



# Release Notes for Cisco Agent Desktop 4.6.0

---

**April 29, 2005**

These release notes describe the new features for Cisco Agent Desktop version 4.6.0.21.

Use these release notes in conjunction with the Cisco Desktop Product Suite 4.6.0 documentation, provided on the installation CD.

## Contents

These release notes discuss the following topics:

- System Requirements, page 1
- New and Changed Information, page 2
- Limitations and Workarounds, page 4
- Open Caveats, page 4
- Resolved Caveats, page 6
- Obtaining Documentation, 8
- Obtaining Technical Assistance, page 9

## System Requirements

Cisco Agent Desktop 4.6.0 is compatible with Cisco Intelligent Contact Management (ICM) versions:

- 4.6(2), hot fixes 1–137
- 5.0(0) SR2



---

**Corporate Headquarters:**

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

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

# New and Changed Information

Cisco Agent Desktop 4.6.0.21 includes the following new features:

- Desktop monitoring
- Support of Cisco Outbound Option
- Localization for Japan

## New Software Features

### Cisco Desktop Administrator

#### Desktop Monitoring

The VoIP Monitor administrative window in Cisco Desktop Administrator has been modified to enable the administrator to choose how to monitor specific MAC addresses—via desktop monitoring or server monitoring.

The administrator can check a checkbox next to a listed MAC address to enable desktop monitoring, or select a VoIP Monitor server from a dropdown list to enable server monitoring. These actions are mutually exclusive: an agent phone cannot be monitored by both. However, desktop monitoring can be checked and a VoIP Monitor server can be selected for the same MAC address. In that case, the agent phone is monitored by the desktop monitor. If that fails, the VoIP Monitor takes over.

The administrator can also set a default VoIP Monitor server. The default VoIP Monitor server is used for monitoring those devices not assigned to desktop monitoring or a specific VoIP Monitor server.

#### Cisco Outbound Option

Cisco Desktop Administrator has been modified to enable administrators to set up agent responses to Cisco Outbound Option (COO) calls through the use of task buttons. This new feature is similar to the existing Utility Action feature.

**Note**

---

Cisco Outbound Option requires ICM 5.0(0) or greater.

---

The administrator configures four task buttons to perform the following actions on COO calls:

- Accept
- Skip
- Reject
- Callback/Cancel Reservation

The Accept, Skip, and Reject actions are enabled only in Preview Dialing Mode. The Callback/Cancel Reservation action is enabled only when the agent is in Talking or Wrapup state on a COO call.

COO calls can be dialed in three modes: Predictive, Preview, and Progressive. These modes are configured in ICM.

## Cisco Agent Desktop

### Desktop Monitoring

If an agent is configured by the administrator for desktop monitoring, software on the agent's desktop handles the recording and monitoring requests for that agent. Desktop monitoring is available only on agent desktops that are physically connected to the network through a hard IP phone (Cisco models 7910, 7940, and 7960) or through a media terminated soft phone.

Desktop monitoring avoids the use of SPAN configuration on the Cisco Catalyst switch, which can be difficult to implement and support.

### Cisco Outbound Option

Cisco Outbound Option is available to agents through the use of actions assigned to task buttons on the toolbar. This functionality enables agents to receive both inbound and outbound calls.

### Localization for Japan

Cisco Agent Desktop has been localized for Japan. The interface, online help, and quick reference cards have been translated into Japanese Kanji.

## Cisco Supervisor Desktop

### Localization for Japan

Cisco Supervisor Desktop has been localized for Japan. The interface, online help, and quick reference cards have been translated into simplified Japanese Kanji.

## Enterprise Server

The Enterprise server has been modified by adding the following COO and Cisco E-mail (CEM) Extended Call Context (ECC) variables. These variables are predefined in the Enterprise server's `ssECCs.cfg` configuration file.

- `BAAccountNumber`
- `BABuddyName`
- `BACampaign`
- `BADialedListID`
- `BAResponse`
- `BAStatus`
- `BATimeZone`
- `cisco.cem.Category`
- `cisco.cem.MessageKey`
- `cisco.cem.Priority`

In previous versions of Enterprise server, it was assumed that all ECC variables are prefixed with "user." For 4.6.0, it has been modified to support variables that do not have this prefix.

## IP Phone Agent Server

The IP Phone Agent server configuration file TIAJ.cfg has been modified so that an administrator can set the agent login and password format to be either numeric or alphanumeric.

# Limitations and Workarounds

## Installing Desktop Applications on Windows XP Service Pack 2 Platforms

Windows XP Service Pack 2 (XP-SP2) has increased security features, including a firewall that is automatically enabled.

When you install Cisco Agent Desktop (with or without Media Termination), Cisco Supervisor Desktop, or 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, a user will see a Windows Security Alert when attempting to use the desktop application.

The Windows Security Alert varies depending on how the user is logged in.

- If the user 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 below.

- If the user 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 user should click the **Unblock** button to continue. If the user clicks the **Keep Blocking** button or the **Ask Me Later** button, various features in the desktop application will not work properly. To correct these problems, perform the procedure below.

### Procedure

- 
- Step 1** Log into the PC as the Windows administrator.
  - Step 2** Choose **Start > 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.
    - **Cisco Agent Desktop**—In all cases
    - **MediaClient Module**—In all cases
    - **Cisco Supervisor Desktop**—If Cisco Supervisor Desktop is running on the PC

- **Supervisor Record Viewer**—If Cisco Supervisor Desktop is running on the PC
- **Cisco Desktop Administrator (administrator.exe)**—If Cisco Desktop Administrator is running on the PC
- **Cisco Desktop Administrator (IPCCAdm.exe)**—If Cisco Desktop Administrator is running on the PC
- **Cisco Desktop Administrator (Personnel.exe)**—If Cisco Desktop Administrator is running on the PC
- **Cisco Desktop Administrator (SplkView.exe)**—If Cisco Desktop Administrator is running on the PC
- **Cisco Desktop Administrator (TSSPAdm.exe)**—If Cisco Desktop Administrator is running on the PC

**Step 5** Click **OK**.

---

## 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. For a procedure for testing if a NIC card is fully NDIS-compliant, see [www.cisco.com/en/US/customer/products/sw/custcosw/ps427/prod\\_tech\\_notes\\_list.html](http://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.
- Cisco IP Phone Agent is not localized for Japan.

## CAD and ICM Upgrades

The CAD 4.4 Sync Server is not compatible with ICM 5.0. Therefore, CAD 4.4 must be upgraded to CAD 4.6 before ICM 4.6 is upgraded to ICM 5.0 in order to function correctly.

# Open Caveats

**Table 1** *Open caveats for Cisco Agent Desktop 4.6.0*

<b>DDTS Number</b>	<b>Explanation</b>
CSCma24851	<p>Symptom: Enterprise Data history does not show the correct amount of time spent by a call in the IVR.</p> <p>Condition: This problem occurs in ICM 5.0(0) SR2.</p> <p>Workaround: No workaround is currently available.</p>
CSCma24909	<p>Symptom: Enterprise Data values are sometimes missing when ACD calls are delivered.</p> <p>Condition: This problem occurs in ICM 5.0(0) SR2.</p> <p>Workaround: The CAD code has been revised to fix this problem.</p>
CSCma25282	<p>Symptom: The Media Client executable is not properly shut down when an agent using media termination on an NT workstation exits CAD.</p> <p>Condition: This problem occurs in ICM 5.0(0) SR2.</p> <p>Workaround: No workaround is available.</p>
CSCma26589	<p>Symptom: IP Phone service stops when an instance of Cisco Desktop Administrator is installed on the same box as IP Phone service.</p> <p>Condition: This problem occurs if the IP Phone Agent server is already installed on the box.</p> <p>Workaround: Restart the IP Phone Agent service and the Tomcat service after installing Administrator.</p>

# Resolved Caveats

**Table 2** *Resolved caveats for Cisco Agent Desktop 4.6.0*

<b>DDTS Number</b>	<b>Explanation</b>
CSCma23691	An error occurs when trying to view the CAD Installation Guide.
CSCma24504	After upgrading, the logical contact center is not found in the dropdown list.
CSCma24639	The secondary LDAP server fails to start after installation.
CSCma24702	Blind transfer needs to be a single-step transfer in CAD.

**Table 2** *Resolved caveats for Cisco Agent Desktop 4.6.0*

<b>DDTS Number</b>	<b>Explanation</b>
CSCma24713	If two or more supervisors monitor the same agent at the same time, this may cause the supervisors' desktops to freeze.
CSCma25371	The IP Phone Agent exit softkey does not work when in call.
CSCma25601	Supervisors cannot log in the first time until they have logged in first as a CAD agent.

# Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

### Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

### Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—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 Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

All other trademarks mentioned in this document or Web site 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. (0304R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

