



Release Notes for CiscoWorks Common Services 3.2

Revised: June 19, 2008, OL-15514-01

Contents

This document has the following sections:

- [Introduction](#)
- [Whats New in This Release](#)
- [Time Zone and Acronyms and Offset Settings](#)
- [Multi-homed Machines](#)
- [Operating System Upgrade](#)
- [Server and Client Requirements](#)
- [Integrating with Third-party Vendors](#)
- [Known Problems in CiscoWorks Common Services 3.2](#)
- [Resolved Problems in CiscoWorks Common Services 3.2](#)
- [Product Documentation](#)
- [Related Documentation](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)
- [Notices](#)



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

Introduction

CiscoWorks Common Services (Common Services) represents a common set of management services that are shared by CiscoWorks applications.

It also provides a common framework for all basic system-level operations. Some of these operations are:

- Installation
- Data management including Backup-Restore and Import-Export
- Event and message handling
- Job and process management

Common Services allows you to share critical information among the various products. It provides a new framework to support new devices. In addition, it supports new platforms, and provides enhanced security mechanisms.

Common Services 3.2 is available along with CiscoWorks LAN Management Solution (LMS) 3.1 solution and can be installed from LMS 3.1 Product DVD.

Whats New in This Release

The following are the new features and enhancements in Common Services 3.2:

- [Third Party Tools and Software Changes](#)
- [Aggregated Device Center](#)
- [New User Interface to Configure and Schedule Log File Rotation](#)
- [Multiple Device Discovery Jobs With Multiple Device Discovery Settings](#)
- [Adding Discovered Devices to a Group](#)
- [Device Type Selector for SysObjectID Filter](#)
- [Enhancements to Common Services Device Discovery](#)
- [Common Services Device Discovery Logging](#)
- [Enhancements to Audit Log Reports](#)
- [Enhancements to Server Administration](#)
- [Device Allocation Summary Portlet](#)

Third Party Tools and Software Changes

The following are the third-party tools and software changes in Common Services 3.2:

- JRE Upgrade
Common Services 3.2 ships JRE 6.0 Update 3 (JRE_6u3) along with JRE 1.5.0_13. The JRE version 1.4.2_12 has been discontinued in this release.
- Upgrade to Sybase ASA version
Earlier Common Services shipped iAnywhere version 9.0.2. In this release, Common Services ships Sybase ASA 10.0.1 on both Windows and Solaris.

See *Installing and Getting Started With CiscoWorks LAN Management Solution 3.1* for more details on third party tools and software changes.

Aggregated Device Center

Earlier, in a multi-server environment, Device Center listed the device details only when it was managed by any one of the applications in local server. Device Center did not display the device summary, tools and management task links for the devices that were managed by remote servers in the same DCR domain.

In this release, Device Center is enhanced to:

- Display a device in Device Selector although it is not managed by applications installed in local server.
- Display aggregated summary of a device that is managed in all applications installed in all servers in a DCR domain.

You must set up all the servers in SSO domain to get maximum benefit from this functionality.

New User Interface to Configure and Schedule Log File Rotation

Earlier, the log files rotation feature was available only through CLI.

In this release, Common Services provides a new user interface to configure and schedule log files rotation.

You can configure the log rotation for a specified size and compression format. You can also schedule immediate or periodic log rotation jobs.

Multiple Device Discovery Jobs With Multiple Device Discovery Settings

Earlier, you were able to configure Device Discovery jobs with only one set of Device Discovery Settings. You could not create schedules with different Device Discovery settings.

In this release, you can create multiple Device Discovery schedules with different Device Discovery settings.

Adding Discovered Devices to a Group

In the earlier releases, the devices were directly added to DCR at the end of Device Discovery. Because of this, there was difficulty in getting the list of recently discovered devices and updating the device credentials.

In this release, you can add the discovered devices to a selected group at the end of discovery. You can later select the devices in the group that you have configured and update device credentials.

Device Type Selector for SysObjectID Filter

Earlier, when configuring a sysObjectID filter, you needed to enter a value of sysObjectID manually.

In this release, a device type selector is provided which allows you to select a sysObjectID of a device easily.

Enhancements to Common Services Device Discovery

The following enhancements in Common Services Device Discovery are available in this release:

- The Jump Router Boundaries option is available for CDP module. This option extends the discovery set by routers in the network.
- Earlier, discovery information is maintained only for the module that first discovered the device although many modules were used for Device Discovery.

Now, Device Discovery maintains information about all modules.

Common Services Device Discovery Logging

In this release, Common Services provides the option to enable debugging for only selected Device Discovery modules and components. This eliminates the need to store the debug messages for all Device Discovery components in a log file.

Enhancements to Audit Log Reports

Earlier, in ACS mode, you were not able to view the Audit reports from CiscoWorks Server that were generated in non-ACS mode.

In this release, you can now view all Audit reports that are created in both the non-ACS mode and in the ACS mode from CiscoWorks Server.

Enhancements to Server Administration

The following are the changes to Server Administration tasks:

- Earlier, core dump files that were created after an abnormal process termination, were stored with the same names. This resulted in overwriting of core files.
In this release, the core dump file names are controlled. The executable filename of the program and the runtime process ID is now appended to the core file name.
- You can now enable e-mail attachments in the mails from CiscoWorks Server when scheduled jobs are complete.

Device Allocation Summary Portlet

Earlier, you were not able to get the manageability status of devices that were managed by any CiscoWorks application in any server in the DCR domain.

In this release, a Device Allocation Summary Portlet is introduced that lists the manageability status of all devices.

See *User Guide for CiscoWorks LMS Portal 1.1* for details.

Time Zone and Acronyms and Offset Settings

Common Services and associated CiscoWorks applications support many time zones. However, applications that have scheduling and reporting functions, and applications that produce or use time stamps vary based on:

- Server and client—Time stamps can differ between server and client if they are located in different time zones.
- Platforms—Windows and UNIX servers support different time zones and are not synchronized.

[Table 1](#) 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.
- 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 1](#) also provides possible outputs 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.

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 1 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	Argentina Standard Time	Argentina/ Buenos Aires	-3:00	Buenos Aires, Georgetown	GMT -3:00	ART ARST (DST)
ARST	Argentina Daylight Saving Time	Argentina/ Buenos Aires	-2:00	Buenos Aires, Georgetown	GMT -2:00	ARST (DST) ART
AST	Arabic Egypt Standard Time	Africa/ Cairo	+2:00 +3:00 (DST)	Cairo	GMT +2:00 GMT +3:00 (DST)	AST
BRT	Brazil Standard Time	Brazil/ Brasilia	-3:00	Brasilia	GMT -3:00	BRT BRST (DST)
BRST	Brazil Daylight Saving Time	Brazil/ Brasilia	-2:00	Brasilia	GMT -2:00	BRST (DST) BRT

Table 1 Supported Server Time Zones (continued)

Time Zone Acronym Set- ting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Set- ting on Server	Output in Report	
					GMT	Acronym
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
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/ Casablan- ca	None	Greenwich Mean Time	GMT +0	GMT
HST	Hawaiian Standard Time	Pacific/ Honolulu	-10:00	Hawaii	GMT -10:00	HST
IRDT	Iran Daylight Time	Iran/Tehran	+4:30	Tehran	GMT +4:30	IRDT (DST) IRST
IRST	Iran Standard Time	Iran/Tehran	+3:30	Tehran	GMT +3:30	IRST IRDT (DST)
IST	Indian Standard Time	India	+5:30	Chennai, Kolkata, Mumbai, New Delhi	GMT +5:30	IST

Table 1 Supported Server Time Zones (continued)

Time Zone Acronym Set- ting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Set- ting on Server	Output in Report	
					GMT	Acronym
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
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)
UTC	GMT Standard Time	Great Britain/ London	None	Greenwich Mean Time	GMT +0	GMT
VET/VST	Venezuela Standard Time	Venezuela/ Caracas	-4:30	Caracas	GMT -4:30	VST
WDT	Western Daylight Time	Western Australia/ Perth	+9:00	Perth	GMT +9:00	WDT (DST) WST
WST	Western Standard Time	Western Australia/ Perth	+8:00	Perth	GMT +8:00	WST WDT (DST)
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, all IP addresses must be configured in DNS.

Operating System Upgrade

While installing CiscoWorks Common Services, the installation process checks for required patches. You must install:

- Any missing required patches, recommended patches, and cluster patches on Solaris systems.
- Required service packs on Windows systems

For a list of prerequisites, see Chapter 2 of *Installing and Getting Started with CiscoWorks LAN Management Solution 3.1* at:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html.

If CiscoWorks does not operate properly after you install all necessary patches or service packs, check the permissions in the directory `install-directory\objects\dmgt\ready`. Local administrators group and casusers group 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 service packs or patches, it will not function properly.

Server and Client Requirements

For information on server and client requirements for the system and browser, see Chapter 2 of *Installing and Getting Started with CiscoWorks LAN Management Solution 3.1* at:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html.

Integrating with Third-party Vendors

Use Integration Utility to integrate Cisco device information and Cisco applications into SNMP management platforms such as HP OpenView and NetView.

For information about supported Network Management Systems in Common Services 3.2, see Chapter 1 of *Installing and Getting Started with CiscoWorks LAN Management Solution 3.1* at:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html.

Integration Utility 1.8 is available along with CiscoWorks LAN Management Solution (LMS) 3.1 solution and can be installed from LMS 3.1 Product DVD.

You might need to run 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.

See the following documents:

- *Installing and Getting Started with CiscoWorks LAN Management Solution 3.1* for information on supported NMS and NMIDB versions for Integration Utility 1.8.
- *User Guide for CiscoWorks Integration Utility 1.7* for information on installing and using Integration Utility.
- *User Guide for CiscoWorks Common Services 3.2* and the Online help for information about importing devices from NMS.

Known Problems in CiscoWorks Common Services 3.2

This section contains:

- [Device Discovery Known Problems](#)
- [CiscoWorks Server Administration Known Problems](#)
- [General Known Problems](#)
- [Integration Utility Known Problems](#)

Device Discovery Known Problems

[Table 2](#) contains the known problems in Device Discovery.

Table 2 *Device Discovery Known Problems in Common Services 3.2*

Bug	Summary	Explanation
CSCsm34330	Discovered devices are added to a group during Discovery Settings configuration although you do not have permission to group-related tasks.	<p>During the Device Discovery Settings configuration, if you selected the option to add the discovered devices to a group, you must enter a new or existing group name.</p> <p>Discovered devices are added to a group that you have entered during Discovery Settings configuration although you don't have permissions to group-related tasks.</p> <p>This problem occurs when the CiscoWorks Server is in ACS mode.</p> <p>Workaround: None.</p>

Table 2 Device Discovery Known Problems in Common Services 3.2

Bug	Summary	Explanation
CSCsg61414	Ping Sweep Discovery module does not discover all devices from the network.	<p>Ping Sweep Discovery module does not discover all devices from the network. Sometimes, Device Discovery stops during the Discovery process.</p> <p>This problem occurs when you provide networks that span many devices.</p> <p>This could occur if there is a mismatch in the destination address of the Echo request and the source address of the Echo reply.</p> <p>Workaround: None.</p>
CSCsj43330	Routing Table Discovery module does not discover all devices from the network.	<p>Routing Table Discovery module does not discover all devices in the network.</p> <p>This module discovers only the devices that are connected through the networks that are available in the ipRouteNextHop.</p> <p>Workaround: None.</p>
CSCsj56517	Routing Table Discovery module does not discover all Content Engine devices from the network.	<p>Routing Table Discovery module does not discover Content Engine devices in all Virtual Private Networks (VPN).</p> <p>Workaround: None.</p>
CSCsj93562	Device Discovery does not work properly for Address Resolution Protocol (ARP) and Routing Table (RT) when Global seed device settings are used.	<p>Device Discovery does not run if you have selected the following Discovery Settings:</p> <ul style="list-style-type: none"> Address Resolution Protocol (ARP) and Routing Table (RT) Discovery modules Global seed device option for seed device settings <p>However, Device Discovery runs properly when module-specific seed devices are configured for ARP and RT modules.</p> <p>Workaround: None.</p>

Table 2 **Device Discovery Known Problems in Common Services 3.2**

Bug	Summary	Explanation
CSCsk19197	Correct set of SNMP credentials are not updated in DCR after Device Discovery.	<p>Correct set of SNMP credentials are not updated in DCR even after a Device Discovery cycle has completed successfully.</p> <p>This happens if you:</p> <ol style="list-style-type: none"> 1. Configure incorrect SNMP credentials in DCR. 2. Configure correct set of SNMP credentials in the Device Discovery Settings screen. 3. Select the Use DCR As Seed List option for Seed Devices Settings. <p>Owing to the incorrect SNMP credentials in DCR, CiscoWorks applications cannot perform the operations on network devices.</p> <p>Workaround: None.</p>
CSCsk88625	Device Discovery process hangs when you have enabled the debugging option for Device Discovery components.	<p>Device Discovery process takes more time to run and finally hangs.</p> <p>This problem occurs when you have enabled the debugging option for Device Discovery components.</p> <p>Workaround: Disable the debugging option for Device Discovery components.</p>
CSCs113291	Some of the SNMP properties are not migrated from Campus Manager Device Discovery to Common Services Device Discovery.	<p>The following SNMP properties are not migrated from Campus Manager Device Discovery to Common Services Device Discovery.</p> <ul style="list-style-type: none"> • snmp.getBulkSize • snmp.threadadmin • snmp.threadmax <p>Workaround: Common Services Device Discovery already contains these properties and do not depend on Campus Manager for Discovery. Configure the values for these properties for better Discovery performance.</p>
CSCso62148	Found By Modules field in Discovery reports display incorrect entries for CDP and Routing Table modules.	<p>Found By Modules field in Discovery reports display incorrect entries for CDP and Routing Table modules.</p> <p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Select CDP and Routing Table modules as Device Discovery modules. 2. Specify a same seed device and the correct SNMP credentials for both the modules. <p>After Device Discovery is completed, the Found By Modules field in Discovery reports display only CDP.</p> <p>It does not display both CDP and Routing Table modules.</p> <p>Workaround: None.</p>

Table 2 Device Discovery Known Problems in Common Services 3.2

Bug	Summary	Explanation
CSCsq37833	<p>Post filtering of devices does not work properly for IP Address-based Include or Exclude filters.</p> <p>This problem occurs particularly when the SNMP credentials are incorrect.</p>	<p>Post filtering of devices does not work for certain filters.</p> <p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Configure IP Address based Include or Exclude filters with wild cards. For example, enter the filter pattern 10.77.209.* for IP Address filters. 2. Enable post filtering of devices. <p>The post filtering of devices discovers the devices that are out of filter range, from the network.</p> <p>This is because of the incorrect SNMP credentials.</p> <p>Workaround:</p> <p>None.</p>
CSCsq52970	<p>The <code>userdns</code> attribute is not migrated from LMS 2.6 or LMS 3.1 to Common Services.</p>	<p>When you perform a data migration from LMS 2.6 or LMS 3.1 to Common Services 3.2, the <code>userdns</code> attribute is not migrated from Campus Manager.</p> <p>This caused problems during Device Discovery.</p> <p>Workaround:</p> <p>Use the <code>HostNameResolveType</code> attribute in Discovery Engine tag.</p>
CSCsk15483	<p>Any error that occurs while configuring seed devices are not displayed in the user interface.</p>	<p>Any error that occurs while configuring seed devices are not displayed in the user interface.</p> <p>This problem occurs when you selected the Seed Devices From a File option.</p> <p>Workaround:</p> <p>None.</p>

CiscoWorks Server Administration Known Problems

Table 3 describes the known problems in CiscoWorks Server administration.

Table 3 CiscoWorks Server Administration Known Problems in Common Services 3.2

Bug	Summary	Explanation
CSCsq16705	The stdout.log file size grows rapidly on a LMS 5000 server.	<p>The stdout.log file size grows rapidly on a LMS 5000 server.</p> <p>The log file grows at the rate of 1 GB per minute.</p> <p>Workaround:</p> <p>None.</p>
CSCsk17402	An error occurs on LMS server because the certificate has expired.	<p>The <code>CertificateExpiredException</code> error occurs on LMS servers when you click the Peer Server Certificate Setup page.</p> <p>This is because a third-party certificate has expired.</p> <p>Workaround:</p> <p>You must either:</p> <ul style="list-style-type: none"> • Use another root certificate <p>Or</p> <ul style="list-style-type: none"> • Get a newer version of expired certificate <p>Import the certificate to CiscoWorks Server using the SSL Utility Script.</p> <p>See the Uploading Third Party Security Certificates to CiscoWorks Server section in <i>User Guide for CiscoWorks Common Services 3.2</i>.</p>
CSCsk44387 (Solaris Only)	Login to <code>dcrc1i</code> fails when the username contains special characters.	<p>When you try to login into <code>dcrc1i</code> using the login username with special characters, the login fails.</p> <p>This problem occurs because some of the Solaris shells may already use those special characters for shell commands and do not accept the special characters in the <code>dcrc1i</code> username.</p> <p>Workaround:</p> <p>Either:</p> <ul style="list-style-type: none"> • Set your <code>dcrc1i</code> login username without special characters. <p>Or</p> <ul style="list-style-type: none"> • Choose the appropriate shells to run the <code>dcrc1i</code> commands.

Table 3 CiscoWorks Server Administration Known Problems in Common Services 3.2

Bug	Summary	Explanation
CSCsq02667	Common Services application portlets are displayed twice in Functional View of CiscoWorks LMS Portal after a remote data migration from LMS 2.6 to LMS 3.1.	<p>Common Services application portlets are displayed twice in Functional View of CiscoWorks LMS Portal.</p> <p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Back up the LMS 2.6 data from a server <i>X</i> that contain the applications registered from server <i>Y</i>. 2. Upgrade the server <i>Y</i> to LMS 3.1. 3. Restore the backed up data of server <i>X</i> on server <i>Y</i>. The applications in the backup are registered. <p>This is because the application templates are registered twice in Cisco Management Integration Center component.</p> <p>Workaround: None.</p>

General Known Problems

Table 4 describes the miscellaneous known problems associated with Common Services (not specific to any module in Common Services).

Table 4 General Known Problems in Common Services 3.2

Bug	Summary	Explanation
CSCsg97728	Jobs scheduled on March 11 between 12 AM to 1:30 AM are moved to Missed Start state or rescheduled for the next run.	<p>All jobs that are scheduled on March 11 between 12 AM to 1:30 AM are not running.</p> <p>They are either moved to the Missed Start state or rescheduled for the next run.</p> <p>This happens when the DST patch is installed on March 11 between 1 PM to 3 PM.</p> <p>Workaround: Install the DST Patch available on Cisco.com well before the DST observance.</p>
CSCsj82286	Devices added in DCR are not displayed in Device Selector although they are added in ACS.	<p>In ACS mode, devices added in DCR are not displayed in Device Selector although they are added in ACS.</p> <p>This is because you added the devices after restarting ACS services in ACS.</p> <p>This problem occurs only on ACS 4.0 servers.</p> <p>Workaround: Either:</p> <ul style="list-style-type: none"> • Restart the Daemon Manager in CiscoWorks Server. <p>Or</p> <ul style="list-style-type: none"> • Upgrade the ACS 4.0 software to later versions.

Table 4 **General Known Problems in Common Services 3.2**

Bug	Summary	Explanation
CSCsk35018	Database engines supports broadcast clients and open UDP ports to listen for client broadcasts.	<p>CiscoWorks databases open UDP ports to listen for client broadcasts.</p> <p>This may result in a server response with information about the database port and engine name. However, the confidential information cannot be broadcast although the ports are open.</p> <p>This occurs with the default database configuration for all CiscoWorks databases.</p> <p>Workaround: Use access-lists or firewalls to restrict client access to the CiscoWorks Server.</p>
CSCso06399	Event Services Software (ESS) does not receive events from messaging system.	<p>Event Services Software (ESS) does not receive events from Java Light Weight Messaging System (JLWMS).</p> <p>Workaround: None.</p>
CSCso40152	Device reports launched from the Device Allocation Summary portlet expands when you click the buttons in the reports page.	<p>The Device managed by <i>Application</i> Reports launched from the Device Allocation Summary portlet, expands when you click the Go, First, Previous, Next, or Last buttons in the Reports page.</p> <p>This problem occurs only on Firefox browser.</p> <p>Workaround: None.</p>
CSCso40294	Command Services fails while connecting to IOS-XR device using SSHv1 credentials.	<p>Command Services fails while connecting to IOS-XR device using SSHv1 credentials.</p> <p>This happens although you have generated RSA keys for SSHv1 connection.</p> <p>Workaround: None.</p>

Table 4 General Known Problems in Common Services 3.2

Bug	Summary	Explanation
CSCso95015	<p>DomainInfo.properties file is created after restoring the data from:</p> <ul style="list-style-type: none"> • A DCR Master server to another Master/Slave/Standalone server • A DCR Slave server to another DCR Master server 	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Back up the data from a DCR Master server <i>M1</i> whose Slave is <i>S1</i>, for example. 2. Restore the data on any one of the following servers: <ul style="list-style-type: none"> – Another DCR Master server <i>M2</i> – Slave server <i>S2</i> of Master server <i>M2</i> – Standalone server 3. Restart the Daemon Manager. <p>The domain information remains and are not removed from the:</p> <ul style="list-style-type: none"> • Peer servers of <i>M1</i> • Slave server <i>S2</i> if you have restored the data on <i>M2</i> or Master Server <i>M2</i> if you have restored the data on <i>S2</i>. <p>This problem also occurs (domain information remains) when you:</p> <ol style="list-style-type: none"> 1. Back up the data from a DCR Slave server <i>S1</i> whose Master is <i>M1</i>, for example. 2. Restore the data on another DCR Master server <i>M2</i>. 3. Restart the Daemon Manager. <p>The domain information remains and are not removed from the peer server of <i>S1</i> (<i>M1</i>) and peer server of <i>M2</i> (<i>S2</i>).</p> <p>Workaround:</p> <p>Workaround 1</p> <ol style="list-style-type: none"> 1. Delete the DomainInfo.properties files from the server (<i>M2</i>, <i>S2</i> or Standalone) where you have restored the data. 2. If you have restored the data on <i>M2</i>, delete the DomainInfo.properties files from the peer servers (<i>S2</i>) of <i>M2</i>. 3. If you have restored the data on <i>S2</i>, remove the domain information entries of <i>S2</i> from the DomainInfo.properties file of <i>M2</i>. 4. Remove the domain information of the server where you have restored the data, from the DomainInfo.properties file of <i>S1</i>. <p>You must follow this workaround when you back up the data from a DCR Master server and restore the data on another Master/Slave/Standalone server.</p>

Table 4 **General Known Problems in Common Services 3.2**

Bug	Summary	Explanation
CSCso95015 (continued)		Workaround 2 <ol style="list-style-type: none"> 1. Delete the DomainInfo.properties files from the server (<i>M2</i>) where you have restored the data. 2. Delete the DomainInfo.properties files from the peer servers (<i>S2</i>) of <i>M2</i>. 3. Remove the domain information entries of <i>M2</i> from the DomainInfo.properties file of <i>M1</i>. You must follow this workaround when you back up the data from a DCR Slave server and restore the data on another Master server.
CSCsq35816	Duplicate headers found in the exported PDF reports.	Sometimes duplicate headers are found in the exported reports of PDF format. Workaround: None.
CSCsq54877	The resolver.pl tool may not properly resolve IP Address to hostname.	The resolver.pl tool may not properly resolve IP Address to hostname. This problem occur although the proper resolution path exists. Workaround: Use the nslookup or host command from the Operating System to get proper lookup results.
CSCsh36085	Tomcat logs are not rotated properly.	The following Tomcat logs are not rotated properly. <ul style="list-style-type: none"> • stdout.log • stderr.log Some of the contents of log files are missing after the daemons are restarted. Workaround: None.
CSCsk46142	The Job Details popup window for DCR jobs displays wrong start time.	In Common Services Job Browser page, when you select a DCR job to view the details, the Job Details popup window does not display the correct start time. This problem occurs when you schedule DCR jobs before installing the DST patch. Workaround: None.
CSCsk55579	Problem occurs in daily job schedules before and after the DST patch installation.	All daily jobs that are scheduled after applying the DST patch are advanced by an hour. The jobs that are scheduled before applying the patch are postponed by an hour. Workaround: None.

Table 4 *General Known Problems in Common Services 3.2*

Bug	Summary	Explanation
CSCsk57503	Daily jobs scheduled in the DST timings as the second instance, run as the first instance.	Daily jobs that are scheduled in the DST timings to run as the second instance do not run. Instead they run in the first instance. Workaround: None
CSCsq31632 (Windows Only)	Close buttons and text fields do not work properly in the CiscoWorks installation window.	The following problems occur in the CiscoWorks installation window: <ul style="list-style-type: none"> • Close buttons do not work properly. • Text fields in the license windows displays the cached text value These problems occur in the CiscoWorks installation window because of base defects in InstallShield 2008. 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 5](#) describes the known problems related to Integration Utility.

Table 5 *Integration Utility Known Problems in Common Services 3.2*

Bug	Summary	Explanation
CSCsa51353	Network Management Information Center (NMIC) does not exit during integration.	Network Management Information Center (NMIC) does not exit during integration although the Network Management System (NMS) is not installed on the system. This happens when the Hitachi NMS Adapter is selected for integration. Workaround: None.

Table 5 *Integration Utility Known Problems in Common Services 3.2*

Bug	Summary	Explanation
CSCsc38944	Problem occurs while integrating HPOV 7.5 with CiscoWorks applications.	<p>Integration Utility does not work for HP Open View Network Node Manager 7.5.</p> <p>When you right click on a Cisco device, the CiscoView/RME/Traceroute option is not available.</p> <p>This problem occurs only when you integrate HP Open View Network Node Manager 7.5 using the 2.1 Adapter and 1.0.086 nmiddb.</p> <p>This does not occur with HP Open View Network Node Manager 7.1 or earlier version of NMS.</p> <p>Workaround:</p> <p>Use the Cisco Applications menu to select the CiscoView menu item.</p>
CSCin28182	The Integration Utility Adapter window does not display the description of the adapters properly.	<p>The Integration Utility Adapter window does not display the description of the adapters properly.</p> <p>This problem occurs only for NetView Adapters.</p> <p>Workaround:</p> <p>None.</p>
CSCin80600	Temporary files created while integrating CiscoWorks with NMS are not removed after integration	<p>The temporary files that were created during the integration of CiscoWorks with NMS are not removed completely after the integration is completed.</p> <p>Workaround:</p> <p>None.</p>
CSCsl00295	Network Management Information Center application version displayed in HP Open View is incorrect.	<p>Network Management Information Center application version displayed in HP Open View is incorrect.</p> <p>Workaround:</p> <p>None.</p>
CSCsl60984	Some MIBs are not completely loaded while integrating CiscoWorks with NetView.	<p>Some MIBs are not completely loaded while integrating CiscoWorks with NetView and an error occurs.</p> <p>Workaround:</p> <p>None.</p>
CSCdr24473	Cannot invoke Pathtool application from NMS for Integration Utility.	<p>You cannot invoke Pathtool application from NMS for Integration Utility.</p> <p>Workaround:</p> <p>None.</p>
CSCdr41597	There is no support for device-specific application integration with NMS.	<p>You cannot perform device-specific application integration and then invoke additional applications for certain devices only.</p> <p>Workaround:</p> <p>None.</p>

Table 5 *Integration Utility Known Problems in Common Services 3.2*

Bug	Summary	Explanation
CSCsa57080 (Solaris Only)	Temporary files are not removed even after the uninstallation of Integration Utility.	Temporary files are not removed even after the uninstallation of Integration Utility. Workaround: None.
CSCsb84839	There is no option to configure proxy server settings in Integration Utility.	Integration Utility does not provide an option to configure proxy server settings. Owing to this, you cannot connect to Cisco.com through a proxy server and download the adapters and data bundles. Workaround: None.

Resolved Problems in CiscoWorks Common Services 3.2

This section contains:

- [Customer Found Resolved Problems in Common Services 3.2](#)
- [Internally Found Resolved Problems in Common Services 3.2](#)

Customer Found Resolved Problems in Common Services 3.2

[Table 6](#) describes the customer-found resolved problems in Common Services 3.2.

Table 6 *Customer Found Resolved Problems in Common Services 3.2*

Bug ID	Description	Additional Information
CSCsl00042	SNMPWalk did not work with SNMPv2 credentials when LMS is upgraded to LMS 3.0 December 2007 Update or LMS 3.1 This was the because the dependent files were missing.	This problem has been resolved. The dependent files are now added to the CiscoWorks installer and SNMPWalk works well SNMPv2 credentials.
CSCsg62980 (Windows Only)	Backup and Restore operations were unsuccessful when Cygnus mount points existed on the CiscoWorks machine. This problem occurred when the following software that shipped cygwin DLLs for Windows, were installed on the CiscoWorks Server: <ul style="list-style-type: none"> • Third-party OpenSSH for Windows • Cygwin software • IBM Tivoli Backup Manager 	This problem has been resolved. Now new library files are shipped with the product and the Backup and Restore operations works properly.
CSCsj94584	You could not install any additional CiscoWorks application after installing CiscoWorks and an application patch.	This problem has been resolved.

Table 6 Customer Found Resolved Problems in Common Services 3.2

Bug ID	Description	Additional Information
CSCs198252	When you installed new Software Center package updates or ran a backup, all transient processes were started. This resulted in an unexpected behavior in the functionality of CiscoWorks.	This problem has been resolved. In this release, only the non-transient processes are restarted when you install new package updates or run a backup.
CSCsm13114	Cisco Discovery Protocol (CDP) module in Common Services Device Discovery discovered IP Phones that were not SNMP accessible. This resulted in a longer Device Discovery cycle.	This problem has been resolved. Now the CDP module in Common Services Device Discovery ignores the discovery of IP Phones from the network.
CSCsm29546 (Windows Only)	Dbmonitor processes in CiscoWorks were not initialized and remained in the Waiting to Initialize state for a long time. This problem occurred because there were many versions of libeay32.dll and ssleay32.dll installed on the system.	This problem has been resolved.
CSCsm52191	SNMP stack in Common Services went into a deadlock state when there were too many errors.	This problem has been resolved.
CSCsm60582	Tomcat crashed when CiscoWorks Server was integrated with ACS in HTTPS mode.	This problem has been resolved.
CSCsm66330	Common Services Device Discovery sometimes added duplicate devices in DCR instead of updating the existing devices in DCR. This happened when devices were added to DCR using hostname and IP Address in different Discovery cycles.	This problem has been resolved.
CSCsm66348	Common Services Device Discovery created serialized files with clear text credentials data when a Discovery job was started and completed. These files were accessible to all groups except the casuser group.	This problem has been resolved.
CSCsm77245	There was an inconsistent behavior in CiscoWorks URL. When the CiscoWorks URL was launched, alerts and IFrames were displayed.	This problem has been resolved. Alerts and IFrames are not displayed now when the CiscoWorks URL is launched.
CSCsm86513	Common Services did not allow you to enable the debugging option for all Device Discovery modules from the user interface. The debugging option for some of the backend modules was enabled only by editing the ngd-log4j.properties file.	This problem has been resolved. Common Services provides a new user interface to enable the debugging option for log files of all Device Discovery modules. Go to Common Services > Device and Credentials > Device Discovery > Discovery Logging Configuration to open the Discovery Logging Configuration page.

Table 6 Customer Found Resolved Problems in Common Services 3.2

Bug ID	Description	Additional Information
CSCso45657	Discovery might not resolve IP Addresses to hostname properly. This was because the IP Address to hostname lookups do not match exactly.	This problem has been resolved.
CSCso81920	Dbmonitor processes in CiscoWorks crashed and the CiscoWorks applications were inaccessible. This happened when you started Device Discovery from CiscoWorks Assistant Server Setup workflow.	This problem has been resolved.
CSCsd75232	After integrating CiscoWorks LMS with HP Open View, the Cisco related traps were not found in the Event Configuration window. The Cisco alarm category was also not listed in the OV Alarm Browser.	This problem has been resolved.
CSCsk86609	Software Center jobs that were backed up from earlier versions of Common Services did not run after you restored them. This problem occurred when data was backed up from earlier versions of CiscoWorks that were installed in a non-default (other than <i>NMSROOT</i>) location. This was because the Software Center jobs were registered with an absolute path in the earlier versions.	This problem has been resolved.
CSCsk95494 (Solaris Only)	Database backup in Common Services failed on Solaris systems. This problem occurred when the length of the data file names to be backed up, contained more than 100 characters.	This problem has been resolved.
CSCsl16484 (Windows Only)	The syslog.log file did not display the source IP Address of Cisco Wide Area Application Services (WAAS) devices. This problem occurred when you configured the WAAS devices to send Syslog messages to CiscoWorks Server.	This problem has been resolved.
CSCsl30471	Migration of data failed in some cases. This was because the directories were not created while restoring the data.	This problem has been resolved.
CSCsl53840 (Windows Only)	Common Services allowed CiscoWorks applications to be installed on system with an unsupported regional setting. This affected the functionality of CiscoWorks applications.	This problem has been resolved. Common Services installer now provides you a warning message when you try to install CiscoWorks on systems with an unsupported locale.
CSCsl97730	The Packet Capture terminated abruptly when multiple TCP or UDP ports were used.	This problem has been resolved.

Table 6 Customer Found Resolved Problems in Common Services 3.2

Bug ID	Description	Additional Information
CSCsm10925 (Windows Only)	SMTP server settings configured on CiscoWorks Server did not apply. This problem occurred on CiscoWorks running a Microsoft Exchange SMTP server.	This problem has been resolved.
CSCsm33347 (Solaris Only)	A few directories in CiscoWorks Server had Write permissions to groups and all users.	This problem has been resolved. Write permissions are now revoked for groups and all users.
CSCsm71952	In a DCR Master-Slave setup, the Slave server displayed the device count as zero for the Devices not configured in ACS report. This problem occurred although few such devices were present on the Master server. This was because the Master server did not send the Devices not configured in ACS list.	This problem has been resolved.
CSCso06213	When you configure a Master-Slave setup, an error occurred. This error also occurred when you accessed any of the user interface pages that appeared when you selected Common Services > Device and Credentials.	This problem has been resolved.
CSCso19518	CiscoWorks Server communication with ACS failed when ACS returned port 2002 as the dynamic port. This caused some jobs in CiscoWorks applications to fail.	This problem has been resolved.
CSCso54631	An OutOfMemory Exception occurred while running CiscoWorks Server integrated with ACS. This problem occurred when CiscoWorks Server was in HTTPS mode.	This problem has been resolved.
CSCso85728	Information (Info) files were not created after you have installed patches and there was no indication that the patches had been installed. This problem occurred when there was an error in restarting Daemon Manager during the patch installation.	This problem has been resolved.
CSCsa34896	Common Services did not provide a user interface for Logrot tasks.	This problem has been resolved.
CSCsk31402	Audit log file names used an incorrect date format.	This problem has been resolved.
CSCsm43797	DST change in Brazil, Venezuela, Iran, Argentina, and Australia timezones caused problems on CiscoWorks Server and scheduled jobs did not run properly.	This problem has been resolved.
CSCsm82355	An SnmpAgentLoop exception occurred after a SNMPWalk operation on a device did not report the SysObjectID that caused this exception.	This problem has been resolved. Now the SysObjectID that causes the exception is printed on the configured log files.

Table 6 Customer Found Resolved Problems in Common Services 3.2

Bug ID	Description	Additional Information
CSCso16459	The restorebackup.log file in Common Services did not contain the user ID who initiated the Restore process.	This problem has been resolved.
CSCsl58580	DST change in Brazil, Venezuela, Iran, Argentina, and Australia timezones caused problems on CiscoWorks Server and certain features did not work properly. All scheduled jobs ran delayed or advanced by an hour. The timestamp in the log files displayed the time as advanced or postponed by an hour.	This problem has been resolved.

Internally Found Resolved Problems in Common Services 3.2

Table 7 describes the internally found resolved problems in Common Services 3.2.

Table 7 Internally Found Resolved Problems in Common Services 3.2

Bug ID	Description	Additional Information
CSCsa82899 (Solaris Only)	Tomcat crashed because an exception occurred in Core Client Registry.	This problem has been resolved.
CSCsj14266	Backup jobs ran for long hours on LMS 3000 and LMS 5000 servers and did not complete. A core file was also created by Sybase database engine.	This problem has been resolved.
CSCsk42056	During the upgrade installation, roles were not registered for some CiscoWorks applications although the re-registration option was selected. This problem occurred when you upgrade the CiscoWorks Server that was in ACS mode already. This was because the acsmap.txt file had partial entries for few applications only.	This problem has been resolved.
CSCsl31659	Tomcat and other processes did not run on a LMS 5000 server, because of an OutOfMemory exception. This problem occurred on CiscoWorks Server when integrated with ACS.	This problem has been resolved.
CSCsq34071	Include filters were not working properly during Device Discovery. This problem occurred particularly for IP Address based Include filters.	This problem has been resolved.

Table 7 Internally Found Resolved Problems in Common Services 3.2

Bug ID	Description	Additional Information
CSCsj04917	<p>After the port number change in DCR Slave Server, the DCR configuration file was not updated.</p> <p>This problem persisted although you regenerated the certificate.</p> <p>Owing to this, Servers and Applications Portlet, and CiscoWorks Assistant did not work properly in a multi-server setup.</p>	<p>This problem has been resolved.</p> <p>The DCR configuration file is now updated on Tomcat startup.</p>
CSCsk44028	<p>In a Single Sign-On (SSO) multi-server setup, when you launched a SSO Slave Server, it displayed a HTTP Status error.</p> <p>This problem occurred when you entered a Fully Qualified Domain Name (FQDN) of the SSO Master during the SSO Slave Server configuration.</p>	This problem has been resolved.
CSCsk86433	<p>Scheduled periodic jobs did not run after restarting Daemon Manager.</p> <p>If you restarted the Daemon Manager, when a scheduled periodic job was running, the next instance of the scheduled job did not run.</p>	This problem has been resolved.
CSCsk84471	<p>Exporting a report to a file of PDF format generated a PDF document with white spaces and blank pages.</p> <p>This problem occurred with all types of reports such as Tabular Reports, Stacked Table, and Stack of Stacked Table reports.</p>	This problem has been resolved.
CSCsq09813 (Windows Only)	After an HTTP port number change, when you upgraded CiscoWorks using the custom installation, the HTTP port number was updated with the default value 1741.	This problem has been resolved.
CSCsq17289	<p>Device Discovery Include filters queried the devices that were not in the range of Include filter, and included them.</p> <p>Owing to this, Discovery took a longer time to run.</p>	This problem has been resolved.
CSCsl28279	There was no provision to restrict crossing Router boundaries during Common Services Device Discovery.	This problem has been resolved.

Product Documentation

Table 8 describes the product documentation that is available.

Table 8 *Product Documentation*

Document Title	Available Formats
<i>User Guide for CiscoWorks Common Services 3.2</i>	<ul style="list-style-type: none"> On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html PDF on the LMS 3.1 Product DVD and Documentation CD.
<i>Release Notes for CiscoWorks Common Services 3.2 (this document)</i>	<ul style="list-style-type: none"> On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html PDF on the LMS 3.1 Product DVD and Documentation CD.
Context-sensitive Online help	<ul style="list-style-type: none"> Select an option from the navigation tree, then click Help. Click the Help button in the dialog box.



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.

Related Documentation

Table 9 describes the additional documentation that is available.

Table 9 *Related Documentation*

Document Title	Available Formats
<i>Installing and Getting Started With CiscoWorks LAN Management Solution 3.1</i>	<ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html PDF on the LMS 3.1 Product DVD and Documentation CD.
<i>Data Migration Guide for CiscoWorks LAN Management Solution 3.1</i>	<ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html PDF on the LMS 3.1 Product DVD and Documentation CD.



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.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLey License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.
 The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Release Notes for CiscoWorks Common Services 3.2

Copyright © 2008 Cisco Systems, Inc.

All rights reserved.

