# Release Notes for Cisco CTI OS Enterprise & Hosted Editions, Release 7.2(1)

**January 3, 2008**

# Contents

These release notes discuss the following topics:




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

# Introduction

This document provides installation instructions for CTI OS 7.2(1). This document discusses new features, changes, and caveats for Minor Release 7.2(1) of CTI OS Enterprise and Hosted software. It also contains a list of CTI OS issues resolved by this maintenance release. Please review all sections in this document pertaining to installation before installing the product. Failure to install this maintenance release as described may result in inconsistent CTI OS behavior.

This document is a supplement to the:

- Release Notes for Cisco CTI OS Enterprise & Hosted Editions Release 7.0(0)
- Release Notes for Cisco CTI OS Enterprise & Hosted Editions Release 7.1(1)
- Release Notes for Cisco CTI OS Enterprise & Hosted Editions Release 7.1(2)
- Release Notes for Cisco CTI OS Enterprise & Hosted Editions Release 7.1(3)
- Release Notes for Cisco CTI OS Enterprise & Hosted Editions Release 7.1(4)
- Release Notes for Cisco CTI OS Enterprise & Hosted Editions Release 7.1(5)

These release notes can be found at:
http://tools.cisco.com/support/downloads/go/Platform.x?softwareType=Cisco%20Unified%20Intelligent%20Contact%20Management%20Software%20Releases

The CTI OS 7.2(1) Release Notes must be used in conjunction with the previously mentioned Release Notes.

In addition, the CTI OS 7.2(1) Release Notes are available at:
http://tools.cisco.com/support/downloads/go/Platform.x?softwareType=Cisco%20Computer%20Telephony%20Integration%20Software%20Releases

# About Release 7.2(1)

For all CTI OS Releases 7.1(1) and later, service releases (SR) are being renamed as maintenance releases (MR). Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1) is the second minor release built on CTI OS Release 7.0(0).

Minor Releases are cumulative updates to previous releases. As a result, applying CTI OS Release 7.2(1) installs all the functionality contained in CTI OS 7.0(0) SR0 through SR4, 7.1(1), 7.1(2), 7.1(3), 7.1(4), and 7.1(5), as well as the new 7.2(1) content. Due to this, ensure you read the relevant Release Notes prior to installing Release 7.2(1).

Release 7.2(1) can be installed over CTI OS 7.0(0) SR0 through SR4, 7.1(1), 7.1(2), 7.1(3), 7.1(4), or 7.1(5).

CTI OS 7.2(1) also contains functionality delivered in all known Engineering Specials (ESs) built on CTI OS 7.0 SR0 through SR4, and 7.1(1) through 7.1(5) that were released at least 60 days prior to the release date of 7.2(1). If your system has an ES installed whose functionality is not contained in 7.2(1), the installer displays a warning prior to performing any modifications to the system. The pre-7.2(1) ESs must be uninstalled before the installation of 7.2(1) can be restarted.

For more information, and to obtain a replacement ES to be installed on the system after completing the SR2 installation, refer to the Cisco Bug Toolkit located at:
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

The maintenance release is available on CD and as downloadable installers from cisco.com.

For additional information on the Cisco software support methodology, refer to the *CTI OS Enterprise Maintenance Support Strategy*, available at: http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml (requires login).

Release Notes for *Cisco CTI Object Server*, *Cisco Agent Desktop*, *Cisco E-Mail Manager Option*, *Cisco Support Tools,* and *Cisco Web Collaboration Option* (including *Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender*) are separate documents and are not included as part of these release notes.

For a detailed list of language localizations implemented for different portions of this release, refer to the Cisco Unified ICM/Contact Center Product and System Localization Matrix available at: http://www.cisco.com/application/vnd.ms-excel/en/us/guest/products/ps1846/c1225/ccmigration_09186a008068770f.xls

**Note** The most up-to-date version of these release notes is available on the web at: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html

## About Cisco CTI OS and CTI OS Maintenance Releases

Cisco CTI OS software is a component of Cisco IPCC Enterprise, Cisco ICM Enterprise, Cisco ICM Hosted Edition and System IPCC deployments. CTI OS maintenance releases deliver code updates that resolve issues in CTI OS software. They are made available as part of the CTI OS software maintenance strategy.

As of CTI OS Release 7.1(1), service releases are being renamed as maintenance releases. Cisco CTI OS Release 7.2(1) is the second minor release built on CTI OS Release 7.0(0).

Minor releases for particular CTI OS versions are cumulative; they include code updates present in earlier minor, maintenance and service releases for their respective version. In the case of Release 7.2(1), the earlier minor release was Release 7.1(1).

Release 7.2(1) is a cumulative update to Release 7.1(5). As a result, applying Release 7.2(1) installs all the functionality of Release 7.1(5), as well as the new Release 7.2(1) content. Due to this, ensure you read the CTI OS 7.1(5) Release Notes prior to installing CTI OS Release 7.2(1).

CTI OS Minor Release 7.2(1) incorporates the following minor, maintenance, and service releases:

- Minor Release 7.1(1)
- Maintenance Releases 7.1(2) through 7.1(5)
- Service Releases 7.0(0) SR0 through SR4

CTI OS Release 7.2(1) can be installed over CTI OS 7.1(5), CTI OS 7.1(4), CTI OS 7.1(3), CTI OS 7.1(2), CTI OS 7.1(1) or CTI OS 7.0(0) SR0-SR4. The minor release is available on CD and as downloadable installers from cisco.com.

For additional information on the Cisco software support methodology, refer to the ICM/IPCC Enterprise Maintenance Support Strategy, available at: http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml (requires login).

CTI OS 7.0(0) must be installed prior to installing Release CTI OS 7.2(1). For an explanation of the specifications for ICM/IPCC Enterprise & Hosted Edition Release 7.0(0), see the Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) and 7.1(1) Hardware and System Software Specifications (Bill of Materials), accessible from: http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1626/ccmigration_09186a00804d7607.pdf.

For a detailed list of language localizations implemented for different portions of this release, refer to the Cisco Unified ICM/Contact Center Product and System Localization Matrix available at: http://www.cisco.com/application/vnd.ms-excel/en/us/guest/products/ps1846/c1225/ccmigration_09186a008068770f.xls

**Note** The most up-to-date version of these release notes is available on the web at: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html

### A Note about Product Naming

Cisco IPCC Enterprise Edition has been renamed to Cisco Unified Contact Center Enterprise (abbreviated as Unified CCE).

Cisco IPCC Hosted Edition has been renamed Cisco Unified Contact Center Hosted (abbreviated as Unified CCH).

These new names were introduced for Agent and Supervisor product opening-screens and in documentation that was revised for Release 7.1(1), but they do not yet appear throughout the user interface or documentation. These release notes use the previous naming convention.

# System Requirements

For hardware and third-party software specifications for Maintenance Release 7.2(1), refer to the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, which is accessible from: http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1626/ccmigration_09186a00804d7607.pdf .

Release 7.2(1) updates are also available for CTI OS. The CTI OS 7.2(1) Release Notes are available at: http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_release_notes_list.html

# CTI OS 7.2(1) Compatibility and Support Specifications

This section provides information to help you understand on which CTI OS components CTI OS 7.2(1) can and must be installed. It contains these subsections:

- CTI OS Version Support
- CTI OS Component Support
- Network Environment Support
- Cisco Security Agent

For overall information and restrictions on the product, the customer must also refer to the base Release Notes for Cisco CTI OS version 7.0(0), available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/ctidoc7/ctios7d/cti70rln.pdf .

# CTI OS Version Support

CTI OS 7.2(1) must only be installed on systems running Cisco CTI OS Release 7.0(0) including those nodes where Cisco CTI OS Release 7.0(0) is co-located with Cisco ICM Peripheral Gateways.

CTI OS 7.2(1) has been tested and verified to be compatible with the inter operability criteria for CTI OS Release 7.0(0), 7.1(2), 7.1(3), 7.1(4), and 7.1(5). Additional CTI OS 7.0(0) interpretability support information is available from these sources:

- CTI OS 7.0(0) support information for other Cisco products is listed in the Cisco IP Contact Center Enterprise Edition Software Compatibility Guide, available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/ipctt_cg.pdf.
- CTI OS 7.0(0), ICM, CRM and Operating System interoperability is described in the CTI Compatibility Matrix, available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/ctimatrx.zip.
- CTI OS 7.0(0) third-party platform support information is listed in the Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials), available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/icm70bom.pdf.
- Cisco Security Agent (CSA) for CTI OS, if used, must be the correct version. Support information is available at: http://www.cisco.com/kobayashi/sw-center/contact_center/csa/.
- CTI OS 7.2(1) was tested per the Bill of Materials, and with the latest Microsoft Security Patches installed.

# CTI OS Component Support

A CTI OS 7.2(1) minor release installs files that resolve caveats on different CTI OS 7.2(1) components. The installation program automatically detects the components installed on a machine and installs only those files specific to those components.

This section lists the CTI OS components on which this minor release can be installed, and those on which it cannot.

## Supported CTI OS Components

CTI OS 7.2(1) is compatible with, and must be installed on, the following CT I OS components:

- CTI OS Server
- CTI OS Desktops (Agent and IPCC Supervisor)
- CTI OS Driver for Siebel 7.x
- CTI OS Data Store (Used only in conjunction with CTI OS Driver for Siebel 7.x)
- CTI OS Software Development Kit (SDK)
  - Client Interface Library for C++ (C++ CIL)
  - Client Interface Library for COM (COM CIL)
  - Client Interface Library for Java TM (Java CIL)
  - Client Interface Library for .Net TM (.Net CIL)
  - CTI OS ActiveX Controls
  - Samples

**Note** The ICM release version on a PG must match the release version of CTI OS which is always co-resident. For example: a PG with ICM Release 7.2(1) requires CTI OS Release 7.2(1).

- ICM Outbound Option Dialers
- ICM WebView Server
- System IPCC Enterprise Deployments

**Note** CTI OS 7.2(1) must be installed on all of the components listed above. Installing this minor release on only some of these components in an ICM system can result in inconsistent behavior in the CTI OS software. Be aware that it is not necessary to upgrade CTI OS clients unless you want to access new functionality or a bug fix. Please refer to the *CTI OS Compatibility Matrix* for supported client versions: http://www.cisco.com/application/x-zip-compressed/en/us/guest/products/ps14/c1225/ccmigration_09186a0080264775.zip.

# Network Environment Support

## CTI OS Silent Monitor Does Not Work With All NIC Cards

If agents use supported IP hard phones with their desktops connected to the second port of the phone and if the network is configured to use a VLAN for voice traffic, the network card and driver in the agent desktop PC need to be capable of capturing packets on a different VLAN in order for Silent Monitor to work. This restriction does not apply if the network is not configured for VLANs.

Cisco testing has determined that several NIC cards manufactured by Intel are not capable of capturing packets from a different VLAN. No workaround exists for the Intel 8255x-based PCI Ethernet Adapter cards. A workaround is available for the Intel Pro/1000 and Intel Pro/100 NIC cards; see the following Intel website for information: http://www.cisco.com/application/pdf/en/us/guest/products/ps14/c1221/cdccont_0900aecd800e3149.pdf.

For NIC cards from other manufacturers, there are procedures you can run to determine if your NIC card can capture packets on a different VLAN. If you have Cisco CallManager installed, perform the procedure listed in *the CTI OS Troubleshooting Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)*, Chapter 1, section “Silent Monitor Problems”, symptom “A supervisor has clicked the silent monitor start button, the session seems active (monitored indicator in the agent real-time status window for voice), but after a while the following message box appears”. Ensure that the PC is connected to the second port of the hard phone when you perform this procedure.

## CTI OS Silent Monitor Does Not Work With Network Address Translation (NAT)

Cisco CTI OS Silent Monitor is not supported on network environments where more than one disjoint network is interconnected using Network Address Translation.

## Not All Call Flows Can Be Monitored When Silent Monitoring Mobile Agents

When the silent monitor server is used to silent monitor mobile agents, traffic that does not leave the agent gateway cannot be silent monitored. For example, agent-to-agent and consultation calls between mobile agents that share the same gateway cannot be silent monitored. In most cases, the only calls that can be reliably silent monitored are calls between agents and customers.

# Cisco Security Agent

A standalone Cisco Security Agent for CTI OS Server Software Component is supported with CTI OS/IPCC 7.2(1). The standalone Cisco Security Agent provides intrusion detection and prevention for Cisco CTI OS Server Software Component. Cisco Security Agent removes potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications. It dramatically reduces downtime, widespread attack propagation and clean-up costs. The Agent is provided free of charge by Cisco Systems for use with release 7.2(1) of the Cisco CTI OS Server Software Component. While Cisco highly recommends its installation, it is optional. The "CTI OS Server Software Component" protected by the Cisco Security Agent includes Cisco CTI OS Server (but not the CTI OS Desktops), ICM Enterprise and Hosted Edition 7.2(1), Cisco IP Customer Contact (IPCC) Enterprise and Hosted Edition 7.1(4), Cisco Outbound Option (formerly Blended Agent) 7.2(1), Cisco E-Mail Manager 5.0(0), Cisco Web Collaboration Option 5.0(0) [Cisco Collaboration Server 5.0(0), Cisco Dynamic Content Adapter (DCA) 2.0(1), Cisco Media Blender 5.0(0)], Cisco CTI Object Server (CTI OS) 7.2(1), and Cisco Remote Monitoring Suite (RMS) 2.0(0). The standalone Cisco Security Agent for CTI OS/IPCC, the Installation Guide and the Cisco Security Agent release specific Readme document can be downloaded from: http://www.cisco.com/cgi-bin/tablebuild.pl/csa10-crypto.

The Cisco Security Agent Installation Guide and the Read Me document must be read before installing.

In addition to being specifically tuned for Cisco CTI OS Server Software Component, the standalone Cisco Security Agent for Cisco CTI OS Server Software Component provides support for a select number of Cisco approved third-party applications. These are listed in the 7.0(0) Bill of Materials. ***No other third-party applications are supported.***

Cisco Security Agent requires that any software installed on a CTI OS server, whether Cisco Software, or third-party applications, must be installed into the default directories presented during the installation process. If customers are upgrading and have not installed in default directories (and do not wish to de-install and re-install using the default directories), or if new customers do not want to install in default directories, they should not use Cisco Security Agent.

If you use a third-party software application that is not Cisco-approved, you must purchase and install the Management Center for Cisco Security Agents, because you will then need to modify and maintain your own application-server security policy-something that is not possible with the standalone Agent.

**Note** Using Cisco Security Agent for CTI OS Server Software Component has the potential for adversely impacting your system if not used appropriately. For a discussion of issues and troubleshooting tips, see the document just mentioned. For additional information on Cisco Security Agent, see the Management Center for Cisco Security Agent documentation set at: http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html.

# New and Changed Information

The following sections describe new features and changes that are pertinent to this release.

## Overview

CTI OS Release 7.2(1) is a minor release that contains fixes. Release 7.2(1) is incremental and cumulative, and can be rolled back. CTI OS 7.2(1) contains the following new functionality:

- CallManager (CCM) Based Silent Monitor
- Agent Routing Integration (ARI)
- Russian and Traditional Chinese Localization

## CallManager (CCM) Based Silent Monitor

In addition to the existing silent monitoring capability, Cisco CallManager now provides the capability to perform silent monitoring.

CCM based Silent Monitor provides a supervisor with a means to listen in on agent calls in IPCC call centers that use Cisco CallManager version 6.0 and higher. Supervisors can send Silent Monitor requests to monitor agents without the agent being aware of any monitoring activity. When the CCM based approach is adopted for silent monitoring, the agent's phone is used to mix the media streams of the agent's call. The mix is then sent to the supervisor's phone.

CCM based silent monitor provides the following advantages:

- No NIC card restrictions
- Any 7.x version of any desktop (C++, Java, .Net, Siebel) can be silent monitored provided the agent is not a mobile agent.
- Silent monitor is implemented via a call therefore the silent monitor call is carried on the voice LAN. With CTI OS silent monitor, the silent monitor stream was carried on the data LAN.
- Silent monitor calls are reported as agent-to-agent calls for supervisors. With CTI OS silent monitor, supervisor’s time spent silent monitoring is not tracked.

The following items prevent the use of CCM based silent monitor:

- Agents using phones other than 79x1 phones (7941, 7961, or 7971)
- Agents using IP communicator
- Supervisors using 7.1(x) or earlier desktops
- IPCC 7.1(x)
- CCM 5.x and earlier
- Silent monitoring SRTP streams is not supported
- Mobile agents cannot be silent monitored

## Agent Routing Integration (ARI)

The Agent Routing Integration (ARI) deployment allows the Unified ICM software to select agents and to route calls directly to them.

ARI is implemented by using an ARS PG.

Before ARI was introduced, the method by which Unified ICM interfaced with an Automatic Call Distributor (ACD) was through a customized TDM PG designed specifically for that ACD. Reporting management, agent skill mapping, and routing decisions remained under control of the ACD. It was the role of the ACD (and *not* Unified ICM), to select the agent. Although using TDM-specific PGs remains a viable deployment, the option of using an ARS PG adds flexibility to the Unified ICM environment.

In an ARI deployment with an ARS PG, traditional "ACD functions" move to the Unified ICM. The role of the ACD changes from a “TDM ACD” to an “ACD/PBX” that serves as the telephone switching system. In this role, the “ACD/PBX” provides connections for agent phones and connects a call to an agent, as directed by the Unified ICM Router.

## Russian and Traditional Chinese Localization

In addition to retaining support for localizations in earlier releases, Release 7.2(1) provides localization for Russian and Traditional Chinese. See the *Installation Guide Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)* for a more detailed discussion of localization.

# CTI OS Maintenance Release Installation Planning

This section provides information to help you understand when to install a CTI OS maintenance release and the tasks it involves. It contains the following subsections:

- When to Install a CTI OS Maintenance Release
- Installation Order for CTI OS Components
- CTI OS Maintenance Release Installation Checklists

## When to Install a CTI OS Maintenance Release

Installing a CTI OS release requires temporarily stopping all CTI OS services and CTI OS Client Applications. Therefore, to limit impact to a live CTI OS system, schedule and install CTI OS releases during a maintenance period when your CTI OS system is out of production.

## Installation Order for CTI OS Components

CTI OS releases need to be installed first on the server platform (Side A and B), then on the client components in order to avoid a temporary situation of mismatched components.

## CTI OS Maintenance Release Installation Checklists

Deploying a CTI OS Maintenance Release requires the following general tasks:

- CTI OS Server Installation Checklist
- CTI OS Desktops Installation Checklist
- CTI OS Driver for Siebel 7.x Installation Checklist
- CTI OS Data Store Installation Checklist

- CTI OS SDK Installation Checklist

## CTI OS Server Installation Checklist

- **Schedule a maintenance period for installation**: Because CTI OS release installation requires bringing down a CTI OS system, schedule release installation for a maintenance period when your CTI OS system is out of production.
- **Determine which CTI OS components require release installation**: Consult the CTI OS 7.2(1) Compatibility and Support Specifications section of this document to determine on which CTI OS components this release should be installed.
- **Inventory CTI OS nodes targeted for release installation:** Take an inventory of all CTI OS nodes on which this release will be installed.
- **Install the release on CTI OS nodes:** Install the release on each Peripheral Gateway in your system where CTI OS is co-located. Consult the How to Install CTI OS 7.2(1) section of this document for step-by-step instructions on installing this release. This step also applies to environments where CTI OS is installed not co-located with a Peripheral Gateway (CTI OS Server in its own server host).
- **Test and troubleshoot the installation:** After installation, test your CTI OS system to ensure that it is working properly.

## CTI OS Desktops Installation Checklist

- **Schedule a maintenance period for installation:** Because CTI OS release installation requires bringing down the CTI OS Agent/IPCC Supervisor Desktop, schedule release installation for a maintenance period when your agents are inactive.
- **Determine which CTI OS components require release installation:** Consult the CTI OS 7.2(1) Compatibility and Support Specifications section of this document to determine on which CTI OS components this release should be installed.
- **Inventory CTI OS desktops targeted for release installation:** Take an inventory of all CTI OS desktops on which this release will be installed.
- **Install the release on CTI OS desktops:** Install the release on each Agent/IPCC Supervisor desktop system where a CTI OS desktop is loaded. Consult the How to Install CTI OS 7.2(1) section of this document for step-by-step instructions on installing this release.
- **Test and troubleshoot the installation:** After installation, test your CTI OS Desktop to ensure that it is working properly.

## CTI OS Driver for Siebel 7.x Installation Checklist

- **Schedule a maintenance period for installation:** Because CTI OS release installation requires closing down the Siebel Client running at an agent's desktop or browser, schedule release installation for a maintenance period when your CTI OS system is out of production.
- **Determine which CTI OS components require release installation:** Consult the CTI OS 7.2(1) Compatibility and Support Specifications section of this document to determine on which CTI OS components this release should be installed.
- **Inventory the call centers in the Siebel configuration database targeted for release installation:** Take an inventory of all call centers defined in the Siebel configuration database that will use this CTI OS Driver release.

- **Install the release on the Siebel Communications Server host:** Install the CTI OS Driver release on each Siebel Communications Server where the CTI OS Driver is loaded. Consult the How to Install CTI OS 7.2(1) section of this document for step-by-step instructions on installing this release.
- **Test and troubleshoot the installation:** After installation, test your CTI OS Driver to ensure that it is working properly.

## CTI OS Data Store Installation Checklist

- **Schedule a maintenance period for installation:** Because CTI OS release installation requires closing down CTI OS Data Store, schedule release installation for a maintenance period when your CTI OS system is out of production.
- **Determine which CTI OS components require release installation:** Consult the CTI OS 7.2(1) Compatibility and Support Specifications section of this document to determine on which CTI OS components this release should be installed.
- **Inventory the CTI OS Data Stores in a Siebel Environment targeted for release installation:** Take an inventory of all CTI OS Data Stores used by the CTI OS Driver for Siebel 7.x that will use this release.
- **Install the release on the CTI OS Data Store Server host:** Install the CTI OS Data Store release on each host where the CTI OS Data Store is loaded. Consult the How to Install CTI OS 7.2(1) section of this document for step-by- step instructions on installing this release.
- **Test and troubleshoot the installation:** After installation, test your CTI OS Driver and CTI OS Data Store together to ensure that they are working properly.

## CTI OS SDK Installation Checklist

- **Schedule a maintenance period for installation:** Because CTI OS release installation requires bringing down the developer's programming environment and may require rebooting the workstation, schedule release installation for a maintenance period when your developer is off hours.
- **Determine which CTI OS components require release installation:** Consult the CTI OS 7.2(1) Compatibility and Support Specifications section of this document to determine on which CTI OS components this release must be installed.
- **Inventory developer's workstations targeted for release installation:** Take an inventory of all developer's workstations on which this release will be installed.
- **Install the release on developer's workstations:** Install the release on each developer's workstation where CTI OS SDK is loaded. Consult the How to Install CTI OS 7.2(1) section of this document for step-by-step instructions on installing this release.
- **Test and troubleshoot the installation:** After installation, test your CTI OS SDK to ensure that it is working properly.

# Installation Notes

This section provides important information to be read before installing the Release 7.2(1) update and how to troubleshoot the installation. It contains the following:



# Deploying CTI OS Releases

## CTI OS Server Deployment

If you are installing this release on multiple CTI OS systems, you must install CTI OS releases on each host one at a time.

### How to Deploy CTI OS Server

**Step 1** Logout all the agents from both servers (side A and side B).

**Step 2** Stop all CTI OS and Cisco Security Agent (CSA) services on each peer (side A and side B).

**Step 3** Install the release on side A, following the steps described in How to Install CTI OS 7.2(1).

**Step 4** Restart the CTI OS services on side A. Ensure the newly patched system is running with no errors and comes back on-line.

**Step 5** Once you have confirmed that side A is working correctly, install the release on side B following the steps described in How to Install CTI OS 7.2(1).

**Step 6** Restart the CTI OS services on side B. Ensure the newly patched system is running with no errors and comes back on-line.

**Step 7** Restart CSA on both sides.

**Step 8** Repeat this procedure on the other CTI OS systems.

## CTI OS Desktops Deployment

This section describes how to install the CTI OS Desktop release.

**Caution** The release installer package cannot be used or replaced by any silent installation tool.

**Caution** Component update must be performed only using the installer package provided with the release. You can not simply copy files from one client system to another as a way of avoiding running the installer package at each system.

### How to Install the CTI OS Desktop Release

**Step 1** Logout all the agents and close the client at each host desktop.

**Step 2** Install the release on the host desktop following the steps described in How to Install CTI OS 7.2(1).

**Step 3** Restart the CTI OS Desktop. Ensure the newly patched CTI OS Phone is running with no errors by logging in a call center agent and perform call and agent state control.

**Step 4** Repeat this procedure for the other host desktops.

## CTI OS Driver for Siebel 7.x Deployment

Installing this release on multiple Siebel Communications servers can be done simultaneously.

**Caution** The release installer package cannot be used or replaced by any silent installation tool.

### How to Install the CTI OS Driver for Siebel 7.x Deployment

**Step 1** Logout all the agents using a Siebel CTI client and close the browser, or Siebel application, at each host desktop.

**Step 2** Install the release on the Siebel Communications server following the steps described in How to Install CTI OS 7.2(1).

**Step 3** Restart the Siebel client. Ensure the newly patched CTI OS Driver for Siebel is running with no errors by logging in a call center agent and performing call and agent state control.

**Step 4** Repeat this procedure for the other host desktops.

## CTI OS Data Store Deployment

If you are installing this release on multiple CTI OS Data Store hosts, you must install CTI OS releases on each host, one at a time.

### How to Deploy CTI OS Data Store

**Step 1** Stop all CTI OS and Cisco Security Agent (CSA) services on each host.

**Step 2** Install the release following the steps described in How to Install CTI OS 7.2(1).

**Step 3** Restart the CTI OS Data Store service. Ensure the newly patched system is running with no errors and comes back on-line.

**Step 4** Restart CSA.

**Step 5** Repeat this procedure for the other CTI OS systems.

## CTI OS SDK Deployment

**Caution** The release installer package cannot be used or replaced by any silent installation tool.

### How to Deploy CTI OS SDK

**Step 1** Close all programming environments and any client applications using any of the components in the CTI OS SDK.

**Step 2** Install the release on a developer workstation following the steps described in How to Install CTI OS 7.2(1).

**Step 3** Restart the programming environment or application. Ensure the newly patched CTI OS SDK works appropriately by building one of the examples included in the SDK and logging in a call center agent and performing call and agent state control.

**Step 4** Repeat this procedure for the other developer workstations.

# Limitations and Restrictions

Limitations and Restrictions are provided in the following documents:

- The *Release Notes for Cisco CTI OS Enterprise & Hosted Editions* are available at: http://tools.cisco.com/support/downloads/go/Platform.x?softwareType=Cisco%20Unified%20Intelligent%20Contact%20Management%20Software%20Releases
- The *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, updated for Release 7.2(1), available from http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm
- The *Software Compatibility Guide for Cisco IPCC Enterprise Edition*, available from: http://cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html
- The *Cisco Unified Mobile Agent Guide for Unified CCE* provides information on limitations in the Mobile Agent feature.
- The *IPCC Solution Reference Network Design (SRND) for Cisco IPCC Enterprise Edition (Updated for Release 7.2(1))* provides additional limitations and restrictions.

Release 7.2(1) is a cumulative update and may rectify restrictions as documented in the CTI OS Release 7.0(0) SR0 though SR2, and CTI OS 7.1(1) through CTI OS 7.1(5) Release Notes.

# Important Notes

## Silent Monitoring and System IPCC

Instead of re-running the CTI OS Server setup, System IPCC administrators can set the Silent Monitor mode in the System IPCC Web Administration tool by performing the following:

**Step 1** Select **System Management > Machine Management > Machines**

**Step 2** From the Machines page, run the Machine Wizard for each machine with the role "Agent/IVR Controller".

**Step 3** On the IPCC Network page of the wizard, select one of the following:

- CTI OS based
- Cisco CallManager based
- Disabled

**Step 4** Finish the wizard for the change take effect.

-or-

Go directly to the IPCC Network page for each Agent/IVR Controller by selecting **System Management > Machine Management > IPCC Network**, and save your silent monitor mode selection.

## Cisco CallManager Configuration for Agent Phones

The agent configuration (set on the Cisco CallManager Administration Directory Number Configuration web page for each IPCC line) should be the following:

- Maximum Number of Calls = 4
- Busy Trigger = 2

## Miscellaneous Caveat Information

### CSCsi84066

During the patching process the following Cisco Data Store registry keys are deleted and must be replaced after the patch is installed:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Ctios\ObjectStoreServerSocket]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Ctios\ObjectStoreServerSocket\Connections]

  "HeartbeatIntervalMs"=dword:0000ea60

  "HeartbeatRetrys"=dword:00000005

  "ListenPort"=dword:0000a42d
- [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Ctios\ObjectStoreServerSocket\Logging]

  "TraceFileName"="ObjectStoreServerSocketLog"

"TraceMask"=dword:00000007

**CSCsb99693**

The CTI OS 7.0 Client Installer installs CTI OS 6.0 documentation. This caveat has been closed.

**CSCsg97026**

CTI OS 7.2(1) allows a maximum of two monitor mode connections per CTI OS Server by default. Any attempt to connect more than two monitor mode connections will result in a CTIOSFailure event. The maximum number of monitor mode connections is configurable using the MaxMonitorModeConnections registry setting. Please see the *CTI OS System Manager's Guide* for details. This caveat has been resolved and verified.

**CSCsg26618**

The error message **CTIERR_BIB_RESOURCE_NOT_AVAILABLE: "Device not capable"**applies to older phones not capable of R&M irrespective of BIB configuration. IPCC Error[13139] Agent device doesn't support monitoring or its build-in-bridge is not enabled, please check your CCM configuration.

In the jtapi log file, the cause is: CAUSE_SERVOROPTNAVAILORIMPL

13139 = PERERR_GW_E_THREADSUPERVISECALL_SM_AGENT_PHONE_NOT_ MONITORABLE.

The error message **CTIERR_BIB_NOT_CONFIGURED: "BIB not configured"** applies to devices that are capable of R&M but that have BIB disabled.

IPCC Error[13144] Monitoring request has encountered error, please make sure that the Built-In-Bridge is turned on and the phone has the monitoring capability.

In the jtapi log file, the cause is: CAUSE_RESOURCES_NOT_AVAILABLE

13144 = PERERR_GW_E_THREADSUPERVISECALL_SM_EXCEPTION_START_MONITOR

This is an open CallManager issue.

# CTI OS 7.2(1) Installation and Uninstallation

## Installing CTI OS 7.2(1)

Follow these steps on each CTI OS component on which you install this release.

### How to Install CTI OS 7.2(1)

**Step 1** Log into the CTI OS node under an account with administrator privileges for the local machine.

**Step 2** If upgrading a CTI OS Server or CTI OS Data Store host, use the ICM Service Control utility to stop all CTI OS services running on the node, and then close the ICM Service Control utility.

**Step 3** If upgrading CTI OS Desktops, stop all phones running at the host desktop.

**Step 4** If upgrading CTI OS Driver for Siebel, stop all Siebel clients.

**Step 5** If upgrading CTI OS SDK, stop all the programming environments.

**Step 6** If installed, stop the Cisco Security Agent (CSA) service.

**Step 7** Start the release installation by running **CTIOS7.2(1).exe**.

**Note** Upon startup, the CTI OS Release installer may disappear from the screen for approximately one minute. When it returns there may be a grey screen displayed for approximately ninety seconds. During these periods, the system displays no other visual indicators that the installer is running. *This is normal behavior and does not signify a "hung" installer.*

Allow at least three minutes before suspecting a hung installer. If after this period you do suspect that the installation has hung, use Windows Task Manager to check its status and, if necessary, end the process. Do not launch a new instance of the installer before ending the previous one. Doing so could result in a faulty installation.

If you mistakenly launch multiple concurrent instances of the Release installer, close all instances and then start the process again.

**Step 8** If prompted during the installation, click **Yes** to allow the installer to replace files as necessary.

**Step 9** When prompted, click **Finish** to complete the installation.

**Step 10** After the installation is complete, restart the CSA service.

**Step 11** If you installed CTI OS Server or CTI OS Data Store, use the CTI OS Service Control utility to restart all CTI OS services.

**Step 12** If the host is part of a duplexed CTI OS system, do not perform this step. Instead, restart the CTI OS services in the order indicated in the *CTI OS Server Deployment* section of this document.

**Step 13** If you installed CTI OS Desktops, restart the desktops.

**Step 14** If you installed CTI OS Driver for Siebel, restart the Siebel clients.

**Step 15** If you reinstalled CTI OS SDK, restart the programming environment.

## Uninstalling CTI OS 7.2(1)

If desired, you can uninstall CTI OS 7.2(1) from any CTI OS host on which it is installed.

**Note** Since removing a CTI OS release requires stopping CTI OS services and CTI OS clients, it must be done during a maintenance period when your CTI OS system is out of production.

To function properly, CTI OS 7.2(1) must be installed on all the CTI OS components it supports. Therefore, if you remove it from one node in a system and do not plan to reinstall it, remove it from all other hosts as well.

To uninstall CTI OS 7.2(1), perform the following on each CTI OS host it is installed on.

### How to Uninstall CTI OS 7.2(1)

**Step 1** Log into the CTI OS host under an account that has administrator privileges for the machine.

**Step 2** If installed, stop the CSA service.

**Step 3** If you are uninstalling CTI OS Server or CTI OS Data Store using the CTI OS Service Control utility, stop all CTI OS services running on the host.

**Step 4** Select **Start > Settings > Control Panel > Add Remove Programs**.

**Step 5** Select and uninstall any engineering specials on this release

**Step 6** Select **Cisco Release 7.2(1)**.

**Step 7** Click **Change/Remove**.

**Step 8** Restart all CTI OS services and clients on each host.

**Step 9** If installed, restart the CSA service.

# Caveats

## Resolved Caveats in This Release

This section lists caveats specifically resolved by CTI OS 7.2(1). You can also find the latest resolved caveat information through the Bug Toolkit, an online tool available for you to query defects according to your own needs.

Caveats in this section are ordered by CTI OS component, severity, and then identifier.

*Table 1 Resolved Caveats for Cisco CTI OS Enterprise & Hosted Editions Release 7.2(1)*

| Identifier | Component | Sev | Headline |
|---|---|---|---|
| CSCsg65792 | ctios.ctiosclient | 3 | Internationalization Kit Cannot Build Due to Read-Only Files |
| CSCsi77092 | ctios-server | 2 | Personal Callback time mismatch with CTI desktop |
| CSCsh25508 | ctios.server | 3 | Registry fails to display correct version when 7.1 is installed |
| CSCsh26512 | ctios.server | 4 | Installation has incorrect default value in ServicesMask |
| CSCsh46739 | documentation | 3 | CTI OS Desktop Client Behavior not as documented in Aspect Environment |

## Bug Toolkit

### How to access the Bug Toolkit

**Step 1** Go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

**Step 2** Log on with your Cisco.com user ID and password.

**Step 3** Click the **Launch Bug Toolkit** hyperlink.

**Step 4** If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for Cisco ICM/IPCC Enterprise and Hosted Editions, go to the "Search for bugs in other Cisco software and hardware products" section, and enter **Cisco Unified Intelligent Contact Management Enterprise** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco Unified Intelligent Contact Management Enterprise**.

**Step 5** Click **Next**. The Cisco Unified Intelligent Contact Management Enterprise search window displays.

**Step 6** Choose the filters to query for caveats. You can choose any or all of the available options:

**a.** Select the Cisco Unified Intelligent Contact Management Enterprise Version:

- Choose the major version for the major releases.

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information.

  A revision release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

**b.** Choose the Features or Components to query; make your selection from the "Available" list and click **Add** to place your selection in the "Limit search to" list.

To query for all caveats for a specified release, choose "All Features" in the left window pane.

**Note** The default value specifies "All Features" and includes all of the items in the left window pane.

**c.** Enter keywords to search for a caveat title and description, if desired.

**Note** To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

**d.** Choose the Set Advanced Options, including the following items:

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the Fixed check box for resolved caveats.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

**e.** Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query. You can modify your results by submitting another query and using different criteria.

# Open Caveats in This Release

This section contains a list of defects that are currently pending in CTI OS 7.2(1).

If you have an account with Cisco.com, use the Bug Toolkit to find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than is reflected in this document. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Caveats in this section are ordered by CTI OS component, severity, and then identifier.

*Table 2 Open Caveats for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)*

| Identifier | Component | Sev | Headline |
|---|---|---|---|
| CSCsi62659 | cti-toolkit-agent | 3 | IPCC Error 10148 Third Party Request Already Outstanding |
| CSCsh30904 | ctios.api | 3 | .NETCombophone and JavaTestphone cannot delete call var via call grid |
| CSCsg65792 | ctios.ctiosclient | 3 | Internationalization Kit Cannot Build Due to Read-Only Files |
| CSCsb99693 | ctios.ctiosclient | 4 | CTIOS 7.0 Client Installer Installs 6.0 Documentation |
| CSCsi77092 | ctios-server | 2 | Personal Callback time mismatch with CTI desktop |
| CSCsi84124 | ctios-server | 3 | Skill Group Name appears as [?] on CTI OS Agent and Supervisor Desktops |
| CSCsi84066 | patch | 3 | CDS registry gets removed after running 7.2.1 in a special case |
| CSCsi53639 | setup | 3 | CTIOS Reg keys lost during upgrade |
| CSCsh30367 | siebel-driver | 3 | Driver Crashing Due to Invalid Paramaters From Siebel |
| CSCsj13049 | silent-monitor | 3 | Silent Monitor has not been qualified with WinpCap 3.1 |

# Documentation

## Related Documentation

Documentation for Cisco CTI OS Enterprise and Hosted Editions, as well as most related documentation, is accessible from: http://www.cisco.com/en/US/products/sw/custcosw/ps14/tsd_products_support_series_home.html.

- Release Notes for Cisco CTI OS Enterprise & Hosted Editions Release 7.0(0): http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_release_notes_list.html.
- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco E-Mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender), Cisco Customer Voice Portal (CVP), Cisco IP IVR, Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).
- Also related is the documentation for Cisco CallManager.
- Technical Support documentation and tools can be accessed from: http://www.cisco.com/en/US/support/index.html.
- The Product Alert tool can be accessed through: http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.

## Additional Documentation

This section contains new documentation that may not be available in the documentation set at the time of release.

None.

## 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: http://www.cisco.com/

You can access international Cisco web sites at: 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: 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: 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.

# Field Alerts and Field Notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into www.cisco.com; then access the tool at: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en.

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at: 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: 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: 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 non emergencies.

- For Non emergencies—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: 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: 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: 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: 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: 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: 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: 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: 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: http://www.cisco.com/go/iqmagazine, or view the digital edition at: 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.