<http://www.cisco.com/warp/public/556/nat-cisco.shtml>

To ensure full bi-directional network connectivity between the contact center servers and client desktops, the client desktops must use virtual private network (VPN) software. Failing to use VPN software will result in connectivity issues and a loss in functionality. Using VPN is also recommended to provide a more secure connection.

It has been verified that Cisco VPN 3000 Concentrator and Cisco VPN Client work properly with CAD client desktops, and are supported for access. VPN solutions from other vendors may work correctly, but since they have not been formally verified, they are not supported. If you want an alternative solution to be verified, please contact your Cisco distributor.

Using Automated Package Distribution Tools

CAD's MSI-based desktop application installations can be deployed ("pushed") via automated package distribution tools that make use of the Microsoft Windows Installer service.

Requirements

CAD support for automated package distribution depends on compliance with the requirements listed below.

Execution

Installations must be executed on the target machine. Deployment methods that capture a snapshot of an installation and redistribute that image are not supported.

Per-Machine vs. Per-User Installation

Installations must be deployed on a per-machine basis. Per-user installations are not supported.

It might be necessary to ensure per-machine installation via command line.

Privileges

CAD installations require either administrative or elevated privileges.

By default, Windows Installer installations run in the context of the logged-on user.

If the installation is run in the context of an administrative account, there is no need to enable policies to grant elevated privileges.

If the installation is run in the context of an account with reduced privileges, then it must be deployed with elevated privileges. The target machine must have the Windows policy "Always Install with Elevated Privileges" enabled for both the User Configuration and the Computer Configuration. When this policy is enabled, Windows Installer installations will run in a context with elevated privileges, thus allowing the installation to successfully complete complex tasks that require a privilege level beyond that of the logged-on user.

Automated Package Installation vs. Manual Installation

Automated installations must use the same files and meet the same installation criteria as manually-deployed installations.

CAD MSI packages are located in a specified location (C:\Program Files\wfvavid\tomcat_appadmin\webapps\TUP\CAD) on a successfully-installed production server and are intended for both manual and automated deployment. Alteration of these files or the use of other MSI files included with the product at other locations is not supported.

Installation criteria such as supported operating systems, product deployment configurations, installation order, and server/client version synchronization must be met. Altering the supplied MSI packages to circumvent the installation criteria is not supported.

Multiple Software Releases

Multiple software releases must not be combined into a single deployment package. Each CAD software release is intended for distribution in its entirety as a distinct deployment. Combining multiple releases (for example, a software package's base release and a subsequent service release) into a single deployment package is not supported.

Reboots

Any reboots associated with CAD installations are required. If the installation's default reboot behavior is suppressed, the target machine must be rebooted before running the installed applications to ensure expected functionality.

Delaying a reboot is not known to be an issue at this time, as long as a reboot occurs before launching the installed applications. If it is determined in the future that delaying a reboot via command line suppression affects expected behavior, then that delayed reboot will not be supported.

Best Practices

Best practices recommendations are listed below.

Windows Installer Logging

Windows Installer logging should be enabled. The installations should be run with the following command line argument:

```
/l*v <logfile path and name>
```



Note

The log file path and name must be a location to which the installation's user context has permission to write.

This ensures that any loggable issues are captured efficiently.

Deployment

Each installation package should be deployed using its own deployment package. Using separate packages offers faster isolation of potential issues than does a composite deployment package.

Installation and Uninstallation Deployment Packages

The deployment engineer should create and test both an installation and uninstallation deployment package.

This is especially important for service release installations, which must be uninstalled before upgrading the underlying software.

Recommended Deployment Preparation Model

1. Use a lab environment to model the pending deployment.
2. Install the servers to obtain valid client installation packages.
3. Manually deploy client installation packages to ensure that the installs are compatible with your environment. This will isolate product installation vs. automated deployment issues.
4. Create your deployment packages in accordance with the requirements listed in [Requirements, page 8](#).
5. Test the deployment packages.
6. At deployment time modify your deployment packages, replacing the client installation packages from the lab environment with valid client installation packages from the production server.

Cisco CAD Service Information Manual

This section contains a correction about the maximum number of agents that can be supported by an LCC. This section also contains troubleshooting information about upgrades and restores that the *Cisco CAD Service Information Manual* does not provide.

The section “Guidelines for Sizing Deployments” on page 25 states:

A set of the base services plus the additional services is a logical contact center, or LCC. The maximum number of agents that can be supported by a single LCC is 2,000 (approximately 15,000 Busy Hour Call Completion [BHCC] with a call volume of 20 calls per agent per hour).

This is incorrect. The maximum number of agents that can be supported by a single LCC is 1,000.

The following troubleshooting items are new.

Problem: After simultaneously upgrading CAD and switching to a new ICM instance, agents cannot log in and the personnel nodes in Cisco Desktop Administrator are blank.

Solution: Wait for the Cisco Sync Service to synchronize the information from ICM.

Problem: After restoring audio files using CDBRTTool, the following line appears at the end of the log file:

```
2007-06-07 10:13:13:031 DEBUG [0xe4c] CDBRT00L::Main: End of
CDBRT00L (Success=0)
```

Solution: The CDBRTTool indicates the status of a backup or restore on the last line of the log file by printing either (Success=0), (Fail=-1), or (Some Errors=1). The result (Success=0) indicates that the return code was 0 and therefore that the run was successful. The result (Some Errors=1) indicates that errors occurred. If errors occur, the log file also includes the message "Some errors occurred with loading agents. See log/dbg file for details."

Problem: The SQL replication subscription and REPL-Merge job disappear and the publisher database cannot replicate to the subscriber database.

Solution: If the publisher database is unable to replicate to the subscriber database for 4 days, the SQL job “Expired subscription clean up” will run and remove the replication subscription (and subsequently delete the REPL-Merge job).

If the subscriber server is powered off for the duration, the jobs will not clean up. The cleanup only occurs when the publisher is able to access the subscriber server but is unable to synchronize (for example, if the SQL Server engine is stopped on the subscriber).

The default timing within SQL Server for the expired subscription cleanup job is 14 days. Recording & Statistics service replication setup changed that timer to 4 days as there should only be 7 days of data, and it was determined that if you hadn't replicated properly in 4 days, you need to set up the Recording & Statistics service replication again.

On page 225, under the heading, “Out of Sync Directory Services Databases,” revise Step 11 to read as follows:

11. Copy the following files from the old_database folder to the database folder:

```
case.dat
cmbel.dat
comp.dat
ctype.dat
decomp.dat
kdecomp.dat
DB_CONFIG
```

Cisco IP Phone Agent User Guide

This section contains information about the Skill Stats screen and the Caller Data screen that the *Cisco IP Phone Agent User Guide* does not provide.



Note

To perform any call control actions when the Skill Stats screen is displayed (for instance, make a call), you must first press Services to return to the normal phone display screen.



Note

To perform any call control actions when the Caller Data screen is displayed (for instance, make a call), you must first press Services to return to the normal phone display screen.

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

Documentation Feedback

You can provide comments about this document by sending email to the following address:

ccbu_docfeedback@cisco.com

We appreciate your comments.