



# Release Notes for Cisco Agent Desktop 7.1 (2)

---

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 2](#)
- [Open Caveats, page 2](#)
- [Resolved Caveats, page 3](#)
- [Documentation Updates, page 4](#)
- [Obtaining Documentation, page 5](#)
- [Documentation Feedback, page 6](#)
- [Cisco Product Security Overview, page 6](#)
- [Obtaining Technical Assistance, page 7](#)
- [Obtaining Additional Publications and Information, page 9](#)

## Introduction

These release notes describe the new features for Cisco Agent Desktop version 7.1(2). 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 November 2006.



---

**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 7.1(2) is compatible with Cisco Unified Contact Center Enterprise and Hosted Edition, Release 7.1(2).

## New and Changed Information

CAD 7.1(2) includes these new features.

### General:

- Localization in Simplified Chinese, Danish, Dutch, French, German, Italian, Japanese, Korean, Brazilian Portuguese, Spanish, and Swedish
- Command line utility for converting \*.raw recording files to \*.wav files individually or in bulk
- MSDE security improvements
- Automatic configuration of service accounts for NT authentication to the Admin Workstation database

### Cisco Agent Desktop—Browser Edition:

- Supports Mozilla Firefox on Windows and Red Hat Linux platforms

### Cisco Supervisor Desktop:

- Mobile Agent silent monitoring and recording
- Supports double-byte languages in graphical displays

### Cisco Desktop Administrator:

- Blind Conference added to the Call Control action
- New Set Enterprise Data action
- New Agent Re-skilling node to enable administrators to configure alternate dynamic re-skilling webpages

## Limitations and Workarounds

None reported.

## Open Caveats

The following issues are open in CAD 7.1(2).



### 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 7.1(2).

Identifier	Severity	Headline
<a href="#">CSCse36357</a>	3	Unexpected callconnectionclear event in conference call.
<a href="#">CSCsg22094</a>	3	Conference event shows duplicate phone number.
<a href="#">CSCsg45013</a>	2	Japanese IPPA screens are garbled in SIP phones.
<a href="#">CSCsg45022</a>	3	Japanese email action sends mail in Shift JIS.
<a href="#">CSCsg72000</a>	3	In multi-byte languages, some strings are garbled when running an MUI.
<a href="#">CSCsg72014</a>	3	Multiple supervisors can not monitor a single CAD-BE mobile agent.
<a href="#">CSCsg72033</a>	3	CAD-BE agents in work states never get logged out if they close browser.
<a href="#">CSCsg72037</a>	3	Reason code strings do not appear when viewing agent state logs in CSD.
<a href="#">CSCsg72048</a>	3	Voice contact workflow rules are disabled after restoring backup data.
<a href="#">CSCsg72063</a>	3	Restore from backup does not restore extended life recordings.
<a href="#">CSCsg72076</a>	3	Restore from backup does not restore supervisor report preferences.
<a href="#">CSCsg72084</a>	3	Occasionally unable to enter text in CAD-BE dialogs on Linux.
<a href="#">CSCsg72093</a>	3	The CAD-BE login dialog does not appear in the task bar.
<a href="#">CSCsg72103</a>	3	Restore from backup allows you to restore a backup from a different system.
<a href="#">CSCsg72106</a>	3	Some multi-byte language input does not work in Desktop Administrator.
<a href="#">CSCsg73738</a>	3	CAD-BE main window displays error after login.
<a href="#">CSCsg76689</a>	3	Restore from backup does not restore new enterprise data fields.
<a href="#">CSCsg76697</a>	3	Restore from backup does not restore new enterprise layouts.
<a href="#">CSCsg76710</a>	3	In some situations RASCAL Database replication does not work.
<a href="#">CSCsj18349</a>	3	Task Button/Alt key issue

## Resolved Caveats

The following issues have been resolved in CAD 7.1(2).



### 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 7.1(2)

Identifier	Severity	Headline
<a href="#">CSCee96040</a>	3	Incorrect value listed for ANI on Agent Desktop
<a href="#">CSCee96071</a>	3	Incorrect value of Customer Number in Callback Screen on Agt. Desktop
<a href="#">CSCsa20595</a>	3	CAD does not show on the task bar after starting.
<a href="#">CSCsa20596</a>	3	Slider bar in CAD for media termination volume does not work
<a href="#">CSCsa52063</a>	6	CAD 4.6 Hotfix 1 does not indicate end of install or reboot required
<a href="#">CSCsb73423</a>	3	Incorrect name for backup tool in Cisco CAD Installation Guide 7.0(0)

**Table 2** Caveats resolved in release 7.1(2) (continued)

Identifier	Severity	Headline
<a href="#">CSCsb92684</a>	3	SLDoc CAD SQL User to Read Logger DB documentation does not exist
<a href="#">CSCsc46525</a>	3	Very long ECC variable xferred from CAD to CTI OS not sent
<a href="#">CSCsc51958</a>	3	Supervisor desktop does not install if agent desktop exist.
<a href="#">CSCsc77053</a>	3	When 2 people access same CDA node, no error msg is received on Win2KPro
<a href="#">CSCse64057</a>	3	The integrated browser is disabled by default in CAD w/premium.
<a href="#">CSCse64074</a>	3	Apply button not enabled when changing workflow classification.
<a href="#">CSCse64143</a>	3	The Answer/Drop button is visible for Mobile Agents in Call-by-Call mode
<a href="#">CSCse64148</a>	3	Supervisor workflows are lost after restore.
<a href="#">CSCse64186</a>	3	CDA always shows CAD-BE browser is disabled.
<a href="#">CSCse64193</a>	3	IPPA is on a call, but no call is shown in CSD.

## Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Agent Desktop release 7.1 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(s)	Change type	Revision date
<i>Cisco CAD Service Information Manual</i>	208	omission	12 Nov 2007
<i>Cisco IP Phone Agent User Guide</i>	14, 16	omission	26 Sep 2007

## Cisco CAD Service Information Manual

This section contains troubleshooting information about upgrades that the *Cisco CAD Service Information Manual* does not provide.

**Problem:** After upgrading from CAD 7.0(x) to CAD 7.2(1) on a replicated system, agents cannot log in.

**Solution:** If you are upgrading a replicated system, you must shut down replication before doing the upgrade. If you do not shut down replication first, the CAD license files will be lost when the LDAP database entries are reloaded.

If CAD license files are lost after an upgrade, you must manually relicense CAD.

## 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

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](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](mailto: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](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](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](mailto: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](mailto:psirt@cisco.com)

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

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



---

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](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>

Cross-references to H1 Heads in this document (to prevent cross-reference markers from being lost):

- [Obtaining Documentation, page 5](#)
- [Documentation Feedback, page 6](#)
- [Cisco Product Security Overview, page 6](#)
- [Obtaining Technical Assistance, page 7](#)
- [Obtaining Additional Publications and Information, page 9](#)