



# Readme Document for Common Services 3.0 Service Pack 2 on Solaris

---

This Readme document is about Common Services 3.0 Service Pack 2 (CS 3.0 SP2) on Solaris and contains the following sections:

- [Description, page 2](#)
- [New Features in CS 3.0 SP2, page 2](#)
- [Resolved Problems in CS 3.0 SP2, page 4](#)
- [Hardware and Software Requirements, page 19](#)
- [Browser Support, page 19](#)
- [Downloading CS 3.0 SP2, page 19](#)
- [Installing CS 3.0 SP2, page 23](#)
- [Uninstalling CS 3.0 SP2, page 24](#)
- [General Guidelines for Using CS 3.0 SP2, page 26](#)
- [Documentation Addendum, page 28](#)



---

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

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

# Description

Service Packs (SP) are cumulative and incremental releases over existing CiscoWorks Common Services software.

Each Service Pack includes:

- Solutions for critical issues that severely impact your production environment.
- Selective upgrade support for important 3rd party applications and Operating System environments.

Each Service Pack release sustains an existing major or minor release (version X.0 or X.y), and addresses critical field issues related to quality, vulnerability, and obsolescence.

Common Services 3.0 Service Pack 2 (CS 3.0 SP2) is the second incremental release over Common Services 3.0 (CS 3.0).

CS 3.0 SP1, the first incremental release over CS 3.0 has been rolled in to CS 3.0 SP2.

## New Features in CS 3.0 SP2

The following are the new features and enhancements in CS 3.0 SP2:

- **acsRegCli.pl** command line script enables registration of individual applications with ACS without affecting the registration status of other applications.
- Audit log provides information on:
  - CiscoWorks Local user addition
  - CiscoWorks Local user modification
  - CiscoWorks Local user deletion
- Conflict resolution option in **acrc11** overwrites DCR data from import source.
- Standardized Service Pack package format for distribution from Cisco.com.
- Software Center CLI provides the option to display the list of dependent packages for a specified psu package.

- Support for Java Plug-in version 1.4.2\_08.
- Support for Meta Data Framework (MDF) package 1.4.

The following new features and enhancements that were part of CS 3.0 SP1 are also rolled in to CS 3.0 SP2:

- Enhancements in Device and Credential Repository (DCR)
  - Support for HTTP related credentials and attributes
  - Support for CNS Configuration Engine and CNS Managed devices



---

**Note** See the application documentation for details on the application version that supports these features.

---

- Enhancements in Software Center
  - Prompt for Cisco.com credentials while selecting, scheduling, and downloading software and device updates
  - Prompt for Proxy credentials while selecting, scheduling, and downloading software and device updates if you have configured Proxy settings
- Support for Cisco Secure ACS 3.3.2
- New options as part of command line arguments to cwjava
- Uninstallation of CS 3.0 Service Packs

# Resolved Problems in CS 3.0 SP2

[Table 1](#) lists the problems in CS 3.0 that are resolved in CS 3.0 SP2.

[Table 2](#) lists the problems in CS 3.0 that were resolved in CS 3.0 SP1.

**Table 1** Resolved Problems in CS 3.0 SP2

Problem	Description	Explanation
<b>Admin Related Resolved Problems</b>		
CSCsa56067	Configuring Microsoft SMTP Server with a valid name or IP address failed on CiscoWorks Server.	Configuring Microsoft SMTP server, was not supported in CS 3.0. CS 3.0 SP2 supports configuring Microsoft SMTP Server.
CSCsb05729	Java Plug-in 1.4.2_06-sparc.tar.gz pam.sh did not have execute permission.	When Java Plug-in1.4.2_06-sparc.tar.gz was extracted into runtime, the file pam.sh did not have the execute permissions. CS 3.0 SP2 supports Java Plug-in 1.4.2_08 that has the file pam.sh with the execute permissions.
CSCsa99960	Could not add username with fewer than five characters in LMS 2.5.	LMS 2.5 did not allow CiscoWorks Local username with fewer than five characters. In CS 3.0 SP2, there is an option to add a property 'validateUser' in the ss.properties file. To add a local username with less than 5 characters, change the entry for 'validateUser' to <b>false</b> in <i>NMSROOT/lib/classpath/ss.properties</i> file. You must restart the Daemon Manager after updating this file.

**Table 1** Resolved Problems in CS 3.0 SP2 (Continued)

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa89029	Proxy settings required a username and password to be set.	In CS 3.0 SP1, the individual user proxy settings required a username and password to be set if you configured a proxy server.  However, you do not require authenticating proxies.  In CS 3.0 SP2, all users require authenticating proxies.
<b>Backup and Restore Related Resolved Problems</b>		
CSCsb02717	Restore failed while restoring certificate.	In CS 3.0, while restoring, the user was prompted to restore the certificate, even if the certificate was invalid.  If you select <b>y</b> and continued to restore the invalid certificate, DCRServer did not start and the RME restoration failed.  CS 3.0 SP2 checks certificate validity before restoring the backed up certificate. <ul style="list-style-type: none"> <li>• If the hostname of the backed up certificate is different from that of the current hostname or if the certificate is not valid, the existing certificate is retained.</li> <li>• If the hostname of the two certificates are same and the certificate is valid, you must confirm overwriting the certificate and proceed.</li> </ul>
CSCsa38245	XML maintree and EDS filter needed to be removed from Backup and Restore.	Unwanted codes for XML maintree and EDS filter have been removed from Backup and Restore functionality.
<b>CAM Related Resolved Problems</b>		
CSCsb01881	User management operations for CiscoWorks Local user needed to be logged in Audit logs.	Auditing information has been added to the audit log for all CiscoWorks Local user management operations in CS 3.0 SP2.

**Table 1** Resolved Problems in CS 3.0 SP2 (Continued)

Problem	Description	Explanation
<b>Device Center Related Resolved Problems</b>		
CSCsa91963	Using community string with special characters failed in Management Station.	Using community string with special characters like %\$&, failed in Management Station.  In CS 3.0 SP2, you can use community strings with special characters at Device Center > Management Station To Device.
CSCeh70483	Management Station to Device had the domain field populated for all devices with Cisco.com.	In CS 3.0, Device Center Management Station to Device had Cisco.com in the domain field for every device.  This string has been removed in CS 3.0 SP2.
<b>DCR Related Resolved Problems</b>		
CSCsa85415	Incorrect device icons used for security devices.	MDF 1.4 device package containing the updated icons will be installed as part of CS 3.0 SP2 installation.  Uninstalling CS 3.0 SP2 does not uninstall the MDF package.
CSCsa48533	Device tree is missing after initialization.	If you open the DCR GUI (used to add, delete, and edit credentials) immediately after daemon manager restart, the device tree for the DCR is sometimes missing.  This problem has been resolved in CS 3.0 SP2.  DCR GUI will not appear if the CMFOGSServer is down.  If the OGSServer is down, the message <code>OGSServer down error</code> , appears.  Refresh the page after the server is up, to view the DCR GUI.

Table 1 Resolved Problems in CS 3.0 SP2 (Continued)

Problem	Description	Explanation
CSCsa62916	Import from ACS fails if device does not have IP address.	In CS 3.0, if ACS had devices without IP address, import from ACS into DCR failed.  This problem has been resolved in CS 3.0 SP2.
CSCsa83444	<code>dcrcli</code> did not allow import data to overwrite existing DCR values.	In CS 3.0, there was no option in the <code>dcrcli import</code> commands to allow data imported from the various sources (for example, a file) to overwrite the values that are already in DCR.  In CS 3.0 SP2, a conflict resolution option is added in <code>dcrcli import</code> commands, using which you can choose to retain data in DCR or the data from the import source, when there is a conflict.  <code>cr</code> (conflict resolution) is the option for conflict resolution. See the Online Help for more details.
CSCsa45039	DCR export did not complete if the file path had spaces.	In CS 3.0, DCR export did not complete if the file path had spaces.  This problem has been resolved in CS 3.0 SP2.
CSCeh53870	Incorrect spelling in import status error message.	Correct error message has been added.  The error message has been changed as <code>No records found. There may not be any previous import operation.</code>
CSCeh78389	JOS DCR Scheduled Import jobs caused internal server error.	In CS 3.0, scheduling a DCR import job fails in server running Japanese OS (JOS).  This problem has been resolved in CS 3.0 SP2.

**Table 1** Resolved Problems in CS 3.0 SP2 (Continued)

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa96498	DCR logging had to be changed for Start and Stop services and events.	In CS 3.0 SP2, the following changes have been made in DCR logging: <ul style="list-style-type: none"> <li>• When DCRServer starts and or stops successfully, the information is logged (even in non-DEBUG mode).</li> <li>• The event messages are logged (XML format events) in DCR logs only when DEBUG is enabled.</li> </ul>
CSCsa78299	If the number of device groups in DCR device selector increased, it took a long time to select the root node.	This problem has been resolved in CS 3.0 SP2.

**Install Related Resolved Problems**

CSCsb07645	Prompt had to be removed while changing casuser attributes.	The CS 3.0 installation framework prompted <i>Do you want to continue</i> before trying to change the casuser attributes.  This prompt has been removed in CS 3.0 SP2.
CSCsb07694	Custom roles in ACS were overwritten on application/SP installation.	If you installed any Service Pack or application on top of CS3.0, when AAA mode is set to ACS, all the custom roles you created were lost.  This happened only with Cisco Secure ACS version 3.3.x.  Installing CS 3.0 SP2 will not register any application with the ACS server. So the custom roles, if any, will be retained.

**Process Management Related Resolved Problems**

CSCsa64386	DM warning had to be changed during startup.	Misleading warning appeared when installation was broken.  This problem has been resolved in CS 3.0 SP2.
------------	--	--

**Software Center Related Resolved Problems**

**Table 1** *Resolved Problems in CS 3.0 SP2 (Continued)*

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa39122	Inconsistent behavior if dependent packages across applications were not selected for download through Software Center > Software Updates.	<p>If dependent packages were not selected for download through Software Center &gt; Software Updates, only the main package got installed.</p> <p>This problem has been resolved in CS 3.0 SP2.</p> <p>You can use the CLI option to download the packages and select them for installation, after ensuring that all the packages are in the server location.</p>
CSCsa73676	Software Center did not automatically pick the dependent packages.	<p>In Software Center &gt; Device Update, after selecting a package to installing or downloading, the summary screen did not show the list of dependent packages.</p> <p>This problem has been resolved in CS 3.0 SP2.</p>
CSCsa73649	Incorrect version reported for missing base package(s) of device updates.	<p>When performing an improper device update which has base package inconsistencies, the Activity Log displayed the incorrect version for the base package.</p> <p>This problem has been resolved in CS 3.0 SP2.</p>
CSCsa80117	Software Center did not report failed installation of packages on the UI.	<p>Software Center did not report failed installation of packages on the UI.</p> <p>This problem has been resolved in CS 3.0 SP2.</p>

Table 1 Resolved Problems in CS 3.0 SP2 (Continued)

Problem	Description	Explanation
CSCsa70667	Software Center CLI did not have the option to display the list of dependent packages for a specified psu package.	<p>This problem has been resolved in CS 3.0 SP2.</p> <p>A separate option <b>-pkgDependents</b> has been added which displays the list of dependent packages for a specified package, of a specified product.</p> <p>The short form of the option is <b>-pdep</b>.</p>
CSCsa88729	Software Center > Device Update operation failed when attempting large updates.	<p>Device Update operation failed when attempting large updates.</p> <p>This problem has been resolved in CS 3.0 SP2.</p>
CSCsa89294	Setting up a proxy breaks other applications.	<p>In CS 3.0, if a proxy was configured in CiscoWorks, and there was an error connecting to Cisco.com, the proxy settings may not be removed from the System properties.</p> <p>The subsequent HTTP sockets established from within Tomcat tried to use these proxy settings.</p> <p>This problem has been resolved in CS 3.0 SP2.</p> <p>Proxy settings have been removed from the System properties.</p>

**Table 1** Resolved Problems in CS 3.0 SP2 (Continued)

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa93475	Notification needed to inform you to manually install Software update.	In CS 3.0, could not notify you that the updates downloaded through Software Center> Software Updates will not be installed through the Software Centre flow.  In CS 3.0 SP2, the following note has been added:  You would need to manually install these software updates, as per the instructions in the associated readme file. Software Center does not support install of the same.
CSCsb01970	Sanctify application registration / unregistration with Software Center.	Software Center framework must sanctify every application's registration / unregistration / reregistration cases, as part of the integrating flow.
CSCsb17998	Software Updates do not work as expected in CiscoView.	This problem has been resolved in CS 3.0 SP2.
<b>SNMP Related Resolved Problems</b>		
CSCin88982	Should resolve hostname containing "-" in IP address.	In CS 3.0, hostname that have "-" escaped from address translation.  Since it has "-", the hostname is assumed as an IP address range and trying to parse the range caused an error.  This problem has been resolved in CS 3.0 SP2, by adding the check for "-" and hostname combination.
<b>ESS Related Resolved Problems</b>		
CSCsa71689	LWMS called System.exit() if cookie validation failed.	LWMS used cookie validation for authentication. When the cookie is invalid LWMS called System.exit() and the rest of the code terminated abruptly.  This problem has been resolved in CS 3.0 SP2.

**Table 1** *Resolved Problems in CS 3.0 SP2 (Continued)*

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
<b>JRM Related Resolved Problems</b>		
CSCsa86805	Canceling a running periodic job remained in the <code>GettingCanceled</code> state for ever.	While canceling a running periodic job, the status of the job remains as <code>GettingCanceled</code> .  This problem has been resolved in CS 3.0 SP2.
CSCsb41959	Error while locking and unlocking JRM.	When more than 1500 devices were tried in an RME job, error appeared while locking and unlocking the devices.  In CS 3.0 SP2, this problem has been resolved by increasing the size of the native stack.
<b>General Resolved Problems</b>		
CSCsb29106	Needed to upgrade Java Plug-in version.  This was caused by a security vulnerability in the implementation of JRE in the Java Plug-in shipped by Common Services.	In CS 3.0 SP2, the Java Plug-in is upgraded to 1.4.2_08.

**Table 2** Resolved Problems in CS 3.0 SP1

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
<b>Admin Related Resolved Problems</b>		
CSCsa88296	Proxy server port validation needed to be set in the range 1-65535.	<p>This problem occurs only if you have installed CS 3.0 SP1 before 9 June, 2005.</p> <p>This problem is not applicable to CS 3.0.</p> <p>If you have installed CS3.0 SP1 before June, 9, 2005, then you can not configure port numbers in the range 1-1023 in Common Services &gt; Server &gt; Security &gt; Proxy Server Setup page.</p> <p>If you try to configure a proxy server on any of the ports in the range 1-1023, the following alert message appears:</p> <p>ProxyServer port must be a number in range 1024- 65535.</p> <p>This problem has been resolved in CS3.0 SP1, posted on 9 June, 2005. You can configure proxy servers in port numbers in the range 1-65535.</p>
<b>DCR Related Resolved Problems</b>		
CSCsa16158	Auto Update Server (AUS) device addition did not have Username, Password, and Enable Password.	<p>Two separate types of credentials were needed for an AUS device.</p> <ul style="list-style-type: none"> <li>• Credentials used when a management station or other entity contacted the AUS device directly and needed authentication.</li> <li>• Credentials sent by a device to the AUS server to authenticate the device with the server.</li> </ul> <p>In CS 3.0 SP1, while adding AUS devices into DCR, you are prompted for Standard credentials and HTTP credentials.</p>

**Table 2** Resolved Problems in CS 3.0 SP1 (Continued)

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa23143	Support for CNS Configuration Engine and CNS Devices.	In CS 3.0 SP1, DCR supported management of CNS Configuration Engine (CNS Server) and CNS Devices (devices managed by CNS Server).
CSCsa52333	Prompt HTTP credentials in Device and Credential Repository (DCR) GUI.	<p>In CS3.0, DCR had the HTTP username and HTTP password as attributes. However, the user could not enter these values in DCR GUI.</p> <p>In CS 3.0 SP1, DCR lists the following HTTP credential fields in the GUI:</p> <ul style="list-style-type: none"> <li>• HTTP username</li> <li>• HTTP password</li> <li>• HTTP port</li> <li>• HTTPS port</li> <li>• Certificate Common Name</li> <li>• Current mode (HTTP or HTTPS)</li> </ul>
<b>Software Center Related Resolved Problems</b>		
CSCsa52966	Needed to prompt for Cisco.com and Proxy credentials when performing software downloads.	<p>In CS 3.0, when you set up Cisco.com credentials at Server &gt; Security &gt; CCO setup, all other users could use your Cisco.com account to download software.</p> <p>In CS 3.0 SP1, each time you attempt device updates or software updates from Cisco.com, you are prompted for Cisco.com credentials.</p> <p>Proxy credentials are also prompted for, if the proxy server is configured at Server &gt; Security &gt; Proxy Setup.</p>

**Table 2** Resolved Problems in CS 3.0 SP1 (Continued)

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa55959	MDF-PSU Adapter code did not remove MDF cache.	During MDF package installation, MDF updates did not get reflected in DCR GUI.  In CS 3.0 SP1, the CMF Adapter is modified to take care of this.
CSCsa58278	Did not support add-on application adapters in Software Center.	CS 3.0 did not support installing adapter packages.  In CS 3.0 SP1, if there is an adapter package in the selected list of packages, it is marked and installed as a separate package.
CSCsa70185	Software Center detected only Readme files that had .README extension.	In CS 3.0 SP1, Software Center supports .readme and .readme.* files.
CSCeh38707	During validation of the Cisco.com credentials, an attempt was made to connect to www.cisco.com/en/US/partner site.	The URL should be either CCO.cisco.com or just cisco.com.  This has been resolved in CS 3.0 SP1.
<b>Event Services Related Resolved Problems</b>		
CSCeg62066	Tibco did not support publishing or subscribing to MapMessages	In CS 3.0, Tibco did not support publishing or subscribing to MapMessages.  In CS 3.0 SP1, Tibco supports publishing or subscribing to MapMessages.
CSCsa42779	Minor issues while receiving jms messages.	When a JMS-LWMS publisher published the events on a particular topic, that event was not received by a jms-lwms subscriber for the first time.  This occurred because when the publisher published the event, it had to create a corresponding mailbox.  In CS 3.0 SP1, a mailbox is added while publishing events.

**Table 2** Resolved Problems in CS 3.0 SP1 (Continued)

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa59368	CS needs to enable LWMS gateway on Tomcat startup.	<p>To forward LWMS events to Tibco and vice versa, Common Services needed to enable the LWMS gateway.</p> <p>CS launched the following URL after login to forward events:</p> <pre>http[s]://server:port/CSCOnm/servlet/com.cisco.nm.cmf.ess.servlet.LTGwayservlet</pre> <p>In CS 3.0 SP1, this servlet gets automatically loaded during startup when you add <code>load-on-startup</code> in web.xml for this servlet.</p>
<b>JRM Related Resolved Problems</b>		
CSCsa37866	JobType needed display value.	In CS 3.0 SP1, JRM displays the Job Type that is provided by the application when the job is created.
CSCsa49724	Could not connect to JRM; tasks such as List Jobs hung.	<p>When multiple jobs were scheduled for a few hundred devices, JRM displayed an OutOfMemory error.</p> <p>In CS 3.0 SP1, the heap memory size is increased, and a few ORB parameters are tuned to resolve this problem.</p>
<b>Install Related Resolved Problems</b>		
CSCsa63439	CS Service Packs did not support uninstallation.	CS 3.0 SP1 supports uninstallation of CS Service Packs.
<b>Backup and Restore Related Resolved Problems</b>		

**Table 2** Resolved Problems in CS 3.0 SP1 (Continued)

<b>Problem</b>	<b>Description</b>	<b>Explanation</b>
CSCsa12929	PERL applications in CiscoWorks that required fork() emulation or large file support did not work.	<p>PERL applications that were shipped with CiscoWorks (5.00502) did not support large files on Solaris or Windows.</p> <p>The <b>stat</b> function returned either 0 or a negative number when it encountered files greater than 2 GB.</p> <p>In CS 3.0 SP1, large files are supported by a helper utility, <code>logrot_stat</code> located at <code>NMSROOT/bin</code>.</p>
<b>Security Related Resolved Problems</b>		
CSCsa50470	Authorization error in DBreader when logged into any Common Services server with Fully Qualified Domain Name (FQDN).	This error has been corrected in CS 3.0 SP1.
<b>MDF Related Resolved Problems</b>		
CSCsa57266	New MDF types for sysObjectIds for the PIX/ASA devices.	CS 3.0 SP1 includes the MDF 1.2 package that contains the new set of sysObjectIds.
CSCsa46502	Need MDF support for Catalyst 6000 CMM Service Module.	CS 3.0 SP1 includes the MDF 1.2 package that contains the new set of sysObjectIds.
<b>General Resolved Problems</b>		
CSCef95618	Common Services should compile and ship with JDOM 1.0 instead of beta8.	<p>CS 3.0 was compiled with JDOM beta8, and also installed beta8 in the Tomcat/shared directory.</p> <p>CS 3.0 SP1 supports JDOM 1.0, that is the first official release of JDOM.</p>

Table 2 Resolved Problems in CS 3.0 SP1 (Continued)

Problem	Description	Explanation
CSCsa38726	Could not specify jar files by manifest in cwjava.	<p>Several processes registered with the Daemon Manager had many jar files and required long command line arguments.</p> <p>In CS 3.0 SP1, the following options are included as part of command line arguments to cwjava:</p> <ul style="list-style-type: none"> <li>• <code>-cp:mf &lt;manifest file&gt;</code></li> <li>• <code>-cp:amf &lt;append manifest file&gt;</code></li> <li>• <code>-cp:pmf &lt;prepend manifest file&gt;</code></li> </ul> <p>These are for passing the manifest file.</p>
CSCsa52301	Discovery went into an infinite loop when Multiplexing and Multiple community were enabled.	<p>When Multiplexing and Multiple community were enabled, the master request as well as the individual requests tried multiple community entries.</p> <p>In CS 3.0 SP1, SNMP checks whether the request has an associated master request. If so, it times-out individual requests.</p>

# Hardware and Software Requirements

CiscoWorks Common Services 3.0 or CiscoWorks Common Services 3.0 SP1 must be installed on your system.

Hardware and software requirements for CS 3.0 SP2 are similar to those needed for Common Services 3.0 installation.

To check the hardware and software requirements, see [Installation and Setup Guide for CiscoWorks Common Services 3.0 \(Includes CiscoView\) on Solaris](#).

**Note**

---

CS 3.0 SP2 installation checks for Solaris patch 112874-31, apart from the patches required/recommended for CS 3.0. We recommend you download and install this patch on the Server.

---

To get the detailed documentation on CiscoWorks Common Services 3.0, go to: [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000\\_d/comser30/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/index.htm)

## Browser Support

- Netscape Navigator 7.0.
- Mozilla 1.7.

**Note**

---

You must install OS patches on the client system as suggested in the Readme for Mozilla.

---

## Downloading CS 3.0 SP2

You can download CS 3.0 SP2 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

The CS 3.0 SP2 is available on Cisco.com.

To download CS 3.0 SP2:

- 
- Step 1** Click <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-cd-one>
  - Step 2** Enter your user name and password.
  - Step 3** Locate the file cwcs3\_0\_2\_sol.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 the CS 3.0 SP2.

To download CS 3.0 SP2 from Software Center:

- 
- Step 1** From the CiscoWorks Homepage, 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**
    - Or
    - **Select Updates**
-

To download CS 3.0 SP2 using the Download Updates option:

- 
- Step 1** Click **Download Updates** in the Software Updates page.  
The CCO and Proxy Server Credentials dialog box appears.
- Step 2** Enter your CCO username and password. Both are mandatory.  
Enter the Proxy server username and password only if you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**.
- 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 device or software updates in the same directory where you have installed CiscoWorks Common Services, or any of its sub- directories. Also you can not download device or software 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. The Summary page shows a summary of your inputs.
- Step 6** Click **Finish** to confirm the download operation.
- 

To download CS 3.0 SP2 using the Select Updates option:

- 
- Step 1** Click **Select Updates** in the Software Updates page.  
The CCO and Proxy Server Credentials dialog box appears.
- Step 2** Enter your CCO username and password. Both are mandatory.  
Enter the Proxy server username and password only if you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**.  
The available Image page appears:

**Step 3** Select the cwcs3\_0\_2\_sol.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 device or software updates in the same directory where you have installed CiscoWorks Common Services, or any of its sub- directories. Also you can not download device or software 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. The Summary page shows a summary of your inputs.

**Step 7** Click **Finish** to confirm the download operation.

---

# Installing CS 3.0 SP2

This section provides information on installing CS 3.0 SP2 on a Solaris platform.

You must download the installable image either from Cisco.com or from Common Services Software Center. You must install CS 3.0 SP2 on a server that has CS 3.0/CS 3.0 SP1 installed.

To install CS 3.0 SP2:

---

**Step 1** Unzip the `cwcs3_0_2_sol.zip` file by entering:

```
unzip cwcs3_0_2_sol.zip
```

The contents of the zip file are extracted to the directory where you have downloaded the zip file.

The following files are listed:

- `cwcs3_0_2_sol`
- `/com/cisco/.../PkgDescr.class`

The following files are listed under `cwcs3_0_2_sol`:

- `cwcs3_0_2_sol.readme`
- `cwcs3_0_2_sol.readme.pdf`
- `cwcs3_0_2_sol-installer.sh`
- `setup.sh`
- `cwcs3_0_2_sol.zip`

**Step 2** Change the directory to `cwcs3_0_2_sol` by entering:

```
cd /Downloaded directory/cwcs3_0_2_sol
```

**Step 3** Run the installation program by entering either:

```
./setup.sh
```

Or

```
./cwcs3_0_2_sol-installer.sh
```

This script unzips the cwcs3\_0\_2\_sol.zip file and runs the installer.

A message appears:

Press **ENTER** to read/browse the following License Agreement:

**Step 4** 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 5** Enter **y** to accept the license and proceed with the installation.

Or

Enter **n** to deny and stop the installation.

If you accept the license agreement and continue with the installation, the installation program installs CS 3.0 SP2 in the same directory where you have installed CS 3.0.

---

## Uninstalling CS 3.0 SP2

This section provides information on uninstalling CS 3.0 SP2 on a Solaris platform.

You can uninstall CS 3.0 SP2 alone. The installation program backs up the files that will be modified and deleted during the installation of SP2. This backup is done during SP2 installation, before the installation of the packages.

The backup is stored as a tar.Z file under *NMSROOT*/backup/cdone. *NMSROOT* is the directory where you have installed CiscoWorks Common Services.

To uninstall CS 3.0 SP2 on Solaris:

---

**Step 1** At the command prompt, enter:

```
cd /NMSROOT/bin
```

**Step 2** Enter:

```
NMSROOT/bin/perl cs_sp_uninstall.pl
```

A message appears:

```
Do you really want to uninstall Service Pack (Y/N) y
```

**Step 3** Enter **y** to continue uninstallation.

The following message appears:

```
Starting Common Services SP uninstall  
You can find the messages logged in /var/tmp/ciscouninstall.log
```

The uninstallation completes and the following message appears:

```
CS Service Pack Uninstall Completed.
```

**Step 4** Check the ciscouninstall.log for possible messages during uninstallation.

---

## Notes on Uninstallation

- You cannot uninstall CS 3.0 SP2 if any of your CiscoWorks applications depends on CS 3.0 SP2.
- If you uninstall CS 3.0 SP2 on a server that has CS 3.0, CS 3.0 SP1 and CS 3.0 SP2, only CS 3.0 SP2 will be uninstalled. The CS 3.0 SP1 setup will be retained.
- If you uninstall CS 3.0 SP2 on a server that has CS 3.0 and CS 3.0 SP2, only CS 3.0 SP2 will be uninstalled. CS 3.0 will be retained.
- The uninstallation script for CS 3.0 SP2 restores the backup of the files by adding, modifying, or deleting the files. In this way it avoids uninstalling Common Services 3.0.
- All configuration changes that occurs during the installation of CS 3.0 SP2 will be reverted.

- Any configuration change done after the installation of CS 3.0 SP2 will be retained.
- Uninstallation of CS 3.0 SP2 will not remove the newly added attributes and related data for DCR, from the database. However, this will not impact your CiscoWorks server. You can still use the server normally as it was before installing CS 3.0 SP2.
- The Metadata Framework (MDF) package version 1.4 that is installed as part of CS 3.0 SP2 will not be uninstalled.

## General Guidelines for Using CS 3.0 SP2

This section describes the general guidelines related to the following tasks, while using CS 3.0 SP2:

- [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 CS 3.0 SP1/SP2, CS 3.0, CWCS 2.2, or CDOne Fifth Edition installed, on a server that has CS 3.0 SP2 installed.

You must not restore the data backed up from a CS 3.0 SP2 server, on a server that has CS 3.0 installed. The database changes in CS 3.0 SP2, for Device and Credential Repository (DCR), may cause discrepancies.

For more details on backing up and restoring data, see [Backing Up Data](#) section in the *User Guide for CiscoWorks Common Services 3.0*.

## Multi-server Deployment

You must upgrade all the servers part of Device and Credential Repository (DCR), and Single Sign-On (SSO) domains to CS 3.0 SP2.

CS 3.0 SP2 does not support a DCR Master-Slave setup with a mix of CS 3.0 and CS 3.0 SP1/SP2 servers.

For more information on Multi-server deployment and SSO see the following sections in the *User Guide for CiscoWorks Common Services 3.0*.

- [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 CS 3.0/CS 3.0 SP1 server and import them into a CS 3.0 SP2 server. You can also export devices and credentials from a CS 3.0 SP2 server and import them into another CS 3.0 SP2 server.

You must not import devices and credentials from a CS 3.0 SP2 sever into a CS 3.0 server. The changes in CS 3.0 SP2, for Device and Credential Repository (DCR), may cause discrepancies.

For more information on importing and exporting devices and credentials see the following sections in the *User Guide for CiscoWorks Common Services 3.0*:

- [Importing Devices and Credentials](#)
- [Exporting Devices and Credentials](#)

# Documentation Addendum

This section describes the new features and work flows that are added or changed in CS 3.0 SP2. This section contains:

- [Registering Individual Applications With ACS Using CLI](#)
- [Support for MDF Package 1.4](#)

Following are the new features and work flows that are added or changed in CS 3.0 SP1. Since CS3.0 SP2 is cumulative, all these changes are available in CS 3.0 SP2, also.

- [Adding Peer Server Certificates](#)
- [New Features and Enhancements in Device and Credential Repository](#)
- [New Features in Software Center](#)

## Registering Individual Applications With ACS Using CLI

If you register an application using the **Register all installed applications with ACS** check box in the GUI, it will reregister all the installed applications with ACS. This leads to loss of all the custom roles created till then in ACS. This is applicable only if you are using ACS 3.3.x.

You can use the `acsRegCli.pl` command line script to register an application without affecting the registration status of other applications. The script is located at `NMSROOT/bin`.

You can run `acsRegCli.pl` only when the CiscoWorks server is in ACS mode.

You can login to the CiscoWorks server using the ACS log in module.

See [Setting the Login Module to ACS](#) section in the *User Guide for CiscoWorks Common Services 3.0* for more details on logging in using ACS.

**AcsRegCli.pl** does the following:

- Lists the applications registered with ACS from this CiscoWorks server.
- Lists the applications installed in this CiscoWorks server that are not registered with ACS.
- Registers a given application with ACS.
- Registers all the installed applications with ACS.

## Running the Script

To get a list of available options, run the script **AcsRegCli.pl** without specifying any option.

The following options will be listed:

- **listRegApp**—List the applications registered with ACS in the current CiscoWorks server.
- **listNotRegApp**—List the installed applications that are not registered with ACS in the current CiscoWorks server.
- **register *AppName***—Register an application with ACS. *AppName* is the name by which an application will be registered with ACS.

To know this value, run **AcsRegCli.pl** with the option `-listRegApp` or `-listNotRegApp`.

- **register all**— Register all the installed applications with ACS.

For Example:

```
/opt/CSCOpX/bin/perl /opt/CSCOpX/bin/AcsRegCli.pl -register rme
```

This registers RME with ACS.

If the application is already registered with ACS, you are prompted to confirm whether you want to proceed with the registration. If you confirm this, the application is registered with ACS, and any custom roles created in ACS for this application are lost.

If you use the **-register all** option, you are prompted to confirm whether you want to proceed with registering all the installed applications with ACS. If you confirm, all the installed applications will be registered with ACS, and any custom roles created in ACS are lost.

You will be prompted for confirmation even when you have not registered the application from the current server. If you have already registered the application with ACS from another server and if you confirm and proceed after the warning message, any custom roles you have created in ACS for this application will be lost.

## Notes on Usage

During the installation of CS 3.0 SP2, the following assumptions are made:

- If the Cisco Works server is in non ACS mode, none of the existing applications are considered registered with ACS. This occurs even if some of the applications are already registered with ACS.
- If the Cisco Works server is in ACS mode, all the existing applications are considered registered with ACS. This occurs even if some of the applications are not registered with ACS.

Hence, `-listRegApp` and `-listNotRegApp` options of `AcsRegCli.pl` script might some time show wrong list of registered and non registered applications.

To resolve the discrepancy, you can either:

- Register the individual application using the `AcsRegCli.pl` script.
- Or
- If you are sure that you do not have any custom roles defined for any applications in ACS, you can either register all applications from the GUI or register individual applications using the `AcsRegCli.pl` script.

See the Online help for more information on registering applications from the GUI or registering applications using the `AcsRegCli.pl` script.

---

## Support for MDF Package 1.4

Meta Data Framework (MDF) Package defines device types in a uniform way across CiscoWorks applications. MDF Package allows you to add new device types to the existing set of device types defined in Common Services 3.0.

The MDF Version 1.4 is a cumulative package that includes the new device types added after the Common Services 3.0 release.

**Note**

---

Addition of new device types through MDF Package does not guarantee the support for these device types in all the 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.

---

The MDF package version 1.4 contains the following new device type definitions and icons:

**Devices Supported:**

- Cisco CSS 11501 Content Services Switch (1.3.6.1.4.1.9.9.368.4.7)
- Cisco 1801 Integrated Services Router (1.3.6.1.4.1.9.1.638)
- Cisco 1802 Integrated Services Router (1.3.6.1.4.1.9.1.639)
- Cisco 857 Integrated Services Router (1.3.6.1.4.1.9.1.567)
- Cisco 877 Integrated Services Router (1.3.6.1.4.1.9.1.569)
- Cisco MWAM (1.3.6.1.4.1.9.1.621)
- Cisco Catalyst 6509 NEB (1.3.6.1.4.1.9.1.310)
- Cisco IDS 4210 Sensor (1.3.6.1.4.1.9.1.645)
- Cisco IDS 4215 Sensor (1.3.6.1.4.1.9.1.646)
- Cisco IDS 4235 Sensor (1.3.6.1.4.1.9.1.647)
- Cisco IDS 4240 Sensor (1.3.6.1.4.1.9.1.648)
- Cisco IDS 4250 Sensor (1.3.6.1.4.1.9.1.649)
- Cisco IDS 4250 XL Sensor (1.3.6.1.4.1.9.1.651)
- Cisco IDS 4255 Sensor (1.3.6.1.4.1.9.1.652)

- MeetingPlace Express (1.3.6.1.4.1.9.1.710)
- Cisco Works 1132 for Wireless LAN Solution Engine (1.3.6.1.4.1.9.1.712)

The device icons used in various device selector pages are updated and new icons are added for 'Security and VPN' device types. These icons will be refreshed on installing CS 3.0 SP2.

---

## Adding Peer Server Certificates

In CS 3.0, you can add peer server certificate only through a non-SSL port. However, in CS 3.0 SP2, you can add peer server certificate only through an SSL port. Owing to this you cannot add a certificate from a CS 3.0 SP1/SP2 server to a CS 3.0 server and vice versa.

This disables features such as Single Sign-On (SSO) and registration of applications from remote server in a multi server domain consisting of both CS 3.0 and CS 3.0 SP1/SP2 servers. Copying peer certificate is one of the pre-requisites for such features.

For more information, see [Managing Security in Multi-Server Mode](#) section in the *Configuring the Server* chapter of the *User Guide for CiscoWorks Common Services 3.0*. See also, [Multi-server Deployment, page 27](#)

To add peer CiscoWorks Server certificates in CS 3.0 SP1/SP2:

- 
- Step 1** In the CiscoWorks Homepage, select **Common Services > Server > Security > Peer Server Certificate Setup**.
- The Peer Server Certificate page appears with a list of certificates imported from other servers.
- Step 2** Click **Add**.
- Step 3** Enter the IP address/hostname of the peer CiscoWorks server in the corresponding fields.
- Step 4** Enter the port number of the peer CiscoWorks server. This must be an SSL port. By default this is 443.

- Step 5** Click **OK**.  
The peer CiscoWorks Server certificate will be displayed.
- Step 6** Click **Accept** to accept the certificate.  
Or  
Click **Cancel** to reject the certificate.
- 

## New Features and Enhancements in Device and Credential Repository

In CS 3.0 SP1/SP2, the Device and Credential Repository (DCR) has been modified to accommodate the following features:

- Support for HTTP related credentials/attributes
- Support for CNS Configuration Engine
- Support for CNS Managed devices

Also, DCR has been modified to support HTTP credentials/attributes while adding AUS Managed devices.

This section contains:

- [Adding HTTP Credentials/Attributes](#)
- [Adding AUS Managed Devices](#)
- [Adding CNS Configuration Engine](#)
- [Adding CNS Managed Devices](#)
- [Editing Devices](#)

### Adding HTTP Credentials/Attributes

You can add devices (to the device list), and their attributes and credentials to DCR.

The following HTTP credentials are added to the credentials list:

Credential/Attribute Name	Description
http_username	HTTP username
http_password	HTTP password
http_port	HTTP port
https_port	HTTPS port
http_mode	Current transfer mode (http or https)
cert_common_name	Common name attribute value in the server's certificate

To add HTTP Credentials/Attributes:

**Step 1** From the CiscoWorks Homepage select **Common Services > Device and Credentials > Device Management**.

The Device Management page appears.

The Device Management page helps you perform operations on Standard Devices, DSBU Clusters, DSBU Cluster Managed devices, Auto Update devices, and CNS Managed devices. You can perform operations on Auto Update Servers only from the Auto Update Server Management UI.

**Step 2** Click **Add**.

The Device Properties window appears.

In the Device Properties window, if you select any of the following management type, you are prompted to enter the values for the HTTP credentials/attributes.

- Standard
- Auto Update
- CNS Managed

## Adding Standard Devices

To add devices and credentials using Standard Management type:

- Step 1** Select **Standard** from the Select a Management Type drop-down list box.
- Step 2** Enter the Device IP address, the hostname, domain name.  
The display name you want for the device in reports or graphical displays in the corresponding fields.  
You can also select the domain name.
- Step 3** Select the device type by clicking **Select** and choosing from the list.
- Step 4** Click **Add to List**.  
The device is added to the Added Device List in the page.  
To remove a device from the Device List select the device and click **Remove from List**.  
Device and Credential Repository uses a device record to represent a DSBU Cluster.  
You can add a DSBU Cluster in the Standard Management option by selecting the Device Type field as Cisco Cluster Management Suite. If you add DSBU Clusters in this way, you can select the Cluster Management option for the field Cluster.  
You can add a Cisco CNS Configuration Engine in the Standard Management option by selecting the Device Type field as Cisco CNS Configuration Engine. The Cisco CNS Configuration Engine added here can be selected in the CNS Server field in the CNS Managed option.  
After a Cisco CNS Configuration Engine or DSBU Cluster is successfully added, it will appear under  
**Network Management > Other Network Management Products > Cisco CNS Configuration Engine/Cisco Cluster Management Suite**, in the device selector.
- Step 5** Click **Next**.  
The Standard Credentials page appears.
- Step 6** Enter the credentials in the Standard Credentials dialog box.  
You can add the following credentials:
- Primary Credentials (Username, Password, Enable Password)
  - SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)

- SNMPv3 Credentials (Username, Password, authentication Algorithm, Engine ID)
- Rx Boot Mode Credentials (Username, Password)

**Step 7** Click **Next**.

The HTTP Settings page appears.

**Step 8** Enter these credentials in the HTTP Settings dialog box.

- HTTP Username
- HTTP Password. Re-enter the HTTP password in the Verify field.
- HTTP Port
- HTTPS Port
- Certificate Common Name

Specify the current connection mode (HTTP or HTTPS) by selecting the appropriate radio button.

**Step 9** Click **Next**.

The User Defined Fields dialog box appears.

**Step 10** Enter your choices for user-defined fields and click **Finish**.

Device and Credential Repository allows you to define four attribute fields for a device, by default. These fields store additional user-defined data for a device.

You can change the attribute fields at

**Device and Credentials > Admin > User Defined Fields.**

---

## Adding AUS Managed Devices

The CiscoWorks Auto Update Server is a web-based interface for upgrading device configuration files and software images on firewalls that use the Auto Update feature.

The Auto Update Server managed device has its own attributes and credentials similar to the normal devices in Device and Credential Repository. In addition, it has the following attributes:

- **Device Identity:** This is the string value that uniquely identifies the device in the parent Auto Update Server.
- The DCR Device ID of the parent Auto Update Server record.

To add devices and credentials using Auto Update type:

- 
- Step 1** Select **Auto Update** from the Select a Management Type drop-down list box.
- Step 2** Enter the Display Name, Auto Update Device ID, Host Name, Domain Name, and IP address in the corresponding fields.
- To select Auto Update Server, Domain Name, and the Device Type, click **Select** and choose the server from the resulting popup window.
- The Display Name and Device-Identity are identities for Auto Update Server managed devices.
- Device and Credential Repository uses a device record to represent an Auto Update Server.
- You can add an Auto Update Server in the Auto Update Server Management page. If you add an Auto Update Server in this way, you can select this for the field, Auto Update Server.
- Step 3** Click **Add to List**.
- The device is added to the Added Device List in the window.
- To remove the device from the Device List select the device and click **Remove from List**.
- Step 4** Click **Next**.
- The Auto Update Server Credentials page appears.

**Step 5** Enter the credentials in the Standard Credentials dialog box.

You can add the following credentials:

- Primary Credentials (Username, Password, Enable Password)
- SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Username, Password, authentication Algorithm, Engine ID)
- Rx Boot Mode Credentials (Username, Password)

**Step 6** Click **Next**.

The HTTP Settings page appears.

**Step 7** Enter these credentials in the HTTP Settings dialog box.

- HTTP Username
- HTTP Password. Re-enter the HTTP password in the Verify field.
- HTTP Port
- HTTPS Port
- Certificate Common Name

**Step 8** Specify the current connection mode (HTTP or HTTPS) by selecting the appropriate radio button.

**Step 9** Click **Next**.

The Auto Update Server Credentials dialog box appears.

**Step 10** Enter username and password. You must re-enter the password in the Verify field.



---

**Note** These are the credentials to login to the Auto Update Server — not to access the managed device.

---

**Step 11** Click **Next**.

The User Defined Fields dialog box appears.

**Step 12** Enter your choices for the user-defined fields, and click **Finish**.

---

## Adding CNS Configuration Engine

The Cisco CNS Configuration Engine is a secure network product that supports the activation of customer-premises equipment based network services through centralized template-based configuration management.

The Cisco CNS Configuration Engine provides a scalable infrastructure to manage the large-scale deployment of Cisco devices.

To Add CNS Configuration Engine:

---

**Step 1** Select **Standard** from the Select a Management Type drop-down list box.

**Step 2** Select Device Type field as Cisco CNS Configuration Engine.

**Step 3** Enter the Device IP address, the hostname, domain name.

The display name you want for the device in reports or graphical displays in the corresponding fields.

You can also select the domain name.

**Step 4** Select the device type by clicking **Select** and choosing from the list.

**Step 5** Click **Add to List**.

The device is added to the Added Device List in the page.

To remove a device from the Device List select the device and click **Remove from List**.

You can add a Cisco CNS Configuration Engine in the Standard Management option by selecting the Device Type field as Cisco CNS Configuration Engine.

If you add a Cisco CNS Configuration Engine in this way, you can select these engines in the CNS Managed option, for the CNS Server field.

After a Cisco CNS Configuration Engine is successfully added, it appears under **Network Management > Other Network Management Products > Cisco CNS Configuration Engine**, in the device selector.

**Step 6** Click **Next**.

The Standard Credentials page appears.

**Step 7** Enter the credentials in the Standard Credentials dialog box.

You can add the following credentials:

- Primary Credentials (Username, Password, Enable Password)
- SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Username, Password, authentication Algorithm, Engine ID)
- Rx Boot Mode Credentials (Username, Password)

**Step 8** Click **Next**.

The HTTP Settings page appears.

**Step 9** Enter these credentials in the HTTP Settings dialog box.

- HTTP Username
- HTTP Password. Re-enter the HTTP password in the Verify field.
- HTTP Port
- HTTPS Port
- Certificate Common Name

**Step 10** Specify the current connection mode (HTTP or HTTPS) by selecting the appropriate radio button.

**Step 11** Click **Next**.

The User Defined Fields dialog box appears.

**Step 12** Enter your choices for user-defined fields and click **Finish**.

Device and Credential Repository allows you to define four attribute fields for a device.

These fields store additional user-defined data for a device. You can change the attribute fields at

**Device and Credentials > Admin > User Defined Fields.**

---

## Adding CNS Managed Devices

To add devices and credentials using CNS Managed type:

- 
- Step 1** Select **CNS Managed** from the Select a Management Type drop-down list box.
- Step 2** Enter the Device IP address, the hostname, and the domain name.
- The display name you want for the device in reports or graphical displays in the corresponding fields.
- You can also enter or select the domain name.
- Step 3** Select the CNS Server and the device type by clicking **Select** and choosing from the list.
- Step 4** Click **Add to List**.
- The device is added to the Added Device List in the page.
- To remove a device from the Device List select the device and click **Remove from List**.
- Step 5** Click **Next**.
- The CNS Managed Device Credentials page appears.
- Step 6** Enter the credentials in the Standard Credentials dialog box.
- You can add the following credentials:
- Primary Credentials (Username, Password, Enable Password)
  - SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
  - SNMPv3 Credentials (Username, Password, Authentication Algorithm, Engine ID)
  - Rx Boot Mode Credentials (Username, Password)
- Step 7** Click **Next**.
- The HTTP Settings page appears.

- Step 8** Enter these credentials in the HTTP Settings dialog box.
- HTTP Username
  - HTTP Password. Re-enter the password in the verify field.
  - HTTP Port
  - HTTPS Port
  - Certificate Common Name
- Step 9** Specify the current connection mode (HTTP or HTTPS) by selecting the appropriate radio button.
- Step 10** Click **Next**.
- Step 11** Enter your choices for user-defined fields and click **Finish**.
- Device and Credential Repository allows you to define four attribute fields for a device. These fields store additional user-defined data for a device.
- You can change the attribute fields at  
**Device and Credentials > Admin > User Defined Fields**.
- 

## Editing Devices

You can edit device information in the Device and Credential Repository using this feature.

---

- Step 1** From the CiscoWorks Homepage select **Common Services > Device and Credentials > Device Management**.
- The Device Management window appears.
- Step 2** Select one or more devices from the Device Summary List, and click **Edit**.
- The Device Properties dialog box appears.
- You can edit the attributes of individual devices here. The Devices column lists all selected devices. From the Devices column, you should individually select each device that you want to edit.
- Step 3** Select the device from the device list.
- The current attributes are automatically populated in the device information fields.

**Step 4** Edit the device information you want to, in the respective fields.

**Step 5** Click **Next** if you want to edit device credentials.

The Standard Credentials dialog box appears. According to your requirements, you can edit:

- Primary Credentials (Username, Password, Enable Password)
- SNMP v2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Username, Password, Authentication Algorithm, Engine ID)
- Rx Boot Mode Credentials (Username, Password)
- Auto Update Server Managed Device credentials (Username, Password)

Any changes made here will apply to all devices selected in Step 2. This has one exception.

If in Step 2, devices belonging to different device management types are selected, the changes made will apply only to devices of the appropriate type. That is, if a standard-device credential is changed, only the standard devices selected in Step 2 are affected.

**Step 6** Select **Finish** if you have completed editing and do not want to proceed.

Or

Click **Next** if you want to edit HTTP Settings.

You can edit:

- HTTP Username
- HTTP Password. Re-enter the password in the verify field.
- HTTP Port
- HTTPS Port
- Certificate Common Name
- Current Connection Mode.

**Step 7** Click **Finish** after editing

Or

Click **Next** if you want to edit User Defined Fields.

The User Defined Fields window appears. You can edit these fields and click **Finish** after you complete editing.

---

## New Features in Software Center

In CS 3.0, the Cisco.com and Proxy credentials have to be entered at **Server > Admin > Cisco.com User Account Setup** and **Server > Admin > Security > Proxy Server Setup**, respectively.

In CS 3.0 SP2 you have to enter your Cisco.com account credentials to perform the following tasks, through Software Center:

- [Selecting Software Updates From Software Center](#)
- [Downloading Software Updates From Software Center](#)
- [Checking for Device Updates in Software Center](#)
- [Scheduling Device Package Downloads](#)
- [Using PSU CLI for Downloading Software Updates and Device Updates](#)

If you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**, you must enter the Proxy server username and password, while performing these tasks.

## Selecting Software Updates From Software Center

The Software Updates link under Software Center takes you to the Software Updates page.

Enter your Cisco.com username and password to connect to Cisco.com, for software updates. If you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**, you must enter the Proxy server username and password.

To select Updates from Software Center:

- 
- Step 1** From the CiscoWorks Homepage, select **Common Services > Software Center > Software Updates**.  
The Software Updates page appears.
- Step 2** In the Products Installed dialog box, select the check box corresponding to the product for which you want to select update.
- Step 3** Click **Select Updates**.  
The CCO and Proxy Server Credentials dialog box appears.
- Step 4** Enter your Cisco.com username and password. Both are mandatory.  
Both are mandatory if you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**.
- Step 5** Select the product you need to update and click **Next**.
- Step 6** Select a destination location or browse to the location and click **Next**.  
The destination location should not be the location where CiscoWorks is installed. Software Center does not support installing device or software updates in the same directory where you have installed CiscoWorks Common Services or any of its sub- directories.  
The Download Summary page appears.
- Step 7** Click **Next**.  
After the download is complete, a result page appears informing you whether the download was successful or not.
- Step 8** Click **Finish** to confirm installation of the selected packages.  
If you do not want to add the selected packages, click **Back** to reselect packages or click **Cancel** to exit.
-

## Downloading Software Updates From Software Center

You can download the selected updates from Software Center.

Enter your Cisco.com username and password to connect to CCO, for software updates.

If you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**, you must enter the Proxy server username and password.

To download updates from Software Center:

- 
- Step 1** From the CiscoWorks Homepage, 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 the product for which you want to download the update.
- Step 3** Click **Download Updates**.
- The CCO and Proxy Server Credentials dialog box appears.
- Step 4** Enter your Cisco.com username and password. Both are mandatory.
- Both are mandatory if you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**.
- Step 5** Select the product you need to update and click **Next**.
- Step 6** Select a destination location or browse to the location and click **Next**.
- The destination location should not be the location where CiscoWorks is installed. Software Center does not support downloading device or software updates in the same directory where you have installed CiscoWorks Common Services, or any of its sub- directories.
- The Summary page appears. This page a summary of your inputs.

**Step 7** Click **Finish** to confirm the download operation.

If you do not want to download the listed packages, click **Back** to reselect packages or click **Cancel** to exit.

If you click **Cancel**, the Software Update page appears.

---

## Checking for Device Updates in Software Center

You can check for device updates using this option.

Enter your Cisco.com username and password to connect to Cisco.com, for software updates.

If you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**, you must enter the Proxy server username and password.

To check for the updates:

---

**Step 1** From the CiscoWorks Homepage, select **Common Services > Software Center > Device Update**.

The Device Updates page appears.

**Step 2** Select the check box corresponding to the product for which you want to check for updates and click **Check for Updates**.

The Source Location page appears. You can check for updates at Cisco.com or a server.

- To check for updates at Cisco.com, select the Cisco.com radio button.
- To check for updates from a server, select the Enter Server Path radio button and enter the path or browse to the location using the Browse tab.

**Step 3** Click **Next**.

The CCO and Proxy Server Credentials dialog box appears.

**Step 4** 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**.

**Step 5** Click **Next**.

The Available Packages and Installed Packages page appears. It displays:

- Package Name: Name of the package.
- Type: Type of the update. For example, whether the update is a device package or IDU package.
- Product Name: Product for which the update is available.
- Installed Version: Current version of that product installed in the server.
- Available version: Version of the product that is available (Other than the installed version).
- Readme Details: Links to the Readme files associated with the update.
- Posted date: Date on which the update was posted on Cisco.com.
- Size: Size of the update.

**Step 6** Select the check box corresponding to the package that you wish to update and click **Next**.

The Device Update page appears. You can either install the device packages or download them.

- To install device packages, select the Install Device Packages radio button.
- To download device packages, select the Download Device Packages radio button.

If you select Download Device Packages:

- a. Enter the folder in File Selection field or click **Browse** to select the folder.
- b. Set the frequency of downloads, select the run type from the Run Type drop-down list. The options are:
  - Immediate
  - Once
  - Daily

- Weekly
- Monthly

If you choose any of the options other than Immediate, set the date and time.

- Select the date from the date picker.
- Specify the time from the drop-down lists.
- c. In the Job Description field, enter a description for the download job. This is mandatory.
- d. Enter the Email ID in the E-mail field.
- e. Click **Next**.

The Summary window displays the details.

- f. Click **OK** to confirm.

If you select Install Device Packages:

- Click **Next**.

A summary of your inputs appears.

- Click **OK** to confirm.

A message that the daemons are restarted, appears.

**Step 7** Click **OK** to continue with installation.

---

## Scheduling Device Package Downloads

You can schedule device package downloads and specify the time, frequency of the downloads.

If you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**, you must enter the Proxy server username and password.

To schedule device package downloads:

---

**Step 1** Select **Common Services > Software Center > Schedule Device Downloads**.

The Schedule Device Downloads dialog box appears.

**Step 2** Enter your Cisco.com username and password.

Enter the Proxy server username and password only if you have configured proxy settings under **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**.

**Step 3** Click **Next**.

**Step 4** Enter the destination location, or browse to the location using the Browse tab.

**Step 5** Specify the download policy you require.

- To set the frequency of downloads, select the run type from the Run Type drop-down list.
- To set the date and time, select the date from the drop-down calendar, and specify the time using the drop-down lists.

**Step 6** In the Job Description field, enter a description for the download job. This is mandatory.

**Step 7** Enter the E-mail ID in the E-mail field.

**Step 8** Click **Accept** in the confirmation popup dialog box.

Or

Click **Cancel** to exit without making changes.



---

**Note** You can schedule only one download at a time.

---

# Using PSU CLI for Downloading Software Updates and Device Updates

You can use the command line feature to download software updates and device updates.

The following sections provide details on using the PSU CLI to download software updates and device updates:

- [Downloading Software Updates \(-s option\)](#)
- [Downloading Device Updates \(-d option\)](#)

## Downloading Software Updates (-s option)

Use the `-s` option for downloading the Software Updates.

To download the Software Updates:

Enter `NMSROOT/bin/PSUcli.sh -p product -s -dst download directory`

*product*—Specify the Product for which you want to download the Software Update. Invoking CLI with `-h` option lists the valid product names.

*download directory*—Specify the directory to which you want to download the Software Update. Do not specify the same directory where you have installed CiscoWorks Common Services, or any of the sub directories in it.

You will be prompted to enter Cisco.com Username and Password. If you have configured Proxy settings, you will be prompted for Proxy Server User credentials.

## Downloading Device Updates (-d option)

Use the `-d` option for downloading the Device Updates.

To download the Device Updates:

Enter `NMSROOT/bin/PSUcli.sh -p product -d -dst download directory`

*product*—Specify the Product for which you want to download the Device Update. Invoking CLI with `-h` option lists the valid product names.

*download directory*—Specify the directory to which you want to download the Device Update. Do not specify the same directory where you have installed CiscoWorks Common Services, or any of the sub directories in it.

You will be prompted to enter Cisco.com Username and Password. If you have configured Proxy settings, you will be prompted for Proxy Server User credentials.

---