



Release Notes for Cisco Agent Desktop 6.0 (1)

Revised: November 12, 2007

Contents

These release notes discuss the following topics:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 2](#)
- [Limitations and Workarounds, page 3](#)
- [Open Caveats, page 4](#)
- [Resolved Caveats, page 5](#)
- [Documentation Updates, page 6](#)
- [Obtaining Documentation, page 9](#)
- [Documentation Feedback, page 10](#)
- [Cisco Product Security Overview, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 13](#)

Introduction

These release notes describe the new features for Cisco Agent Desktop version 6.0(1). These release notes also provide information that was unavailable at the time of release, including documentation changes and an additional open caveat found after the release in May 2004.

Use these release notes in conjunction with the Cisco Agent Desktop 6.0 documentation provided on the installation CD.



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

Cisco Agent Desktop 6.0(1) is compatible with Cisco Intelligent Contact Management (ICM) 6.0(1).

New and Changed Information

CAD 6.0(1) includes the following new features:

- CTI OS-based implementation
- No longer dependent on shares—configuration data is now stored in Directory Services
- Desktops are automatically updated when new versions are detected at startup
- System redundancy

New Software Features

Cisco Desktop Administrator

- Configuration settings are set up and maintained through CAD Configuration Setup utility, accessed through Desktop Administrator (or as a standalone program). These configuration settings are no longer set up during the installation process.
- HTTP Post/Get action enables interaction between Agent Desktop and web-based applications (Premium version only).

Cisco Agent Desktop

- Improved Agent Desktop interface—it now includes call control, enterprise data, call activity, and an integrated browser in one window.
- Cisco Outbound Option now includes the Direct Preview Dialing mode.
- Improved status bar provides more information about the user and system status.

Cisco Supervisor Desktop

- Agent call data now includes the skill group
- Provides access to agent logs
- Individual agent statistics combined into a Team Agent Statistics report
- Improved status bar provides more information about system status
- Report Preferences allow you to choose which columns are displayed in reports.
- Accessibility improved with the addition of improved icons, screen reader-compatible tool tips for all controls, screen reader-compatible shortcut key, and audible tones that sound when a nonagent-initiated dialog appears (for example, chat windows or supervisor interventions).

Accessibility

Agent Desktop and Supervisor Desktop have been made more accessible by the addition of the following features:

- Follows Windows settings for screen resolution and color/contrast settings
- Screen reader-compatible tool tips for all controls
- Screen reader-compatible shortcut keys for navigating the application and toolbar
- (Agent Desktop) Audible tones that sound when a nonagent-initiated dialog appears (for example, a new chat window or supervisor interventions)
- (Agent Desktop) Screen reader-compatible non-scrolling Team Performance Messages

Chat

- Agents are no longer limited to chatting with conference call participants—agents can chat with supervisors and other team members.
- Chat Selection window displays agent phone hook states
- Messages can be tagged as high priority for immediate notice

Recording

- Recording is scalable—can record more calls simultaneously (32 in Enhanced version, 80 in Premium version)
- Multiple dedicated Recording & Playback servers

Limitations and Workarounds

Recording (Premium version)

CAD 6.0(1) supports 32 simultaneous recordings/playbacks. To increase the number of simultaneous recordings/playbacks to the 80 supported by the Premium version, download and install CAD 6.0(1) Hot Fix 1 from the CCO website.

Silent Monitoring

Desktop monitoring does not function with some NIC cards. The Intel PRO/100 and PRO/1000 NIC card series are unable to detect both voice packets and data packets in a multiple VLAN environment, which prevents desktop monitoring from functioning properly. These NIC cards do not fully support NDIS Promiscuous Mode settings.

A workaround solution is available from the Intel Technical Support website (Solution ID: CS-005897). Other solutions include:

- Using another type of NIC card that is fully NDIS-compliant. A procedure for testing if a NIC card is fully NDIS-compliant is available at this URL: www.cisco.com/en/US/customer/products/sw/custcosw/ps427/prod_tech_notes_list.html
- Monitoring agents via a VoIP Monitor server.

Enterprise Data

Enterprise Data cannot correctly display data passed to it by ICM that contains the pipe (|) character. ICM allows this character; Enterprise Data does not. The enterprise data may be truncated, or not appear at all.

Cisco IP Phone Agent

Cisco IP Phone Agent does not support Cisco Outbound Option.

CAD and ICM Upgrades

CAD 6.0(1) works only with IPCC Enterprise 6.0(1). To stage an upgrade, you may run CAD 4.4.1 or 4.6 while upgrading to IPCC Enterprise 6.0, and then, when a stable system is verified, upgrade CAD to 6.0(1). Running previous versions of CAD with IPCC Enterprise 6.0(1) is recommended only while staging upgrades.

Open Caveats

The following issues are open in Cisco Agent Desktop 6.0(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 for Cisco Agent Desktop 6.0(1)

Identifier	Severity	Headline
CSCma23690	3	<p>Symptom: MSDE uses an excessive amount of memory.</p> <p>Condition: This problem occurs in CAD 6.0.</p> <p>Workaround: Manually cap the MSDE memory usage at 256 MB by running the following script on the base CAD services:</p> <pre>osql -n -S<IP address>\CADSQL -dmaster -i "C:\Program Files\Cisco\Desktop\db\memcap.sql" -E</pre>

Table 1 *Open caveats for Cisco Agent Desktop 6.0(1)*

Identifier	Severity	Headline
CSCsa20593	3	Symptom: Agent call log, state log, and recording log data is missing. Condition: Database inserts fail when single quotes appear in the data. Workaround: Avoid using single quotes in agent ID, agent name, team name, workflow group, call wrapup data, called party name, and calling party name.
CSCsa20595	3	CAD does not show on the task bar after starting.
CSCsa20596	3	Slider bar in CAD for media termination volume does not work.
CSCsa20597	3	The database backup script does not work with long filenames.
CSCsa36988	3	Symptom: During a CAD/CSD installation, the reboot may not complete automatically when the OS is Windows NT Workstation. Workaround: Manually restart (or cold boot if PC does not respond to restart). The install will complete successfully after the PC restarts.
CSCsa36992	3	Silent monitoring and recording do not work with agents using VPN.
CSCsa37141	3	Agents lose phonebook and report settings after agent id change in ICM.
CSCsj18349	3	Task Button/Alt key issue

Resolved Caveats

The following issues have been resolved in Cisco Agent Desktop 6.0(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 *Resolved caveats for Cisco Agent Desktop 6.0(1)*

Identifier	Severity	Headline
CSCma23515	3	Request to filter or add security to .wav files per supervisor.
CSCma23964	3	Request for CAD server fault tolerance.
CSCma24645	3	Request for share-related serviceability tool (licensing).
CSCma24647	3	Request for share-related serviceability tool (recording).
CSCma25442	3	Request for dynamic debug levels.
CSCma25464	3	If closed, CAD Enterprise Data window does not reopen on next call.
CSCma25494	3	CAD VoIP Monitor service test tool requires missing DLLs.
CSCma25877	3	Request for Supervisor Desktop to remember column width settings.
CSCma25879	3	Request for Supervisor Desktop date/time stamp for record log viewer.
CSCma26071	3	The resized width of the agent name column is not remembered in Supervisor Desktop.

Table 2 Resolved caveats for Cisco Agent Desktop 6.0(1)

Identifier	Severity	Headline
CSCma26674	3	The wrapup window is not wide enough to accept the 32 characters allowed if the characters are all capitalized.
CSCma30039	3	Unable to use desktop monitoring feature to monitor/record a CAD agent if the agent's Windows login account does not have administrator rights.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Agent Desktop release 6.0 documentation suite was released.

The following table lists the document that is affected, the pages of the document on which the changes appear, and the revision date.

Document name	Page(s)	Change type	Revision date
<i>Service Information</i>	5-10, 5-75, 5-76	correction	12 Nov 2007

Service Information

Chapter 5 of *Service Information* contains three error code descriptions that refer to DSBrowser, which is no longer available in Cisco Agent Desktop as of release 6.0(1). The two tables below list the original and corrected error code descriptions.

[Table 3](#) lists the original descriptions of the three error codes.

Table 3 Original error code descriptions

Error No.	Description
ASL10002	<p>Text: The state [state] was not found in the transition map.</p> <p>Type: Informational</p> <p>Description: The state [state] was not found in an internal map.</p> <p>Action: Using DSBrowser, check whether the state is defined in LDAP under Application Data, Supported States and Application Data, Transition [state]. There could be some setup errors in LDAP.</p>

Table 3 Original error code descriptions

Error No.	Description
LA0003	<p>Text: Could not open license file [filename] [error description].</p> <p>Type: Informational</p> <p>Description: The specified license file could not be opened.</p> <p>Action: Check that the file exists and can be reached.</p> <p>If the error description says “checksum error,” copy the LicenseFile.lf from another subdirectory over the problem one and relicense that item.</p> <p>If the error description says the license file is missing:</p> <p>Check the config root path key in logical_contact_center/App Data via DSBrowser. It should have the configuration path entered during Desktop Administrator installation.</p> <p>Check that the config root path can be reached from the client PC (via Windows Explorer) and the user has permission to read/write to the LicenseFile.lf file.</p> <p>Check whether the IP address or host name is used in the config root path. The client PC must have it mapped using the same method, IP address or host name.</p> <p>If the config root path is local to the Administration PC, check whether the PC’s network identifier is valid.</p> <p>Check that the agent has read/write access to LicenseFile.lf.</p> <p>Check that the agent can create and delete files in the directory where LicenseFile.lf resides.</p>
LA0006	<p>Text: The license file has been moved.</p> <p>Type: Informational</p> <p>Description: The license file has been moved from where it was when the product was licensed.</p> <p>Action: Check the config root path key in [logical contact center]/App Data via DSBrowser. It should have the configuration path entered during the installation of Administrator. Note that if a second instance of Administrator was installed and used a different configuration path and did not set the license again, it will cause this error.</p> <p>Under the configuration path should be a license directory with subdirectories for each license type. Each of them should have a LicenseFile.lf, which is writable. Relicensing via License Administrator fixes this problem.</p>

Table 4 lists the corrected descriptions of the three error codes.

Table 4 *Corrected error code descriptions*

Error No.	Description
ASL10002	<p>Text: The state [state] was not found in the transition map.</p> <p>Type: Informational</p> <p>Description: The state [state] was not found in an internal map.</p> <p>Action: LDAP may have setup errors. The specific state may not be defined in LDAP under Application Data, Supported States or Application Data, Transition [state].</p>
LA0003	<p>Text: Could not open license file [filename] [error description].</p> <p>Type: Informational</p> <p>Description: The specified license file could not be opened.</p> <p>Action: Verify that the license file exists and that it can be reached.</p> <p>If the error description indicates a checksum error, replace the corrupted license file with a copy of LicenseFile.lf from another directory, then relicense the item.</p> <p>If the error description indicates that the license file is missing, complete the following steps.</p> <ol style="list-style-type: none"> 1. Verify that LDAP has the correct config root path key in logical_contact_center/App Data. The key should have the configuration path that was entered during Desktop Administrator installation. 2. Verify that the config root path can be reached from the client PC (via Windows Explorer). 3. Verify that the same type of identification (IP address or host name) was used in the config root path and client PC mapping. 4. If the config root path is local to the Administration PC, verify that the PC's network identifier is valid. 5. Verify that the agent has read/write access to LicenseFile.lf. 6. Verify that the agent can create and delete files in the directory that contains LicenseFile.lf.

Table 4 *Corrected error code descriptions*

Error No.	Description
LA0006	<p>Text: The license file has been moved.</p> <p>Type: Informational</p> <p>Description: The license file has been moved from its location when the product was licensed.</p> <p>Action: Verify that LDAP has the correct config root path key in logical_contact_center/App Data. The key should have the configuration path that was entered during Desktop Administrator installation. If a second instance of Desktop Administrator was installed with a different configuration path without setting the license again, this error will result.</p> <p>The configuration path should contain a license directory with subdirectories for each license type. Each subdirectory should contain a writable copy of LicenseFile.If. Relicensing via License Administrator fixes this problem.</p>

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

<http://www.cisco.com/techsupport>

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

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

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

<http://www.ciscopress.com>

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

<http://www.cisco.com/packet>

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

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

or view the digital edition at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>