



# Readme for CiscoWorks Common Services 3.0.6 on Solaris

---

This Readme is for CiscoWorks Common Services 3.0.6 on Solaris. This document contains the following sections:

- [Description](#)
- [Hardware and Software Requirements](#)
- [Downloading Common Services 3.0.6](#)
- [Installing Common Services 3.0.6](#)
- [Uninstalling Common Services 3.0.6](#)
- [Known Problems in Common Services 3.0.6](#)
- [Resolved Problems in Common Services 3.0.6](#)
- [Support for MDF 1.22](#)
- [General Guidelines for Using Common Services 3.0.6](#)
- [Related Documentation](#)
- [Open Source License Acknowledgements](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

## Description

CiscoWorks Common Services 3.0.6 is a service pack release and contains solutions to the known problems of Common Services 3.0.5.

Common Services 3.0.5 should be installed before installing Common Services 3.0.6. Common Services 3.0.5 is a separate installable on top of Common Services 3.0.3 and is bundled within the LMS 2.6 mega patch.

The solutions to some known problems of Common Services 3.0.5 (that are part of Common Services 3.0.6), may not be available in Common Services 3.1 version. You must upgrade to Common Services 3.1.1 to obtain the solution for these problems.

See [Table 2](#) and [Table 4](#) for the resolved problems in Common Services 3.0.6 (fixes to known problems of Common Services 3.0.5) that are available only in Common Services 3.1.1.

If you are a customer of LMS, we recommend you to upgrade the following CiscoWorks LMS applications after installing Common Services 3.0.6:

- Upgrade to Campus Manager 4.0.10  
You can download Campus Manager 4.0.10 from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus>.  
See [Readme for CiscoWorks Campus Manager 4.0.10 on Solaris](#) for download and installation instructions.
- Upgrade to Device Fault Manager 2.0.10  
You can download Device Fault Manager 2.0.10 from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.  
See [Readme for CiscoWorks Device Fault Manager 2.0.10 on Solaris](#) for download and installation instructions.
- Upgrade to Resource Manager Essentials 4.0.6  
You can download Resource Manager Essentials 4.0.6 from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>.  
See [Readme for CiscoWorks Resource Manager Essentials 4.0.6 on Solaris](#) for download and installation instructions.

## Hardware and Software Requirements

Before installing Common Services 3.0.6, CiscoWorks Common Services 3.0.5 must be installed on your system.

The hardware and software requirements remain the same as the requirements for Common Services 3.0.5.

To check the hardware and software requirements, see the Prerequisites chapter of *Installation and Setup Guide for CiscoWorks Common Services 3.0.5 on Solaris*. This guide is available at:

[http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products\\_installation\\_guide\\_chapter09186a00806ab77b.html](http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_chapter09186a00806ab77b.html)

# Downloading Common Services 3.0.6

You can download Common Services 3.0.6 either from Cisco.com or as a Software Update from **Common Services > Software Center > Software Update**.

- [Downloading From Cisco.com](#)
- [Downloading From Software Center](#)

## Downloading From Cisco.com

Common Services 3.0.6 is available on Cisco.com. To download Common Services 3.0.6:

- 
- Step 1** Click <http://www.cisco.com/cgi-bin/tablebuild.pl/cd-one-3des>.
  - Step 2** Enter your Cisco.com username and password.
  - Step 3** Locate the file cwcs3\_0\_6\_sol\_k9.zip.
  - Step 4** Download the file into a temporary directory on your system.
- 

## Downloading From Software Center

You can use the Software Update function in Common Services Software Center to download Common Services 3.0.6.

To download Common Services 3.0.6 from Software Center:

- 
- Step 1** Go to the CiscoWorks home page and select **Common Services > Software Center > Software Updates**.  
The Software Updates page appears.
  - Step 2** In the Products Installed table, select the check box corresponding to CiscoWorks Common Services.
  - Step 3** Click either:
    - **Download Updates**. See [Using the Download Updates Option](#).
    - Or
    - **Select Updates**. See [Using the Select Updates Option](#).
-

## Using the Download Updates Option

To download Common Services 3.0.6 using the Download Updates option:

- 
- Step 1** Click **Download Updates** on the Software Updates page.  
The Cisco.com and Proxy Server Credentials dialog box appears.
- Step 2** Enter your Cisco.com username and password. Both are mandatory.  
If you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**, enter the Proxy server username and password.
- Step 3** Click **Next**.  
The Destination Location page appears. The destination location should not be the location where CiscoWorks is installed. The default download directory is /opt/psu\_download.  
Software Center does not support downloading software or device updates into the same directory where you have installed CiscoWorks Common Services, or any of its sub- directories. Also, you cannot download software or device updates under System directories.
- Step 4** Enter the location, or browse to the location using the Browse tab.  
The destination location must have casuser write-permissions.
- Step 5** Click **Next**.  
The Summary page appears with a summary of your inputs.
- Step 6** Click **Finish** to confirm the download operation.
- 

## Using the Select Updates Option

To download Common Services 3.0.6 using the Select Updates option:

- 
- Step 1** Click **Select Updates** in the Software Updates page.  
The Cisco.com and Proxy Server Credentials dialog box appears.
- Step 2** Enter your Cisco.com username and password. Both are mandatory.  
If you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**, enter the Proxy server username and password.  
The Available Images page appears.
- Step 3** Select the cwcs3\_0\_6\_sol\_k9.zip file.
- Step 4** Click **Next**.  
The Destination Location page appears. The destination location should not be the location where CiscoWorks is installed. The default download directory is /opt/psu\_download.  
Software Center does not support downloading software or device updates into the same directory where you have installed CiscoWorks Common Services, or any of its sub- directories. Also, you cannot download software or device updates under System directories.

- Step 5** Enter the location, or browse to the location using the Browse tab.  
The destination location must have casuser write-permissions.
- Step 6** Click **Next**.  
The Summary page appears with a summary of your inputs.
- Step 7** Click **Finish** to confirm the download operation.
- 

## Installing Common Services 3.0.6

This section provides information on installing Common Services 3.0.6 on a Solaris platform. See [Downloading Common Services 3.0.6](#) for information on downloading Common Services 3.0.6.

Before you install Common Services 3.0.6, ensure that Common Services 3.0.5 is installed on the CiscoWorks Server.

To install Common Services 3.0.6:

---

- Step 1** Navigate to the location on your system, where you have downloaded the cwcs3\_0\_6\_sol\_k9.zip file.

- Step 2** Unzip the cwcs3\_0\_6\_sol\_k9.zip file by entering:

```
unzip cwcs3_0_6_sol_k9.zip
```

The contents of the zip file are extracted to the cwcs3\_0\_6\_sol\_k9 folder and stored in the system location where you have downloaded the zip file.

- Step 3** Change the directory to cwcs3\_0\_6\_sol\_k9 by entering:

```
cd Downloaded directory/cwcs3_0_6_sol_k9
```

- Step 4** Run the installation program by entering either:

```
./setup.sh
```

A message appears:

```
Welcome to Common Services 3.0.6 setup program.
```

- Step 5** Press **Enter** to read the license agreement.

The following message appears at the end of the license agreement:

```
You must accept this License agreement for the installation to
proceed.
If you enter N/n, the installation will exit.
Do you accept all the terms of the preceding License Agreement ?
(y/n)
```

**Step 6** Either:

- Enter **y** to accept the license and continue with the installation.

Or

- Enter **n** to stop the installation.

If you accepted the license agreement, the installation proceeds.

If Common Services is not installed on the system, this message appears and the installation terminates:

```
Cannot install Common Services 3.0.6. Common Services 3.0.5 is not installed on your
system. You must install Common Services 3.0.5 before installing Common Services 3.0.6.
Common Services 3.0.5 is available as a part of the LMS 2.6 at
http://www.cisco.com/cgi-bin/tablebuild.pl/lms26.
```

If CiscoWorks is in ACS mode, the following message appears:

```
The application that you are installing requires new tasks to be registered with ACS. If
you have already registered this application with ACS from another server, you do not need
to register it again. However if you re-register the application, you will lose any custom
roles that you had created earlier for this application in ACS.
Enter (Y)es to Register and continue installing.
Enter (N)o to continue without registering, (Q)uit.
```

**Step 7** Either:

- Enter **y** to register the application with ACS Server.

Or

- Enter **n** to continue the installation without registering the application.

**Caution**


---

If you enter **y**, to register with ACS server, you will lose the custom roles which are defined in the previous version. If you enter **n**, not to register with ACS server, all the custom roles which are defined in Common Services 3.0.5, will be carried forward.

---

The Daemons Restart Option message appears:

```
If no other CiscoWorks application installations are pending, you can choose to start
CiscoWorks Daemons. Do you want to restart CiscoWorks Daemons at the end of this
installation ? (y/n) [n]:
```

**Step 8** Either:

- Enter **y** to restart the daemons at the end of the installation.

Or

- Enter **n** if you do not want to restart the daemons at the end of the installation.

If you enter **y**, the following warning message appears:

```
Exiting installation beyond this point might result in system instability.
Do you want to continue the installation? (y/n)
```

- Step 9** Either:
- Enter **y** to continue with the installation.

Or

- Enter **n** to stop the installation.

If you enter **y** and continue with the installation, the installation program installs Common Services 3.0.6 in the same directory where you have installed Common Services 3.0.5.

## Verifying the Installation

To verify whether Common Services is installed successfully:

- Step 1** Log into CiscoWorks Server.
- Step 2** Go to **Common Services > Software Center > Software Update**.  
The Software Updates page appears.
- Step 3** Check the version for Common Services in the Products Installed table.  
If Common Services 3.0.6 is installed successfully, it will be listed as 3.0.6.

## Uninstalling Common Services 3.0.6

Use the **Uninstall** script to remove Common Services files and settings.

Uninstall all applications dependent on Common Services before uninstalling Common Services. The uninstallation process will take approximately 10 minutes to complete.



### Caution

You must use the Uninstall script to remove the product. If you try to remove Common Services or its components manually, you may damage your system.

To uninstall Common Services:

- Step 1** As root, enter the following commands to start the uninstall script:

```
# cd /
# /opt/CSCOpX/bin/uninstall.sh
```

where */opt/CSCOpX* is the default installation directory.

If you have installed applications dependent on Common Services, a list of applications appear.

- Step 2** Enter the number corresponding to the option you have chosen or **Q** to quit. You can select more than one component. Enter the number corresponding to the components separated by commas.
- When you remove Common Services, the uninstall script removes any changes made to the */etc/services* file. The */etc* directory still contains all system file changes. The uninstall messages get appended to the */var/tmp/ciscouninstall.log* file.

**Step 3** Enter **Y** to confirm uninstallation of the selected components.

The uninstallation proceeds.

After the uninstall is complete, the following messages appear:

```
All files were deleted successfully.
Possible Warnings/Errors Encountered.
```

The installation program lists the warning and error messages.

**Step 4** Check the following files:

- /etc/syslog.conf  
For syslog changes.
- /etc/services  
To ensure that port assignments for the CiscoWorks applications have been removed.
- /etc/inetd.conf  
To ensure that CiscoWorks tftp entry is removed.

## Known Problems in Common Services 3.0.6

None

## Resolved Problems in Common Services 3.0.6

This section contains the following sections:

- [Customer Found Resolved Problems in Common Services 3.0.6](#)
- [Internally Found Resolved Problems in Common Services 3.0.6](#)

## Customer Found Resolved Problems in Common Services 3.0.6

[Table 1](#) lists the customer found resolved problems in Common Services 3.0.6 that are also available in CS 3.1 (with LMS 3.0).

**Table 1** *Customer Found Resolved Problems in Common Services 3.0.6*

Problem	Description	Explanation
CSCdz05119	CiscoWorks Server integrated with Active Directory Server did not support User Principal Name (UPN) based authentication to Active Directory Server.	This problem has been resolved. CiscoWorks Server integrated with Active Directory Server now supports UPN based authentication to present the credentials to Active Directory Server.

**Table 1** Customer Found Resolved Problems in Common Services 3.0.6

Problem	Description	Explanation
CSCsb97406	The CiscoWorks login screen did not launch after entering <code>http://Server_Name:Port_Number</code> in web browser.  This happened when the CiscoWorks Server in ACS mode. This was because many threads were launched from CiscoWorks environment.	This problem has been resolved by closing all connections established between ACS Server and CiscoWorks Server.
CSCsg52428	Apache executable shipped with Common Services contained many unused module files which might cause security risks.	This problem has been resolved.  Unused modules are now removed from the web server executables.
CSCsh87623	GUI screens did not launch when you ran many jobs.  This was because of improper registration of some of the jobs. This added the error messages in syslog.	This problem has been resolved by replacing the <code>WaitForMultipleObjects</code> function with <code>WaitForSingleObject</code> in the Daemon Manager API code.
CSCsh89486	In a CiscoWorks Server integrated with ACS, devices did not appear in Device Selector although they were added to DCR.  This happened when devices in ACS did not have IP Address configured.	This problem has been resolved.  The devices appear in Device Selector.
CSCsh93500	When you added or removed a device from Network Device Group (NDG) in ACS, Core Admin Module cache corrupted and the devices did not display in CiscoWorks.	This problem has been resolved by rebuilding the device cache.
CSCsi74887	Running the Daemon Manager init script with stop or kill arguments terminated non CiscoWorks processes such as system SSH daemons.	This problem has been resolved.  The non CiscoWorks processes are not terminated when the Daemon Manager init script is run.
CSCsb71245	Stopping Daemon Manager created a core dump in certain cases.	This problem has been resolved.
CSCsc12829	Stopping Daemon Manager took a long time.  This happened if you ran the <code>pdshow</code> command and terminated it when the command did not display any results.	This problem has been resolved.
CSCsd37328	Performing a backup after restoring the data, resulted in a core dump in certain cases.  This happened when you performed a backup after you restored the data in the same of version of CiscoWorks LMS software.	This problem has been resolved by generating standard temp files during backup.
CSCse09319	IP Addresses configured using /31 or /32 masks were reported as invalid.	This problem has been resolved.  The IP Addresses configured using /31 and /32 masks are now treated as valid addresses in CiscoWorks.
CSCse96095	When an SNMPWalk was performed with no starting oid or .1 specified on a device, it failed.	This problem has been resolved.

**Table 1** Customer Found Resolved Problems in Common Services 3.0.6

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsf28207	Group Selector selected more than one object during group assignment.  This happened because the form was submitted twice.  This problem occurred only on Internet Explorer.	This problem has been resolved by removing the form submit using the Java Script functions.
CSCsf96866	Device Center did not resolve the hostname and domain name combination.	This problem has been resolved.  Device Center now resolves the hostname and domain name combination of devices.
CSCsf97090	Common Services Core Admin Module did not add any message to the log files when there was a protocol mismatch between ACS and Common Services.	This problem has been resolved.  Common Services now adds an error message to the log files when there is a protocol mismatch between ACS and Common Services.
CSCsg00563	Authorization failed for few CiscoWorks applications during Common Services—ACS integration in CiscoWorks.  This happened when you entered the hostname of CiscoWorks Server in ACS, instead of IP Address.	This problem has been resolved.  Device without IP Address is now added to cache and authorization succeeds for CiscoWorks even if you have configured hostname during Common Services—ACS integration.
CSCsg02991	SMTP Server Settings did not apply in the Common Services System Preferences page even if you had configured a valid SMTP Server.  This occurred when the SMTP HELLO reply spanned multiple lines.	This problem has been resolved.
CSCsg33950	Edit Identity task was not available in Device Center	This problem has been resolved by adding a new link under the Tools section.
CSCsg34042	When you launched the Edit Device Credentials page from Device Center, the wizard buttons were hidden.	This problem has been resolved.  The Edit Device Credentials page launched from Device Center now has a vertical scroll bar which helps you to scroll down and see the wizard buttons.
CSCsg42058	DCR could not import CSV files with values containing one or more embedded commas.  This happened because the values with embedded commas were not parsed properly.	This problem has been resolved.  The values with embedded commas in DCR CSV import file are now parsed properly.
CSCsg48359	Common Services Home displayed the status of Authorization Mode in red color although the CiscoWorks was integrated properly with ACS Server.  This happened because the authorization request was not sent to ACS in the proper format.	This problem has been resolved.  The authorization requests are now sent to ACS in the proper format.
CSCsg61898	The Who is Logged On report showed incorrect privileges for users configured in ACS.  This was because the report displayed only the local privileges for the users.	This problem has been resolved.  A warning message stating that the report is valid only for the local mode of security is now displayed when you launch the report in ACS mode.

**Table 1** *Customer Found Resolved Problems in Common Services 3.0.6*

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsg86450	CiscoWorks applications such as Device Center and Software Center were not working properly.  This happened if you entered the proxy server credentials or if you performed Software Center operations without restarting daemons.	This problem has been resolved.
CSCsh27277	When application such as RME used Command Services, during device configuration extra lines were inserted in the commands that spanned over multiple lines.  This happened only when applications used SSH Transport protocols provided by Command Services.	This problem has been resolved.  Extra lines are not inserted in the commands that spanned over multiple lines.
CSCsh34009	When a device was probed for supported SSH versions, an additional probe was also sent to see if the device listening on Telnet port.  The Telnet probe was sent even though Telnet is disabled on the device.	This problem has been resolved.  A new API is introduced to probe only the SSH versions.
CSCsh75033	Device Selector appeared empty and did not display the device groups.  This problem occurred when certain device types are managed in CiscoWorks.	This problem has been resolved.  The device groups are now displayed properly in Device Selector.
CSCsi08393	In a DCR Master-Slave setup, packet capture from Slave to Master was not constant and increased over a period of time.	This problem has been resolved.
CSCsi10674	The CiscoWorks Online help system was affected by a cross-site vulnerability through the help topics search.	This problem has been resolved.

[Table 2](#) lists the customer found resolved problems in Common Services 3.0.6 that are also available in CS 3.1.1 (with LMS 3.0 December 2007 Update).

**Table 2** *Customer Found Resolved Problems in Common Services 3.0.6*

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsj52471	Incorrect Display Name was displayed when you registered the CiscoWorks applications from a remote server in the local server.	This problem has been resolved.  The local server now displays the correct Display Name of the remote server.
CSCsg47200	Software Center did not download software updates and device updates from Cisco.com.  This occurred for few Cisco.com or Proxy credentials (username and password).  This was because wrong Base-64 encoding used in Software Center.	This problem has been resolved.  Software Center now uses the Base-64 encoder used by the security module which encodes any combination of username and password properly.

**Table 2** *Customer Found Resolved Problems in Common Services 3.0.6*

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsj58812	Software Center device and package maps were corrupted.  This was because multiple Software Center jobs were started before the completion of the previous jobs.	This problem has been resolved.
CSCsi01380	Support for Western Australia DST Time change was not provided.	This problem has been resolved.  The support for Western Australia DST Time change is now available.
CSCsk09505	Daemon Manager was not stopped when a Solaris system was shut down or rebooted. This resulted in database corruption.	This problem has been resolved.  The Daemon Manager is stopped properly when a Solaris system is shut down or rebooted.
CSCsj25221	Security vulnerability in processing GIF images in Java Runtime Environment was reported.	This problem has been resolved.

## Internally Found Resolved Problems in Common Services 3.0.6

[Table 3](#) lists the resolved problems in Common Services 3.0.6 that are also available in CS 3.1 (with LMS 3.0).

**Table 3** *Resolved Problems in Common Services 3.0.6*

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsh73775	Resource Manager Essentials (RME) Software Image Management could not learn the device prompt when performing a sync archive against the NAM devices.	This problem has been resolved.  A time delay is introduced before reading the data from the NAM devices.
CSCsg99571	In ACS mode, Common Services Home displayed an error on the browser page after a few hours.  This was because the connection to ACS server was not closed properly.	This problem has been resolved.
CSCsj05465	Few CiscoWorks processes were not stopped even after the daemons were stopped.	This problem has been resolved.  The time taken to stop the daemons is now increased from 6 minutes to 10 minutes.
CSCsa26822	The Go button did not work when there were many tables on the same page.	This problem has been resolved.

Table 4 lists the resolved problems in Common Services 3.0.6 that are also available in CS 3.1.1 (with LMS 3.0 December 2007 Update).

**Table 4** Resolved Problems in Common Services 3.0.6

Problem	Description	Explanation
CSCsk28621	Support for New Zealand DST Time change was not provided.	This problem has been resolved. The support for New Zealand DST Time change is now available.
CSCsj53183	UI pages were not accessible because of an Apache crash.	This problem has been resolved. With the modified web server executable and .dll file, the web server do not crash.

## Support for MDF 1.22

Meta Data Framework (MDF) Package defines device types in a uniform way across CiscoWorks applications. This package contains new device types, new device type definitions, new device icons, and solutions to some problems in earlier MDF packages.

Common Services 3.0.6 supports the MDF package version 1.22 that contains the following new device types:

- Cisco Catalyst 2960-24-S Switch (1.3.6.1.4.1.9.1.929)
- Cisco Catalyst 2960-24TC-S Switch (1.3.6.1.4.1.9.1.928)
- Cisco Catalyst 2960-48TC-S Switch (1.3.6.1.4.1.9.1.927)
- Cisco MDS 9216i Multilayer Fabric Switch (1.3.6.1.4.1.9.12.3.1.3.472)
- Cisco 7603 Router (1.3.6.1.4.1.9.1.862)
- Cisco SFS 3504 Multifabric Server Switch (1.3.6.1.4.1.6203.16)
- Cisco BladeCenterH (1.3.6.1.4.1.6203.15)
- Cisco WAE-612 Wide Area Application Engine (1.3.6.1.4.1.9.1.761)
- Cisco ME 3400G-2Common Services-A Switch (1.3.6.1.4.1.9.1.825)
- Cisco Catalyst Switch Module 3110G for IBM BladeCenter (1.3.6.1.4.1.9.1.909)
- Cisco Virtual Switching System (1.3.6.1.4.1.9.1.896)
- Cisco Catalyst 3560E-12D-S Switch (1.3.6.1.4.1.9.1.930)
- Cisco Catalyst 3750G-12S Switch (1.3.6.1.4.1.9.1.530)
- Cisco Unity Express Network Module(1.3.6.1.4.1.9.1.711,1.3.6.1.4.1.9.1.866)
- Cisco Unity Express Advanced Integration Module (1.3.6.1.4.1.9.1.867, 1.3.6.1.4.1.9.1.868)
- Cisco 1861 Integrated Services Router(1.3.6.1.4.1.9.1.939, 1.3.6.1.4.1.9.1.940)
- Cisco 7609 Router(1.3.6.1.4.1.9.1.835)
- Cisco Unified Communications 500 Series for Small Business (1.3.6.1.4.1.9.1.878, 1.3.6.1.4.1.9.1.879, 1.3.6.1.4.1.9.1.880, 1.3.6.1.4.1.9.1.881, 1.3.6.1.4.1.9.1.882, 1.3.6.1.4.1.9.1.883, 1.3.6.1.4.1.9.1.884, 1.3.6.1.4.1.9.1.885, 1.3.6.1.4.1.9.1.886, 1.3.6.1.4.1.9.1.888, 1.3.6.1.4.1.9.1.890, 1.3.6.1.4.1.9.1.892, 1.3.6.1.4.1.9.1.894, 1.3.6.1.4.1.9.1.895)

When you add new device types through MDF Package, it does not guarantee support for these device types in all CiscoWorks applications. Device support has to be provided by individual applications such as DFM, RME and Campus Manager. For a list of supported device types, see the relevant product documentation.

## General Guidelines for Using Common Services 3.0.6

This section describes the general guidelines related to the following tasks, while using Common Services 3.0.6:

- [Backup and Restore](#)
- [Multi-Server Deployment](#)
- [DCR Import and Export](#)

### Backup and Restore

You can restore the data backed up from a server that has Common Services 3.0.x or Common Services 2.2.x installed, on a server that has Common Services 3.0.6 installed.

You must not restore the data backed up from Common Services 3.0.6, on a server that has Common Services 3.0.x (where,  $x \leq 5$ ) installed.

For more details on backing up and restoring data, see the Backing Up Data section in the *User Guide for CiscoWorks Common Services 3.0.5*.

### Multi-Server Deployment

You must upgrade all the servers that are part of Device and Credential Repository (DCR), and Single Sign-On (SSO) domains to Common Services 3.0.5/3.0.6.

DCR Master-Slave setup is not supported with a combination of DCR Master with Common Services 3.0.x (where,  $x \leq 4$ ) and DCR Slave with Common Services 3.0.5/3.0.6.

For more information on Multi-server deployment and SSO see the following sections in the *User Guide for CiscoWorks Common Services 3.0.5*.

- DCR Architecture
- Administering Device and Credential Repository
- Master-Slave Configuration Prerequisites
- Managing Security in Multi-Server Mode
- Enabling Single Sign-On

## DCR Import and Export

You can export devices and credentials from a Common Services 3.x server and import them into a Common Services 3.0.5 server. You can also export devices and credentials from a Common Services 3.0.6 server and import them into another Common Services 3.0.6 server.

You must not import devices and credentials from a Common Services 3.0.6 sever into a Common Services 3.0 server.

For more information on importing and exporting devices and credentials, see the following sections in the *User Guide for CiscoWorks Common Services 3.0.5*.

- Importing Devices and Credentials
- Exporting Devices and Credentials

## Related Documentation

This section contains the information of related documentation of Common Services 3.0.6.

This section contains:

- [Documentation for Common Services 3.0.6](#)
- [Documentation for Common Services 3.0.5](#)
- [Accessing Online Help](#)

## Documentation for Common Services 3.0.6

This table contains the documentation set for Common Services 3.0.6:

Document Title	Available Formats
Readme for CiscoWorks Common Services 3.0.6 on Solaris ( <i>this document</i> )	PDF on Cisco.com Software Download site: <a href="http://www.cisco.com/cgi-bin/tablebuild.pl/cd-one-3des">http://www.cisco.com/cgi-bin/tablebuild.pl/cd-one-3des</a>
Readme for CiscoWorks Common Services 3.0.6 on Windows	PDF on Cisco.com Software Download site: <a href="http://www.cisco.com/cgi-bin/tablebuild.pl/cd-one-3des">http://www.cisco.com/cgi-bin/tablebuild.pl/cd-one-3des</a>
Context-sensitive Online help	Part of software image. See <a href="#">Accessing Online Help</a> for more information.

## Documentation for Common Services 3.0.5

This table contains the documentation set for Common Services 3.0.5:

Document Title	Available Formats
Release Notes for CiscoWorks Common Services 3.0.5 on Solaris	<ul style="list-style-type: none"> <li>PDF on the LMS 2.6 Documentation CD-ROM.</li> <li>On Cisco.com at: <a href="http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html">http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html</a></li> </ul>
Release Notes for CiscoWorks Common Services 3.0.5 on Windows	<ul style="list-style-type: none"> <li>PDF on the LMS 2.6 Documentation CD-ROM.</li> <li>On Cisco.com at: <a href="http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html">http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html</a></li> </ul>
User Guide for CiscoWorks Common Services 3.0.5	<ul style="list-style-type: none"> <li>PDF on the LMS 2.6 Documentation CD-ROM.</li> <li>On Cisco.com at: <a href="http://cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html">http://cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html</a></li> </ul>
Installation and Setup Guide for CiscoWorks Common Services 3.0.5 (Includes CiscoView) on Solaris	<ul style="list-style-type: none"> <li>PDF on the LMS 2.6 Documentation CD-ROM.</li> <li>On Cisco.com at: <a href="http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html">http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html</a></li> </ul>
Installation and Setup Guide for CiscoWorks Common Services 3.0.5 (Includes CiscoView) on Windows	<ul style="list-style-type: none"> <li>PDF on the LMS 2.6 Documentation CD-ROM.</li> <li>On Cisco.com at: <a href="http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html">http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html</a></li> </ul>

## Accessing Online Help

To access the Online help, go to CiscoWorks home page and click Help located at the extreme right corner of your browser window.

The Online help launches in a separate browser window.

## Open Source License Acknowledgements

The following acknowledgements 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](mailto:openssl-core@openssl.org).

### OpenSSL License:

© 1998-1999 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](mailto: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 ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**Original SSLeay License:**

© 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].

This document is to be used in conjunction with the documents listed in the Common Services 3.0.6 Related Documentation section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient,

IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

*Readme for CiscoWorks Common Services 3.0.6 on Solaris*  
Copyright © 2007, Cisco Systems, Inc.  
All rights reserved

