Release Notes for CiscoWorks Common Services 2.2 (Includes CiscoView 5.5) on Solaris

These release notes are for use with the CiscoWorks Common Services 2.2 (formerly CD One) running on a Solaris platform.

These release notes provide:

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

New Features

CiscoWorks Common Services Release 2.2 contains the following new features:

- AAA-ACS mode—The Access Control Server (ACS), that provides Authentication, Authorization, and Accounting (AAA) Security services is used for user authentication and authorization and meets the secured device view requirements.
- User Session Management—This feature helps to pass the session data back and forth between two different servlet engines, Tomcat and JRunProxyServer.
- Database Password Encryption—This helps to provide confidentiality for database passwords which were earlier stored as plain text.
- Report Generation—You can customize your report by selecting the required modules in the Collect Server Info dialog box. By default, reports for all the modules are generated. You can run Collect Server info for individual modules.
- Install—Apart from the existing Typical and Custom installations, a third installation type is introduced - Express. If you choose Express install, you can reduce the number of user interactions during the install process. The Express install is faster compared to the Typical and Custom install types.
- MDC Support Utility—The Multi Device Controller (MDC) Support utility collects log files, configuration settings, memory information, complete system information, process status, and host environment information into a deliverable tar file.

  The MDC Support Utility also queries the Core Client Registrar (CCR) for any other support utilities registered and also runs them. Other Management Center (MC) applications should register their own support utilities which will collect their relevant data.
- MC Application Administration Server (MAAS)—MAAS is used for managing the Management Center (MC) applications. The features available are license management, backup and restore, setting the user preferences, selection of login module, selection of SSL certificate, changing the database credentials and viewing different logs.

CiscoWorks Common Services Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the CiscoWorks Common Services documentation that is available.

Table 1 CiscoWorks Common Services Documentation

Document Title	Available Formats
Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Solaris	• PDF on the product CD-ROM. • On Cisco.com: a. Log into Cisco.com. b. Select **Products & Services > Network Management CiscoWorks > CiscoWorks Common Services Software > Technical Documentation > Installation Guides Books**. • Printed document available by order (part number DOC-7815431=).[1]
User Guide for CiscoWorks Common Services	• PDF on the product CD-ROM. • On Cisco.com: a. Log into Cisco.com. b. Select **Products & Services > Network Management CiscoWorks > CiscoWorks Common Services Software > Technical Documentation > User Guide Books**. • Printed document available by order (part number DOC-7815301=).[1]
CiscoWorks Common Services online help	• Select an option from the navigation tree, then click **Help.** • Click the Help button in the dialog box.

1. See the "Obtaining Documentation" section on page 61.

Time Zone Acronyms and Offset Settings

Table 2 shows time zone acronyms supported in the CiscoWorks applications that use the time zone feature.

- Column 1—alphabetically lists the supported CiscoWorks time zone acronyms. Change Audit reports may display time zone information differently.
- Column 2—lists the spelled out time zone definition.
- Column 3—lists the area covered by the time zone.
- Column 4—lists the column's offsets from Greenwich mean time (GMT).
- Column 5—lists the time zone setting for that zone's server and
- Column 6—lists the resulting output in reports.

If you generate reports, the output will vary depending on whether the data has been processed through Perl or Java. Table 2 also provides possible output for either case scenario.

To ensure that time zones are translated correctly—especially when your devices, servers, and clients are in different time zones—follow these guidelines:

- When configuring time zones on managed devices, use the acronyms listed in the *Time Zone Acronym Setting on Device* column. To set time zones on devices, use the command described in the device-specific Command Reference documentation.
- The device should be configured to send syslogs with the appropriate timezone acronym that indicates whether daylight savings is in effect at the time of sending the syslog. This is to ensure that the syslog analyzer or Essentials uses the correct acronym for time conversion.
- When configuring time zones on CiscoWorks servers, use the supported values in the *Time Zone Setting on Server* column.

Note Changes made to the system time zone from outside CiscoWorks applications might not be reflected in already-running CiscoWorks applications. After changing the time zone, restart all CiscoWorks applications.

Table 2 Supported Server Time Zones

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
ACT	Australia Central Time	Australia/ Darwin	+9:30	Adelaide	GMT +9:30	ACT
AEST	Australia Eastern Standard Time	Australia/ Sydney	+10:00 +11:00 (DST)	Brisbane	GMT +10:00 GMT +11:00 (DST)	AEST
AET	Australia Eastern Time	Australia/ Sydney	+10:00	Brisbane	GMT +10:00 GMT +11:00 (DST)	AET
AHST	Alaska-Hawaii Standard Time	Hawaii/ Honolulu	-10:00	Hawaii	GMT -10:00	HST
ART	Arabic Egypt Standard Time	Africa/Cairo	+2:00 +3:00 (DST)	Cairo	GMT +2:00 GMT +3:00 (DST)	ART
CCT	China Coast Time	Asia/ Shanghai	+8:00	Beijing	GMT +8:00	CST
CDT	Central Daylight Time	United States/ Chicago	-5:00	Central Time	GMT -5:00	CDT (DST) CST
CET	Central European Time	Spain/Madrid	+1:00 +2:00 (DST)	Madrid	GMT +1:00 GMT +2:00 (DST)	CEST
CST	Central Standard Time	United States/ Chicago	-6:00	Central Time	GMT -6:00	CST CDT (DST)
CTT	China Taiwan Time	Asia/ Shanghai	+8:00	Beijing	GMT +8:00	CST

Table 2 Supported Server Time Zones (continued)

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
EAST	East Australian Standard Time	Australia/ Queens Island	+10:00	Brisbane	GMT +10:00	EAST
ECT	European Central Time	Europe/Paris	+1:00 +2:00 (DST)	Paris	GMT +1:00 GMT +2:00 (DST)	CEST
EDT	Eastern Daylight Time	United States/ New York	-4:00	Eastern Time	GMT -4:00	EST EDT (DST)
EST	Eastern Standard Time	United States/ New York	-5:00	Eastern Time	GMT -5:00	EST EDT (DST)
FWT	French Winter Time	France/Paris	+1:00 +2:00 (DST)	Paris	GMT +1:00 GMT +2:00 (DST)	CEST
GMT	GMT Standard Time	Africa/ Casablanca	None	Greenwich Mean Time	GMT +0	GMT
HST	Hawaiian Standard Time	Pacific/ Honolulu	-10:00	Hawaii	GMT -10:00	HST
JST	Japan Standard Time	Asia/Tokyo	+9:00	Tokyo	GMT +9:00	JST
MDT	Mountain Daylight Time	United States/ Denver	-6:00	Mountain Time	GMT -6:00	MDT (DST) MST
MET	Middle European Time	Spain/Madrid	+1:00 +2:00 (DST)	Madrid	GMT +1:00 GMT +2:00 (DST)	CEST

Table 2 Supported Server Time Zones (continued)

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
MEWT	Middle European Winter Time	Spain/Madrid	+1:00	Madrid	GMT +1:00 GMT +2:00 (DST)	CEST
MST	Mountain Standard Time	United States/ Denver	-7:00	Mountain Time	GMT -7:00	MST MDT (DST)
PDT	Pacific Daylight Time	United States/ Los Angeles	-7:00	Pacific Time	GMT -7:00	PDT (DST) PST
PST	Pacific Standard Time	United States/ Los Angeles	-8:00	Pacific Time	GMT -8:00	PST PDT (DST)

Table 2 Supported Server Time Zones (continued)

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
UTC	GMT Standard Time	Great Britain/ London	None	Greenwich Mean Time	GMT +0	GMT
ZP4	Zone 3	Russia/ Moscow	+4:00	Not Supported	GMT +4:00	ZP4

Multi-Homed Machines

A multi-homed machine is a machine that has multiple NIC cards, each configured with different IP addresses. To run CiscoWorks Common Services on a multi-homed machine, there are two requirements.

- First, all IP addresses must be configured in DNS.
- Second, because of restrictions with CORBA, only one IP address can be used by the client/browser to access the server. You must select one IP address as the external address, with which the client will login to the CiscoWorks server.

To select an IP address, modify the gatekeeper file located in /opt/CSCOpx/lib/vbroker/gatekeeper.cfg. Replace every instance of *external-IP-address* with the external IP address you choose, and remove the "#" character, from the following:

- #vbroker.gatekeeper.backcompat.callback.host=*external-IP-address*
- #vbroker.se.exterior.host=*external-IP-address*
- #vbroker.se.iiop_tp.host=*external-IP-address*
- #vbroker.se.interior.host=*external-IP-address*

After modifying the gatekeeper file, restart the Daemon Manager by entering

`/etc/init.d/dmgtd start.`

Operating System Upgrade

If you upgrade the operating system after CiscoWorks Common Services is installed, you must re-install CiscoWorks Common Services.

Re-installing CiscoWorks Common Services will allow the installation process to check for required patches. Install any missing solaris patches. For a list of required patches, see Chapter 1 of *Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Solaris*.

If CiscoWorks does not operate properly after installing all necessary patches, check the permissions on the directory *install-directory*/objects/dmgt/ready. Administrators and casusers must have full access. If the permissions are incorrect, stop the daemon manager, change the permissions, and start the daemon manager again.

Caution If CiscoWorks Common Services is run without the required patches, it will not function properly.

Note To look up this topic on Bug Navigator II, use bug ID CSCdt32795. For more information on using Bug Navigator II, see the "Known and Resolved Problems" section on page 16.

Support Information

CiscoWorks supports the following:

- Operating System—CiscoWorks supports both the English and Japanese versions of Solaris 2.7 and 2.8 operating systems.

Note CiscoWorks Common Services 2.2 supports only US-English and Japanese versions of Solaris Operating Systems. It does not support any other language version. Set the default locale to US-English for US-English version and Japanese for Japanese version.

- Browser—CiscoWorks supports both the English and Japanese versions of the following browsers:
  - Netscape Navigator 4.76 for Solaris 2.7 and Solaris 2.8 clients.
  - Netscape Navigator 4.78, and 4.79 for Windows 2000 Professional with Service Pack 3, and Windows XP with Service Pack 1.
  - Internet Explorer 6.0 (version 6.0.2600.0000).
  - Internet Explorer 6.0 with Service Pack 1 (version 6.0.2800.1106).
- Hardware—CiscoWorks supports Sun Sparc Ultra 10. CiscoWorks supports Ultra SPARC III machines such as Sun-Fire-280R, Netra-T4, Sun Blade 1000 too.

Java Support

CiscoWorks uses two types of Java. Certain applications use the browser's native Java Virtual Machine (JVM), while others use Sun's Java Plug-in. In order for CiscoWorks to function correctly, you must be using the correct version of Java.

The supported native JVM versions are as follows:

- Microsoft Internet Explorer 6.0—JVM 5.0.0.3802 or later.

Note As part of Microsoft settlement agreement with Sun, Microsoft will stop including the Microsoft VM in new releases of Windows. For details, refer to the following URL:
http://www.microsoft.com/windowsxp/pro/evaluation/news/jre.asp

This has an impact on CiscoWorks because it requires Java environment to operate. If your Windows clients have not been upgraded, CiscoWorks will continue to work. Windows XP clients with Service Pack 1A or later, will not work. However, Windows XP clients with Service Pack 1 are not affected.
Cisco is investigating alternate solutions for inclusion in future releases.

- Netscape Navigator 4.7x—the correct version of JVM is installed.

The supported Java Plug-in version is 1.3.1 for both Solaris and Windows. The Plug-in version is independent of the browser used.

Installing Java Plug-in

You can install the Java Plug-in either on Internet Explorer or on Netscape Navigator. You can also manually install it.

- Internet Explorer—When you attempt to launch any CiscoWorks application that uses the Java Plug-in for the first time, Internet Explorer will automatically install the correct Java Plug-in version for you.
- Netscape Navigator—When you attempt to launch any CiscoWorks application that uses the Java Plug-in for the first time, CiscoWorks will redirect you to a page from which you can download and install the correct Java Plug-in version.
- Manual Installation—To manually install the Java Plug-in, refer to Chapter 3 of *Getting Started with the CiscoWorks Server.*

Note CiscoWorks only supports the Java Plug-in versions mentioned above. Installing a different version, including a newer version, can cause CiscoWorks to malfunction.

To see Java related messages, look in the Java console. To do this, enable and then open the Java console. The two Java consoles involved are:

- Native JVM's Java console
- Java Plug-in's Java console.

To enable the native JVM console when using Internet Explorer:

Step 1 Select **Tools > Internet Options > Advanced.**

Step 2 Click **Java Console.**

Step 3 Select **View > Java Console** to open the console**.**

To enable the native JVM console when using Netscape Navigator:

Step 1 Select **Preferences > Advanced > Enable Java.**

Step 2 Select **Communicator > Tools > Java Console** to open the console**.**

To enable the Java Plug-in console when using Windows:

Step 1 Select **Start > Settings > Control Panel.**

Step 2 Double-click **Java Plug-in.**

Step 3 Select **Enable Java Console.**

The Java Plug-in console will automatically open when you launch an application that uses it.

JSSE is used along with Java Plug-in 1.3.1 for SSL support on the clients. When you invoke CiscoWorks for the first time, in SSL mode from the browser:

- JSSE jars will be downloaded from the server, and will be installed in the Plug-in installation directory on the client, as an add-on.
- For the first time, java.policy file will be updated.

You will be asked to restart the browser after this.

Integrating with Third-Party Vendors

Use the Integration utility to integrate Cisco device information and Cisco applications into SNMP management platforms such as HP OpenView Network Node Manager. This utility allows you to launch CiscoView from an SNMP platform even when CiscoView is running on a different machine than the NMS. It also allows you to integrate other applications into NMS menus.

When CiscoView is installed on the same machine as the target NMS, the Integration utility runs as part of a single CiscoView install. However, when the target NMS is installed on a different machine, the utility walks you through the steps required to integrate Cisco device information and applications into an SNMP management platform. You might need to run the Integration utility to:

- Change your Cisco.com login information.
- Change your CiscoWorks server location.
- Register a new application.
- Change the NMS with which you wish to integrate your Cisco applications.

The following topics are described next:

- Integration Utility Features
- Using the Integration Utility

Integration Utility Features

Use the Integration utility to:

- Download the NMIDB (Network Management Integration Data Bundle) from Cisco.com.
- Prompt for additional configuration information that might not be available to register each application. This information is used to integrate the Cisco applications with the NMS console menu. In some cases, the NMS allows you to double-click on the device icon in the topology map of the NMS console to invoke an application.
- Run an adapter script to integrate the icons, MIBs, and applications into the NMS. You can select an adapter script from the list of NM adapters provided with this utility. New NM adapters can be downloaded and added to the list.

Using the Integration Utility

You can perform certain tasks using the Integration utility, as described in Table 3.

Table 3 Integration Utility Tasks

Task	Description
Starting the utility	Depending on your platform, you can start the Integration utility: • From a UNIX platform: a. Use a Telnet utility to open a connection to the system on which the Integration utility is installed. b. Navigate to the CiscoWorks /bin directory. c. Set the X display environment on your X server. Start the utility by entering `./nmic.sh` on the command line. • From a Windows platform: Click Start > Programs > Change Integration Options. or From the command line, navigate to the CiscoWorks /bin directory. Enter the following script on the command line: `.\nmic.exe`

Table 3 Integration Utility Tasks (continued)

Task	Description
Downloading the Data Bundle	The Network Management Integration Data Bundle (NMIDB) contains the icons and configuration files specific to a Cisco device platform. NMIDB also contains MIBs and the application registration information used to register Cisco applications into the NMS. You can download an NMIDB from a file on your local machine, from Cisco.com, or from another system, or use an already downloaded file.
Registering the Applications	The application registration information is used to integrate Cisco applications with the NMS console menu. The Applications Registration dialog box displays user applications that are to be integrated into the NMS menu. This information is then extracted from the NMIDB. There is one tab for each application.
Running the Adapter Script	The Adapter scripts integrate icons, MIBs, and applications with NMS. The Choose Adapter dialog box provides both the Adapters available and their descriptions. The Adapter script checks whether the NMS exists on the machine before integration.

For more information about Integration utility, refer to the online help.

Note NM integration runs automatically when you download a device package through the Package Support Updater.

Documentation Errata

When reading the "Adding and Deleting Device Support" topic in the CiscoView 5.5 online help, note that Step 4 in the "CiscoWorks UNIX users" section should read: From your CiscoView server, choose **Start > Programs > CiscoWorks for Windows** [or] **CiscoWorks > Package Support Updater**.

Note For more information on Package Support Updater, refer to the "Package Support Updater" section in *Using CiscoView 5.5*.

Known and Resolved Problems

Tables 4 to 10 describe the problems known to exist in this release; Tables 11 and 12 describe the problems resolved since the last release of CiscoWorks Common Services.

Note To obtain more information about known problems, access the Cisco Software Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl (You will be prompted to log into Cisco.com.)

The CiscoWorks Common Services known problems are broken down into the following sections:

Installation Known Problems

Table 4 Installation Known Problems

Bug ID	Summary	Explanation
CSCin35996	Administration folder under VPN / Security Management Solution is missing.	After you upgrade from CD One, 5th Edition or CD One, 4th Edition to CiscoWorks Common Services 2.2, the Administration folder under VPN / Security Management Solution might be missing. This occurs only if you install a Management Center (MC) application in the system, before the upgrade. An error message appears in the install log. Workaround: Enable Core services manually. In cshell: 1. /etc/init.d/dmgtd stop 2. setenv LD_LIBRARY_PATH /opt/CSCOpx/objects/db/lib:/opt/CSCOpx/objects/dmgt:/opt/CSCOpx/MDC/lib; 3. Navigate to *$NMSROOT*conf/cmf/bin; 4. *$NMSROOT*/bin/perl CMFEnable.pl -force Core, System; 5. /etc/init.d/dmgtd start
CSCin36414	Installation or uninstallation aborts during dependency check.	Installation or uninstallation displays the message `Out of memory, exiting` during dependency check, and aborts. This problem occurs when the swap space is very less. Workaround: Increase the swap space before installation or uninstallation.

Table 4 Installation Known Problems (continued)

Bug ID	Summary	Explanation

CSCsa34490	CiscoWorks fails to install on Solaris 2.8 if the Sun Patch 110934-20 or later is installed. However, this problem does not affect Solaris 2.7.	CiscoWorks fails to install on Solaris 2.8 with the following errors:
		`ERROR: /opt/CSCOpx/setup/CSCOmd.info not found.`
		`ERROR: GetProperty called with undefined package name: CSCOmd.`
		`ERROR: /opt/CSCOpx/setup/CSCOmd.info not found.`
		`ERROR: GetProperty called with undefined package name: CSCOmd.`
		`installf: ERROR: invalid number of arguments for </opt/CSCOpx/objects/web/logs`
		`installf: ERROR: ftype <d requires all fields to be specified`
		`ERROR: Configuration of the WebServer was not sucessful.`
		`installf: ERROR: invalid number of arguments for </opt/CSCOpx/www/classpath/com/cisco/nm/cvw/devpksinstallf: ERROR: ftype <d requires all fields to be specified`
		`ERROR: unregister daemons "JRunProxyServer" failed.`
		`:Connection refused ERROR:save failed Add failed, record already exists., Error 0.`
		Workaround:
		• Revert the Sun Patch 110934-20 to an previous version; Sun Patch 110934-19 or the earlier versions do not cause these errors.
		Or,
		Caution The following workaround gives the *install user* root previleges. If you cannot provide the install user root privileges, and you cannot revert the Sun Patch 110934-20, rebuild a Solaris server without this patch.

Table 4 Installation Known Problems (continued)

Bug ID	Summary	Explanation

CSCsa34490 (contd.)	CiscoWorks fails to install on Solaris 2.8 if the Sun Patch 110934-20 or later is installed. However, this problem does not affect Solaris 2.7.	• If you cannot revert the patch:
		– Change the UID of the install user on the system.
		To do this:
		1. Backup the /etc/passwd file.
		2. Edit this file to change the third column from the current value to zero.
		`For example: If there is an entry like:`
		`install:x:1001:1001:Install user:/:`
		`Change this to:`
		`install:x:0:1001:Install user:/:`
		`Save the changes to /etc/passwd.`
		– If an install user does not exist in the system, you have to create one and give it the UID of 0.
		To do this:
		1. Backup the /etc/passwd file.
		2. Edit this file to add:
		`install:x:0:1:Install user:/:`
		3. Save the changes to /etc/passwd.
		After you create the install user or modify the existing UID, re-run all of the desired CiscoWorks installations. Now, revert the changes to the /etc/passwd file.
		Caution Ensure that you revert the changes to the /etc/passwd file after the installations.

Table 4 Installation Known Problems (continued)

Bug ID	Summary	Explanation
CSCin30836	CiscoWorks Common Services 2.2 installation hangs on Solaris 2.8.	This happens when reinstalling or upgrading over a broken installation. Workaround: Clean up the broken installation and then install CiscoWorks Common Services 2.2.
CSCin26986	Reference to point patches exists even after upgrade.	Even after upgrading to the newer version of the product, the patches that were applied to previous version are listed in the Application and Versions page. Workaround: The information though misleading, does not impact the proper functioning.
CSCin21594	Installation hangs or slows down when you install on a mounted path.	Installation on a mounted path may slow down or hang because of the slow response of the remote server. Workaround: 1. Abort the installation. 2. Copy the image locally. 3. Start installation.
CSCin09615	Warning appears after installation if mount path has special character.	When the setup dir name contains '#' character, the admin and guest user passwords will not be changed. Workaround: Remove special characters from the mount point.

Table 4 Installation Known Problems (continued)

Bug ID	Summary	Explanation
CSCdz88260	Package check errors are displayed on upgrading CD One, 4th Edition to CiscoWorks Common Services 2.2.	After direct upgrade from CD One, 4th Edition to CiscoWorks Common Services 2.2, a package check for CSCOeds fails for namedfilter.str. The following error is displayed: `pkgchk CSCOeds failed. /opt/CSCOpx/lib/eds/filter/namedfilter.str permissions <0640> expected <0755> actual` Workaround: None. This does not affect the functionality.
CSCdz11099	Incorrect file permissions for a few files after Remote Upgrade.	After remote upgrade, a package check for CSCOxrts fails for file permissions for the files CRMExtern.hlp and JaasConfig.xml. the following error is displayed: `pkgchk CSCOxrts failed. /opt/CSCOpx/htdocs/help/mappingfiles/CRMExtern.hlp permissions <0640> expected <0755> actual /opt/CSCOpx/www/classpath/com/cisco/nm/cmf/security/jaas/JaasConfig.xm permissions <0640> expected <0755> actual` The package check error can be observed from command line or collect server information. This appears only after performing a remote upgrade from CD One, 4th Edition to CiscoWorks Common Services 2.2. Workaround: None. This does not affect the functionality.

Table 4 Installation Known Problems (continued)

Bug ID	Summary	Explanation
CSCdy04158	No recovery procedure for CiscoWorks, when CD One, 5th Edition upgrade fails.	If an upgrade to CD One, 5th Edition fails, there is no procedure to recover the CiscoWorks installation. Workaround: You can do any of the following: • Remove all CiscoWorks applications manually, reinstall CD One, 4th Edition, and previously installed CiscoWorks applications. Then restore data from a CiscoWorks backup. • Remove all CiscoWorks applications manually, install CD One, 5th Edition, and the corresponding CiscoWorks application. In this case, the CiscoWorks backup done with CD One, 4th Edition cannot be restored. • Rebuild the machine, and restore from system backup.
CSCdx28510	Uninstallation of CiscoWorks Common Services 2.2 fails to remove some directories under /opt/CSCOpx.	When you uninstall CiscoWorks Common Services 2.2 the following directories under /opt/CSCOpx are not removed: bin, etc, htdocs, lib Workaround: Remove the files and directories, manually.

Table 4 Installation Known Problems (continued)

Bug ID	Summary	Explanation
CSCdx01388	CTM (Cisco Transport Manager) does not co-exist with CiscoWorks Common Services.	When CiscoWorks and CTM are installed on the same machine, CiscoWorks daemons do not come up. It displays an error: `EDSMG0001: Process Manager Control is already running` Workaround: Do not install CTM on the server in which CiscoWorks is installed.
CSCdt32795	CiscoWorks malfunctions if operating system is upgraded after installation.	CiscoWorks processes fail to start normally after Operating system upgrade. Workaround: See the "Operating System Upgrade" section on page 9.

Desktop Known Problems

Table 5 Desktop Known Problems

Bug ID	Summary	Explanation
CSCin39993	Java Plug-in 1.3.1 installation modifies directory owner permissions.	Java Plug-in tar file is copied into a temporary location (/tmp) and tar xvf plugin-131-sparc.tar is executed. The ownership permissions of the directory /tmp change, causing problems in the product functioning. Workaround: • Use a sub-folder under /tmp to un-tar. or • Use /usr/sbin/tar xvfo plugin-131-sparc.tar to un-tar the file.
CSCin31048	DiskWatcher displays `CRITICAL` messages when enough disk space is available.	DiskWatcher displays `CRITICAL` messages when enough disk space is available. Reason is unknown. Workaround: Stop and restart the DiskWatcher. If that fails, stop and restart the daemon manager.
CSCin30837	Login Panel does not appear.	Java Console displays the error: `miscalculated data length` A different version of CiscoWorks may be running on the Client, and the CiscoWorks classes are in *CLASSPATH*. There might be other conflicting classes in the client, in *CLASSPATH*. Workaround: Unset *CLASSPATH* variable and invoke the login panel again.

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCin26579	JRun proxy server hogs memory.	JRun hogs CPU when checking the status of a process from CiscoWorks Common Services desktop. The size of syslog.log is huge. Workaround: 1. Restart the JRunProxyServer. 2. Run **`pdshow`** from the command line to get the process status.
CSCin22157	The DiskWatcher popup message does not appear.	The DiskWatcher popup message does not appear when the free disk space goes below 20 percent. Workaround: None.
CSCin10591	Java Plug-in 1.3.1_xx versions are not supported.	If Java Plug-in 1.3.1 and 1.3.1_03 are installed on a client machine, and if you try to launch the CiscoWorks home page, the login panel does not appear for both Internet Explorer and Netscape Navigator. This is a compatibility issue since Java Plug-in 1.3.1_xx versions are not supported. Workaround: Uninstall all Java Plug-ins on the client and invoke CiscoWorks. This will guide you to install Java Plug-in 1.3.1.

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCin06195	Browser version should be changed according to the client.	Windows 2000 clients are shown as Windows NT 5.0. When Windows 2000 clients are used, the version is detected by Javascript standard function call navigator.appVersion. This returns Windows NT 5.0 instead of Windows 2000. Microsoft internally refers to Windows 2000 as Windows NT 5.0. Workaround: None
CSCin02932	Job succeeds but it shows failed in job details window.	When debug is enabled in the device, the job will be successful, but will show `Unsuccessful`. Workaround: Disable debug in the device and run the job.
CSCea59420	The interface link in the Management Station to Device screen is broken if the client uses the hostname to access the server.	The interface link that displays a traceroute from the CiscoWorks server to the device in the Management Station to Device screen is broken if the client uses the hostname to access the server. If the hostname of the server is used, clicking on the interface link results in a `403: forbidden` error. Workaround: Use the IP address of the server to access CiscoWorks.
CSCea00268	Login panel does not show up.	The login panel does not show up after you login and logout continuously at short intervals. This problem occurs in CD One, 5th Edition and CD One, 4th Edition. Workaround: Restart the daemon manager.

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCdz59281	Unable to enable SSL after CD One upgrade.	If you enable SSL after CD One upgrade, the following `CRITICAL` message is displayed: `SSL cannot be Enabled. Some of the Applications installed are not SSL Compliant. Uninstall those Applications and try again` This problem occurs when you upgrade from CD One, 4th Edition, and if applications that are not SSL compliant are installed. SSL cannot be enabled although all the applications are disabled after the upgrade. Workaround: Uninstall or upgrade all the disabled non-SSL Compliant applications after upgrading from CD One, 4th Edition. After this, you may enable SSL. When you upgrade applications, the upgraded application must be SSL compliant.

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCdy76938	Common Services Applets are displayed as blank, grey boxes.	When the CiscoWorks Server is running in non-SSL mode, Common Services Applets under VPN/Security Management Solution > Administration > Common Services / Configuration are displayed as blank, grey boxes. This is observed in other Tomcat based applets also (Example: Topology Groups in Campus Manager). The problem occurs only in the following browser versions: • Internet Explorer 6.0with SP1 • Internet Explorer 5.5 with SP2 and rollup patch Q323759. The output in the Java Console contains IOExceptions when these applets are invoked. Workaround: There are two workarounds. They are given as Option 1 and Option 2. Option 1 has two sections, Option 1-A and Option 1-B. **Option 1-A:** If SSL is not enabled on the CiscoWorks Server, do the following: 1. Invoke CiscoWorks Server and then select any of the Common Services Applets. If the server uses a self-signed Certificate, the dialog box displays the following message: `Certificate is issued by an untrusted site. Do you want to Proceed?`

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCdy76938	Common Services Applets are displayed as blank, grey boxes.	2. Select **View Certificate**. 3. In the Certificate dialog box, select **Install Certificate**. 4. In the Certificate Import Wizard, select the default options. Close the browser and invoke the CiscoWorks Server again. **Option 1-B** If the Common Services WebServer Certificate is not valid, has expired or has a hostname different from what is used to invoke the CiscoWorks server, modify the Common Services WebServer Certificate as follows: 1. Go to *$NMSROOT*\lib\web (in a Windows server) or *NMSROOT*/objects/web/bin (in a Solaris server). 2. Run `SSLUtil.pl` (*$NMSROOT*\bin\perl SSLUtil.pl) 3. Select **Modify Common Services Certificate**. 4. Give the correct Host Name. If the Host is not in DNS, give the IP address. 5. Restart the daemon manager and follow the steps given in Option 1-A. **Option 2:** 1. Enable SSL on the CiscoWorks Server (Server Configuration > Administration > Security Management > Enable/Disable SSL GUI). 2. Invoke Common Services Applets.

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCdx37840	SSL only: resizing the browser resets the desktop.	While resizing the Netscape Navigator browser on Solaris clients after enabling SSL, the desktop content is to set to its original state. Workaround: Do not resize the browser.
CSCdw64365	Inconsistent Tree Structure.	Inconsistent Tree Structure in the browser. The order of About The Server, Setup, Diagnostics, and Administration folders is not consistent. The inconsistent tree structure appears before and after enabling System, Network Services. This may appear when you enable or disable SSL. Workaround: None.
CSCdw61688	JOS:Character circle-c corrupted with Japanese font.	In all platforms, at the bottom of each Help window, `Copyright (c) 2003, Cisco Systems, Inc. All rights reserved.` has a corrupted character for (c) (cmf01.bmp) Workaround: Display the correct character by choosing English encoding of the browser.
CSCdw11344	Telnet succeeds when TCP fails.	The commands tcp/udp small servers work only for IOS and they are disabled by default for the IOS version 12.0M or higher. Workaround: None.

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation

CSCdw04601	Error appears during navigation.	When SSL in enabled, a message appears during navigation:
		`This page contains both secure and non secure items. Do you want to continue.`
		Whether you select **yes** or **no**, an error is displayed:
		`Page cannot be displayed`
		Workaround:
		Refresh the browser or start work from the first step.

CSCdw01537	Collect Server Info shows errors in PACKAGE INFO.	Collect Server Info shows pkgchk Errors in PACKAGE INFO section. This happens when the directory/file characteristics (such as checksum, permissions) change during runtime. Workaround: None. This does not affect the functionality.

Table 5 Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb49238	Tomcat heap size shortage.	CiscoWorks Common Services 2.2 has no setting to increase heap size of tomcat. This leads to heap size shortage. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2
CSCin50393	The CiscoWorks Common Services SSH Client does not connect to some devices.	This occurs when the SSH server version is 1.99. The log file shows the following message: `SSH: ERROR: This SSH version is not supported.` Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2

CiscoView Known Problems

Note To view the known problems for a specific device package release, refer to the readme file provided with that release.

Table 6 CiscoView Known Problems

Bug ID	Summary	Explanation
None.	Runtime error messages are displayed when viewing the CiscoView Quick Start Demo in Internet Explorer.	When viewing the CiscoView Quick Start Demo in Internet Explorer, you may encounter runtime error messages. Workaround: Disable script debugging. To do so: 1. From the Internet Explorer main menu, select Tools > Internet Options. 2. Click the Advanced tab. 3. In the Browsing section, make sure that the Disable script debugging checkbox is selected.

Table 6 CiscoView Known Problems (continued)

Bug ID	Summary	Explanation
CSCdz79848	Not prompted to install Java Plug-in after launching CiscoView.	This problem is observed on Solaris clients running Netscape Navigator 4.76 without Java Plug-in already installed. This problem occurs if you: 1. Launch CiscoWorks. 2. When prompted to install Java Plug-in after clicking certain links, such as Import Device List, click **No**. 3. Click the CiscoView link. A blank page appears and you are not prompted to install the Plug-in. Workaround: Close and relaunch CiscoWorks. The problem does not occur if you click **Yes** the first time you are prompted to install the Plug-in.
CSCdz53375	Configuration dialog box is sometimes hidden when launched.	This problem is observed on Windows 2000 clients running Netscape Navigator 4.79. To reproduce the problem: 1. Open chassis view for a device. 2. Right-click the device and select **Configure**. Configuration dialog box is launched behind chassis view and may be hidden if the chassis view window is maximized. Workaround: Minimize the chassis view window. This problem does not occur on Windows 2000 clients running Internet Explorer or Solaris clients running Netscape Navigator 4.76.

Table 6 CiscoView Known Problems (continued)

Bug ID	Summary	Explanation
CSCdx43581	Unable to import device list when IP address is used to specify source device.	This problem occurs if you: 1. Use the following URL to launch CiscoWorks: http://*localhost*:1741 2. Select Device Manager > Administration > CiscoView Server > CiscoView Device List > Import Device List. 3. Select the Campus or Essentials radio button. 4. In the Host Name field, type the IP address of the device you wish to import from. 5. Click **Import**. The following error message is displayed: `Device import software is not present on this server.` Workaround: Use either *localhost* or the appropriate host name to specify the source device when the previously mentioned URL is used to launch CiscoWorks.

Package Support Updater (PSU) Known Problems

Table 7 Package Support Updater (PSU) Known Problems

Bug ID	Summary	Explanation
CSCdt36869	Installing same device package from Cisco.com using multiple PSU sessions results in errors.	If you download and install device packages from Cisco.com using both PSU web interface and standalone PSU (psu, xpsu), errors appear. Workaround: Do not use PSU web interface and standalone PSU simultaneously to download device packages from Cisco.com.

Table 7 Package Support Updater (PSU) Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt24701	No error message is displayed after an unsuccessful attempt to uninstall NMIDB packages.	After unsuccessful attempt to uninstall NMIDB packages, no error message is displayed stating that process failed. Also, in View History window, `completed successfully` is displayed under status tab when `failed` should be displayed instead. Workaround: None.
CSCdt04070	No error message is displayed when network connection is lost during the download of device packages.	No error message is displayed if network connection is lost when you download device packages from Cisco.com. Workaround: None.

Integration Utility Known Problems

The file NMIDBOptions.properties contains Cisco.com passwords, in an encoded form, and is accessible only to root users. Root access to the host needs to be restricted if Cisco.com password security is a concern.

Table 8 Integration Utility Known Problems

Bug ID	Summary	Explanation
None.	Changing the browser used by one application changes the browser used by all applications registered through the Integration Utility.	This problem occurs if you: 1. Change the browser used by an application in the Application Registration; for example, CiscoView. 2. Click tab for another application, such as Essentials. The browser will be changed. Workaround: None.
CSCin23798	Cannot upgrade to latest NMIDB by clicking Get NMIDB in integration utility GUI.	This problem occurs if the integration utility process was terminated or the local machine was rebooted during the previous NMIDB extraction. If you click Get NMIDB in the Integration Utility GUI, this message appears erroneously: `NMIDB is up to date` Workaround: Remove VersionInfo.properties file from the following directory: *CiscoWorks installation directory*\nmim\

Table 8 Integration Utility Known Problems (continued)

Bug ID	Summary	Explanation
CSCin08716	Unable to launch CiscoWorks applications from third-party NMS after reinstallation of CD One, 5th Edition.	Third-party NMS application links do not reflect changes made to SSL settings after reinstalling CD One, 5th Edition. Workaround: Perform the integration again. This is required to update the application registration in NMS.
CSCin08472	Unable to launch CiscoWorks applications from third-party NMS after enabling or disabling SSL.	After enabling or disabling SSL in CiscoWorks server, you cannot launch CiscoWorks applications from a third-party NMS, such as HP OpenView and IBM Netview. Workaround: You must perform the integration each time you enable or disable SSL in the CiscoWorks server. This is required to update the application registration in NMS.
CSCin08471	Integration with third-party NMS should be performed after installation of CiscoWorks.	Integration with third-party NMS should be performed after installation of CiscoWorks. Workaround: If SSL will be enabled for the CiscoWorks server, it is recommended that you perform integration with a third-party NMS after the installation of CiscoWorks. This is necessary because any change in protocol requires a reintegration.

Table 8 Integration Utility Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt52492	Applications do not always launch from NMS menu if a browser is not already running.	This problem occurs if both of the following conditions occur: • The browser path that you define in the Change Integration Options GUI is a shell or binary wrapper to actual Netscape executable. and • The wrapper script does not return proper error codes. In such a case, you will not be able to start browser from NMS menu. Workaround: • Do not use Netscape wrapper scripts. Instead, configure original Netscape binaries within the Integration Utility. or • Modify wrapper scripts so that error codes are properly returned by browser back to the shell.
CSCdr38931	Error messages may be displayed when running Change Integration Options on a system with insufficient disk space.	After integration, when you run Change Integration Options, your system extracts NMIDB. If there is not enough disk space to extract NMIDB, the extraction fails. Workaround: Free up some disk space and relaunch Change Integration Options. • For Windows NT, if FAT file system is in place, make sure you have at least 190 MB of free disk space. • For other file and operating systems, make sure you have at least 25 MB of free disk space.

Table 8 Integration Utility Known Problems (continued)

Bug ID	Summary	Explanation
CSCdp90728	In UNIX platforms, when the Update Cisco Device Support task is run from the Network Node Manager, generated messages are not displayed.	In UNIX platforms, if you run the Update Cisco Device Support task from the Network Node Manager (for example, HP OpenView), generated messages are not displayed. Workaround: Go to windows from which HP Openview was started to view generated messages.
CSCdm91445	If you run the utility to change only application registration information (such as browser, server, and port number), a full integration occurs.	If you change only the application registration information, only application integration should occur. Instead, full integration occurs. Workaround: None.
CSCdm61980	Cannot launch CiscoView by double-clicking device icons in NMS after integration.	Some NMS adapters do not support double-clicking device icons from the topology map, even if CiscoView is set as default application (using Change Integration Options). Workaround: None.

Browser Known Problems

Table 9 Browser Known Problems

Bug ID	Summary	Explanation
CSCin00944	Java Plug-in 1.3.1 is not recognized properly by Solaris Netscape clients.	This problem occurs when you invoke CiscoWorks on the following Netscape and Plug-in versions: Client Platform: Solaris Netscape versions: 4.77, 4.78, 4.79 Java Plug-in: 1.3.1 Solaris Netscape (versions 4.77,4.78,4.79) In this case, CiscoWorks does not recognize the Java Plug-in already installed on the client and keeps prompting to install Plug-in again. This is due to a bug on Solaris Netscape (4.77 or later) Workaround: For Solaris Clients, use only Netscape Navigator 4.76. This problem also occurs when you invoke CiscoWorks on the following Netscape and Plug-in versions: Client Platform: Windows Netscape Versions: 4.78, 4.79 Java Plug-in: 1.3.1 This problem occurs only if the Java Plug-in option is enabled in Netscape Navigator preferences. The cookies get disabled when you invoke CiscoWorks on Netscape Navigator when Java Plug-in is enabled, and you cannot login to CiscoWorks. Workaround: Turn off (uncheck) the Java Plug-in option from Edit > Preference > Advanced.

Table 9 Browser Known Problems (continued)

Bug ID	Summary	Explanation
CSCdx04645	A blank window sometimes appears after launching online help.	This problem occurs in Solaris clients running CiscoView 5.4 in Navigator 4.76. If you click **Help** in any dialog box, a blank window appears, although status bar displays `Document: Done.` Workaround: Click **Reload** and the appropriate online help is displayed.
CSCdw92538	CPU Utilization peaks when SSL Initializes.	In SSL mode, you are redirected to http mode. After SSL initialization, you are redirected back to https mode. During this time, the CPU utilization on the Client machine might go upto 100%. But it will stabilize after sometime. The browser hangs, when the redirection occurs several times in the same browser session. Workaround: Restart the browser. You must reduce the number of redirections in the same browser session. 1. Do not refresh or reload index.html page of the same server successively. After SSL Initialization has happened once for a particular server in a browser session, successive access (refresh/reload if required) can be done directly through https://*server:port*/login.html instead of index.html. 2. Do not change the CiscoWorks Servers being accessed repeatedly in the same browser session.

Table 9 Browser Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt11838	When launching an application, you are not prompted to install the Java Plug-in.	If RealJukeBox Netscape Plug-in is installed before Java Plug-in is installed, you will not be prompted to install Java Plug-in software when attempting to launch an application. A blank screen appears. Workaround: Install Java Plug-in manually. For more information regarding the Java Plug-in, see the "Support Information" section on page 10.
CSCdt06518	Unable to launch a second instance of CiscoView in Internet Explorer while the first instance is waiting for user input.	The problem occurs if you: 1. Launch CiscoView. 2. Open a device. CiscoView will prompt for community strings. 3. Without entering community strings, launch a second instance of CiscoView. Workaround: Enter community strings before launching the second instance of CiscoView.
CSCdt05102	Netscape Navigator crashes if you resize the browser window while the applet loads.	This problem exists in Netscape Navigator. Workaround: None.
CSCds89236	If you select **No** in the Swing-based confirmation dialog boxes and press **Return**, Yes is applied.	This occurs in Solaris clients running CiscoWorks Common Services 2.2 and also in Netscape Navigator. Workaround: Instead of the **Return**, use mouse or spacebar to select **No**.

General Known Problems

Table 10 General Known Problems

Bug ID	Summary	Explanation
None.	Local machine configuration is used when performing a remote upgrade.	There are two possible sources for configuration information: • Local machine • Remote machine The configuration information for the local machine has precedence. It is this information that is used during a remote upgrade.
None.	CiscoView log file resides in a new location.	For CiscoView, the cv.log file is now located in the following directory: • Windows: *NMSROOT*\log\cv.log For example, c:\Program Files\CSCOpx\log\cv.log • Solaris: /var/adm/CSCOpx/log/cv.log

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCin41762	Help under Logging folder pointing to null:1741(2)...	• Behavior in Netscape Navigator: Using Netscape Navigator, if you access help from VPN/Security Management Solution > Administration > Logging > Completed Jobs, `Page Not Found` error appears. It points to null:1741 (2)... The same problem occurs with all the links under the Logging folder. • Behavior in Internet Explorer: Using Internet Explorer, if you access help from VPN/Security Management Solution > Administration > Logging > Completed Jobs, the help page appears. However, if you click VPN/Security Management Solution > Administration > Logging > Completed jobs > Jobs performed on *Date*, a page with Job details appears. If you click help in that page, `Page Not Found` error appears. It points to null:1741 (2)... Workaround: Access help from VPN/Security Management Solution > Administration > Configuration, or VPN/Security Management Solution > Administration > Common Services.
CSCin28069	The message in the Backup job result window is not fully visible.	With Solaris Netscape 4.76 as client browser, if you perform a backup operation, the Backup job result window appears. The message in this window is only partly visible. This is a Netscape Navigator specific problem. Workaround: Resize the message window.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCin27897	The Database Credentials GUI is not displayed properly.	In the Database Credentials screen, the Finish and Help buttons are not completely visible. The position of the Modify button is shifted to the right. This is a Netscape Navigator specific problem. Workaround: None.
CSCin27753	The AAA Server GUI does not load properly if login mode is changed.	If you change the login mode, navigate to the AAA server GUI (VPN/Security Management Solution > Administration > Common Services > AAA Server), and click **Synchronize**, the AAA Server GUI is not displayed properly. This is a Netscape Navigator specific problem. Workaround: Reload the GUI.

CSCin27092	Command fails to stop Tomcat process.	If you try to stop Tomcat process using the `pdterm` command, the following error appears:
		`# pdterm Tomcat`
		`ERROR: cmd failed. Server reason:`
		The Tomcat process is not stopped, but the dependent process (Apache) is stopped.
		Workaround:
		Run **`pdterm`** command on the Tomcat process again.

CSCin27032	The process EDS-GCF goes down.	This happens when daemons are restarted frequently. Workaround: 1. Stop the daemons. 2. Make sure all ports are free. 3. Restart the daemons.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCin21849	ESS is in shutdown state.	This problem occurs if you install CiscoWorks Common Services 2.2 in Express mode and enable System services. This does not allow you to get the interface information from the system at ESS startup. Workaround: Reboot the system.
CSCin21677	The focus is not restored on the folder selection window.	If you enter an invalid directory path in the Licensing Information/Backup Database/Restore Database GUIs and click **Return**, the following error message appears: `Invalid directory or file` If you again click **Return** to close the error message, it disappears. However, the focus is not restored on the folder selection window. Instead, the focus remains on the Select button. This problem is seen only in Netscape Navigator. Workaround: Instead of clicking **Return** to close the error message, get the focus to the File Browser to continue file browser operations.
CSCin18865	The up arrow icon is not displayed.	The up arrow icon in the File Browser does not appear when you select it. This is a Netscape Navigator specific problem. Workaround: Resize or refresh the File Browser.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCin18239	Redundant horizontal and vertical scrollbars appear in the File Browser.	Some of the directories and files are not visible. Also, redundant scrollbars appear in the File browser. Workaround: Resize or refresh the File Browser.
CSCin17971	When JRM is restarted, no Jobs are displayed in the Job Management UI.	This happens if more than one CiscoWorks Server is running on the network. Workaround: If you restart JRM, you must restart EDS and JRunProxyServer. Then invoke Job Management UI.
CSCin07838	Not able to invoke CiscoWorks if you start daemon immediately.	Unable to invoke CiscoWorks if you stop the daemon manager and restart it immediately. Workaround: Do not restart the daemon manager immediately after stopping it. You must wait for some time for the ports to be released.
CSCin07682	Default button inactive in Java-Plug-in Security warning window.	The Java Plug-in Security Warning window which is displayed just before the launch of the Cisco Works home page, has the Grant this Session button as the default button and it is highlighted. However, if you press **Return**, it does not affect this button. Workaround: Use the mouse to select this button.
CSCin03389	Adhoc template fails for some catalyst devices	When you enable debug on the device, the job will be successful, but will be shown `Unsuccessful`. Workaround: Disable debug in the device and run the job.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCea14488	Common Services does not function if host name is changed.	If you change the hostname of a machine, Common Services does not work. Workaround: 1. Change the HOST_NAME and CMF_HOST_NAME values in the following file: CSCOpx/MDC/tomcat/mdc/WEB-INF/web.xml 2. Change HostName entry in the CCR. For this do the following: – Set LD_LIBRARY_PATH on Solaris: setenv LD_LIBRARY_PATH /opt/CSCOpx/MDC/lib – Navigate to *$NMSROOT*/MDC/bin where *NMSROOT* is the location of CiscoWorks. – Remove HostName containing old host name by: **ccraccess -removeResource Core Custom Custom "" "" HostName** – Add new HostName entry with new host name by: **ccraccess -addResource Core Custom Custom** *NewHostName* **"" HostName** – Check the new HostName entry from CCR: ccraccess -addResource Core Custom Custom "" "" HostName

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCdx22615	Random pop up of security information dialog box.	The security information dialog box pops up randomly. Workaround: None.
CSCdx18854	Errors in daemons.log after stopping the ESS process.	Errors in daemons.log after stopping the ESS process. Workaround: Before stopping ESS: 1. Run **`pdterm`** JRunProxyServer. 2. Run **`pdterm`** ESS. To re-start: 1. Run **`pdexec`** ESS. 2. Run **`pdexec`** JRunProxyServer.
CSCdw61684	JOS:Apache generates error message `localeinfo_ja_jp.properties not exist`	These error messages appear when you invoke Resource Manager Essentials > Availability Dashboard > Device Center > Reachability Trend. These messages are logged only when you invoke the application from a client for the first time. Workaround: None.
CSCdt73198	CiscoWorks freezes when network connection is removed.	CiscoWorks freezes when the machine's connection to network is lost either by • Plugging out the ethernet network cable. or • Powering down the switch. Workaround: Reboot the machine.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCin41906	CiscoWorks applications that use Java Plug-in cannot be launched from NNM 6.4 web console.	HP Openview NNM6.4 requires Java Plug-in 1.4.x to be installed, when invoked from a web browser. There are known compatibility issues when invoking applications that use different Java Plug-in versions, in the same browser sessions. CiscoWorks applications use Java Plug-in 1.3.1 Since this is not the Java Plug-in version used by HP OpenView NNM 6.4, CiscoWorks applications cannot be invoked from NNM 6.4 web console. Workaround: None.
CSCdt21743	Configuration files in Trivial File Transfer Protocol (TFTP) boot directory not secure.	The configuration files, stored in the TFTP boot directory during the TFTP operation, have permission for everyone, though files are owned by the user casuser. This problem occurs only for a short time while downloading. Workaround: None.
CSCdr97090	CiscoWorks fails if Oracle, Ingres, or Informix is installed.	This problem occurs when Oracle, Ingres, or Informix database is installed on a system that has CiscoWorks installed. This happens because these tools use resources that CiscoWorks need. Workaround: Tune the kernel accordingly. Consult your operating system vendor for instructions on tuning the kernel.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCin16992	EDS displays errors if hostname is changed.	The error is displayed if you change the hostname, without restarting the daemons. Workaround: Refer the following links: http://www.cisco.com/warp/public/477/RME/sol_hostname.html (for Solaris) http://www.cisco.com/warp/public/477/RME/winnt_hostname.html (for Windows)
CSCin45238	SqlCoreDB daemon stops IDS_MC daemon during data restore operation.	IDS_Backup is the daemon that does backup and restore of IDS MC database. The daemon is dependent on SqlCoreDB (database server). During IDS MC restore, the database server is stopped. This stops the IDS_Backup daemon and aborts the restore. Workaround: None.
CSCin45735	Browser crashes when executing an immediate backup in VMS or Common Services.	If you use Netscape Navigator 4.79 browser when executing an immediate backup in VMS or Common Services, it crashes. This occurs also when you do remote browsing with Netscape 4.79 and 4.78. Workaround: None. To verify whether the backup is successful, go to Administration > Logging > Backup Jobs.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCdx74061	The scheduling fields do not automatically select the displayed value.	If you try to schedule a Backup or Compact job, the scheduling fields do not automatically select the displayed value. The affected panels are: VPN / Security Management Solution > Administration > Common Services > Compact Database and VPN / Security Management Solution > Administration > Common Services > Backup Database. The values are not selected if they are not highlighted before you click Finish. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2
CSCeb08489	Login panel shows the username of the previous user and inherits the privileges of this user.	This problem occurs because the client browser talks to the server through a NAT. When this happens, the HOST header of the HTTP request does not get translated and hence provides the wrong information. During logout, the header information is used to open a connection to the webserver. Since the host information is wrong, the connection fails, and the user is not properly logged out. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb21179	The VPN / Security Management Solution page does not list the folder names available.	The VPN / Security Management Solution page does not list the folder names available. Though the folder names are not visible, you can launch the application if you click the icon. The problem occurs in Netscape Navigator 7 with the default Java Plug-in version JPI1.4.1 Workaround: Install JPI 1.4.1_02 and point Netscape Navigator 7 to the new JPI.
CSCin53880	The Contents and Index panels in the online help appear blank.	This happens when you use Internet Explorer 6.0.26 on Windows 2000 Professional or Server with Service Pack 4 and Java Plug-in 1.4.1_02. Workaround: Use Internet Explorer 6.0 with Service Pack 1 on Windows 2000 Professional or Server with Service Pack 4.
CSCin44573	The database password changes when you try to restore after a backup operation.	If, during backup and restore of the MC database, you change the database password after backup, restore fails. You will not be able to connect to the database after restore. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb08436	The ESS process of CiscoWorks broadcasts on UDP port 42350.	Broadcast packets are seen on the local subnetwork even though CiscoWorks applications use ESS only for intra-machine messaging. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2
CSCeb15620	PixMC backup fails even after 50 tries.	With only PixMC installed, backup of KrsClient happens only after about 50 tries. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2
CSCeb44684	PIX MC pages not displayed.	PIX MC pages does not come up because unnecessary jars were set to the CLASSPATH in tomcat.sh. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb46559	MICE/CAM to communicate via HTTPS with ACS3.2.	Currently the MICE/CAM component of Common Services communicates with remote ACS server via HTTP mode. Since ACS 3.2 now runs in HTTPS mode, MICE/CAM should be enhanced to communicate via HTTPS. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2
CSCea56786	System memory gets corrupted.	String size change in License.dll corrupts system memory. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2
CSCin43722	SqlcoreDB terminates before its dependent daemons shut down.	IDS MC daemons does not cleanup the semaphores and shared memories after stopping the daemons. Workaround: The problem will be resolved if you install CiscoWorks *Bundle* Update 1, available on CCO. *Bundle* stands for LMS1.3/LMS2.2/RWAN1.3/VMS2.2

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCsd21327	CMF database fails to run and throws the following Sybase Assertion error message: `*** ERROR *** Assertion failed: 100909 (9.0.0.1383).` 100909 is the Assertion ID.	Following are the scenarios where Assertion Error might appear: 1. If you use any third-party backup software to back up a live, running database, the Assertion Error might be thrown. This is because some of the database pages that have been modified will be in the database server cache, so the database file will be in an inconsistent state. 2. If you use any anti-virus software. The reason is, Adaptive Server Anywhere performs many reads and writes other than the normal I/O operations, which contribute to the good performance of Adaptive Server Anywhere. However, anti-virus software might detect this as a potential problem and quarantine the file. This becomes hazardous if the .log or temporary files are quarantined, and it may cause corruption by interfering with the normal functions of the database. Poor performance can also occur if the anti-virus software is checking all I/O operations performed by the database server. Workaround: We recommend that you do not use third-party backup software for backing up a running database. We also recommend that you configure your anti-virus software so that it must not scan the NMSROOT/databases directory. NMSROOT is the directory where you have installed CiscoWorks.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCsd43112	Changes in Australian day light settings affect scheduled backup and/or compaction.	Operating System vendors, Microsoft and Sun Microsystems have released patches for changes in Australian daylight savings from March 27, 2006 to April 2, 2006 due to the Common Wealth Games. It has been found that the java API used to get system time returns one hour less than the actual server time during the affected period. As a result, the scheduled backup and/or compaction of database are executed with a delay of one hour. Also, the logs and/or reports show incorrect time stamp. The following time zones are affected: • Adelaide (GMT +9.30) • Hobart (GMT+ 10.00) • Sydney (GMT + 10.30) Workaround: Reschedule the backup and/or compaction of database by one hour ahead of the actual desirable time from March 27, 2006 to April 02, 2006.

Table 10 General Known Problems (continued)

Bug ID	Summary	Explanation
CSCsd40394	Australian day light settings affect the API to return time.	Operating System vendors, Microsoft and Sun Microsystems have released patches for changes in Australian daylight savings from March 27, 2006 to April 2, 2006 due to the Common Wealth Games. It has been found that the java API used to get system time returns one hour less than the actual server time during the affected period. As a result, the scheduled jobs are executed with a delay of one hour. Also, the logs and/or reports show incorrect time stamp. The following jobs are affected: • PSU Device Downloads. • Sample job through jobcli The following time zones are affected: • Adelaide (GMT +9.30) • Hobart (GMT+ 10.00) • Sydney (GMT + 10.30) Workaround: Reschedule the jobs by one hour ahead of the actual desirable time from March 27, 2006 to April 02, 2006.

Internally-Found Resolved Problems

Table 11 Internally-Found Resolved Problems

Bug ID	Summary	Additional Information
CSCin33131	Scheduled backup failed on upgrading to CiscoWorks Common Services 2.2	This problem has been resolved.

Table 11 Internally-Found Resolved Problems (continued)

Bug ID	Summary	Additional Information
CSCin29682	EDS pages displayed exception when CD One was installed on custom ports.	This problem has been resolved.
CSCin26708	Licensing Database Password cannot start with a special character.	This problem has been resolved.
CSCin09459	The command `run_isql` did not work on solaris.	This problem has been resolved.
CSCin05220	Not able to invoke CiscoWorks from the browser.	This problem has been resolved.
CSCdt50353	Unable to access help files for user-created management connections after direct upgrade of CiscoWorks.	This problem has been resolved.

Customer-Found Resolved Problems

Table 12 Customer-Found Resolved Problems

Bug ID	Summary	Additional Information
CSCea15281	Management Station to Device tool Management Station to device, allowed for remote command execution.	This problem has been resolved.
CSCdz24611	Extremely slow response from CiscoWorks Web GUI.	This problem has been resolved.
CSCdz03633	SSH implementation in CiscoWorks encrypted SSH packets that should not have been encrypted.	This problem has been resolved.
CSCdy10948	If CiscoWorks was installed in a non-default directory such as /u01/apps/CSCOpx on Solaris, the upgrade from DFM 1.1 to 1.2 took 19 hours or longer.	This problem has been resolved.

Table 12 Customer-Found Resolved Problems (continued)

Bug ID	Summary	Additional Information
CSCdx87041	While installing CD One, 5th Edition in a machine which had its CPU in slots other than zero (0), installation terminated abnormally.	This problem has been resolved.
CSCdx70474	db backup failed because on line validation failed.	This problem has been resolved.
CSCdx41552	Scheduled backup was not allowed to /opt/CSCOpx/databases/backups.	This problem has been resolved.
CSCdt18555	CD One did not have the option of configuring a remote mail gateway if sendmail was not running on UNIX platforms where CiscoWorks was installed.	This problem has been resolved.

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

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

All users can order monthly 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_inpck/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, U.S.A.) 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 e-mail your comments to 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

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

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/index.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

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

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

---

This document is to be used in conjunction with the documents listed in the "CiscoWorks Common Services Documentation" section.