



# Readme Document for Common Services 3.0 Service Pack 1

---

This Readme document is about Common Services 3.0 Service Pack 1 (CS 3.0 SP1) and contains the following sections:

- [Description, page 2](#)
- [New Features in CS 3.0 SP1, page 3](#)
- [Resolved Problems in CS 3.0 SP1, page 4](#)
- [Hardware and Software Requirements, page 10](#)
- [Browser Support, page 11](#)
- [Downloading CS 3.0 SP1, page 11](#)
- [Installing CS 3.0 SP1, page 14](#)
- [Uninstalling CS 3.0 SP1, page 20](#)
- [General Guidelines for Using CS 3.0 SP1, page 22](#)
- [Documentation Addendum, page 23](#)



---

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

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



**Note**

---

CS 3.0 SP1 has been obsoleted by CS 3.0 SP2. CS 3.0 SP1 is no longer available for download from Cisco.com. We recommend you download and install CS 3.0 SP2.

---



**Caution**

---

Caution: You must not install CS 3.0 SP1 on a server that has CS 3.0 SP2 installed. This will cause system instability.

---

## 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 1 (CS 3.0 SP1) is the first incremental release over Common Services 3.0 (CS 3.0).

# New Features in CS 3.0 SP1

The following are the new features and enhancements in CS 3.0 SP1:

- 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 Java Plug-In 1.4.2\_06
- Support for Cisco Secure ACS 3.3.2
- Support for Meta Data Framework (MDF) package 1.2
- New options as part of command line arguments to cwjava
- Uninstallation of CS 3.0 Service Packs

# Resolved Problems in CS 3.0 SP1

Table 1 lists the problems in CS 3.0 that are resolved in CS 3.0 SP1.

**Table 1** Resolved Problems in CS 3.0 SP1

Bug ID	Description	Explanation
<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 cannot 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> <pre>ProxyServer port must be a number in range 1024- 65535.</pre> <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> <p>See more details in the following Field Notice:</p> <p><a href="https://www.cisco.com/en/US/ts/fn/620/fn62146.html">https://www.cisco.com/en/US/ts/fn/620/fn62146.html</a></p>
<b>DCR Related Resolved Problems</b>		

**Table 1** Resolved Problems in CS 3.0 SP1 (Continued)

Bug ID	Description	Explanation
CSCsa16158	Auto Update Server (AUS) device addition was missing 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 contacts the AUS device directly and needs 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>
CSCsa23143	Support for CNS Configuration Engine and CNS Devices.	<p>In CS 3.0 SP1, DCR supports management of CNS Configuration Engine (CNS Server) and CNS Devices (devices managed by CNS Server).</p>
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>

**Software Center Related Resolved Problems**

**Table 1** Resolved Problems in CS 3.0 SP1 (Continued)

Bug ID	Description	Explanation
CSCsa52966	Need to prompt for Cisco.com and Proxy credentials when performing software downloads.	In CS 3.0, when a user sets up Cisco.com credentials at Server > Security > CCO setup, all other users can use this user's Cisco.com account to download software.  In CS 3.0 SP1, each time the user attempts device updates or software updates from Cisco.com, the user is prompted for Cisco.com credentials.  Proxy credentials are also prompted for, if the proxy server is configured at Server > Security > Proxy Setup.
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 fixed 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.

**Table 1** Resolved Problems in CS 3.0 SP1 (Continued)

Bug ID	Description	Explanation
CSCsa42779	Minor issues while receiving jms messages.	<p>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.</p> <p>This occurred because when the publisher published the event, it had to create a corresponding mailbox.</p> <p>In CS 3.0 SP1, a mailbox is added while publishing events.</p>
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 fix this problem.</p>
<b>Install Related Resolved Problems</b>		

**Table 1** Resolved Problems in CS 3.0 SP1 (Continued)

Bug ID	Description	Explanation
CSCsa63439	CS Service Packs did not support uninstallation.	CS 3.0 SP1 supports uninstallation of CS Service Packs.
CSCsa51358	CS SPs must not be allowed to install over IP-Telephony Environment Monitor (ITEM) ( <b>only on Windows</b> ).	Installing CS SPs created version conflicts when installing ITEM SPs. CS 3.0 SP1 provides a mechanism to disallow installation of CS SPs over ITEM.
CSCsa57174	Changes in License Agreement Panel ( <b>only on Windows</b> ).	While installing CS 3.0 on Windows, the software license agreement text displayed <code>Click ACCEPT Button</code> . However the button was marked <b>Yes</b> . In CS 3.0 SP1, <b>Yes</b> is changed to <b>Accept</b> and <b>No</b> to <b>Do not Accept</b> .

**Backup and Restore Related Resolved Problems**

CSCsa12929	PERL applications in CiscoWorks that required <code>fork()</code> emulation or large file support did not work.	PERL that is shipped with CiscoWorks (5.00502) did not support large files on Solaris or Windows. The <b>stat</b> function returned either 0 or a negative number when it encountered files greater than 2 GB. In CS 3.0 SP1, large files are supported by a helper utility, <code>logrot_stat</code> located at <code>NMSROOT\bin</code> .
CSCsa66745	Issues while restoring backup data on some Windows systems.	While restoring backup data on few Windows machines, the system called from PERL did not release the directory immediately after system call was done. Hence the attempt to rename the directory failed. The problem has been fixed in CS 3.0 SP1 by providing a mechanism to attempt renaming the directory until the directory is locked.

**Security Related Resolved Problems**

**Table 1** Resolved Problems in CS 3.0 SP1 (Continued)

Bug ID	Description	Explanation
CSCsa50470	Authorization error in DBReader when logged into any Common Services server with Fully Qualified Domain Name (FQDN).	The error has been corrected in CS 3.0 SP1 to solve this problem.
<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 tomcat/shared directory.</p> <p>CS 3.0 SP1 supports JDOM 1.0, that is the first official release of JDOM.</p>
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>

**Table 1** Resolved Problems in CS 3.0 SP1 (Continued)

Bug ID	Description	Explanation
CSCsa45555	Needed to upgrade Java Plug-in version. This was caused by a security vulnerability in the implementation of JRE in the Java Plug-in (JPI 1.4.2_04), shipped by CiscoWorks.	In CS 3.0 SP1, the Java Plug-in is upgraded from 1.4.2_04 to 1.4.2_06.
CSCsa52301	Discovery went into an infinite loop when Multiplexing and Multiple community were enabled.	When Multiplexing and Multiple community were enabled, the master request as well as the individual requests tried multiple community entries.  In CS 3.0 SP1, SNMP checks whether the request has an associated master request. If so, it times-out individual requests.

## Hardware and Software Requirements

CiscoWorks Common Services 3.0 must be installed on your system.

Hardware and software requirements for CS 3.0 SP1 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](#)
- [Installation and Setup Guide for CiscoWorks Common Services 3.0 \(Includes CiscoView\) on Windows](#)

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

## On Windows:

- Microsoft Internet Explorer 6.0.26 and Microsoft Internet Explorer 6.0.28.
- Netscape Navigator 7.1.
- Mozilla 1.7.

## On Solaris:

- 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 SP1

You can download CS 3.0 SP1 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 SP1 is available on Cisco.com.

To download CS 3.0 SP1:

- 
- 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 following files:
    - cwcs\_3\_0\_sp1\_sol.zip (For Solaris)

- cwcs\_3\_0\_sp1\_win.zip (For Windows)

**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 SP1.

To download CS 3.0 SP1 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 SP1 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.




---

**Note** 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.

---

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




---

**Note** The destination location must have casuser write-permissions.

---

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

The Summary page appears. The Summary window shows a summary of your inputs.

**Step 6** Click **Finish** to confirm the download operation.

---

To download CS 3.0 SP1 using the Software 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 either:

- **cwcs\_3\_0\_sp1\_sol.zip (For Solaris)**
- Or
- **cwcs\_3\_0\_sp1\_win.zip (For Windows)**

**Step 4** Click **Next**.

The Destination Location page appears. The destination location should not be the location where CiscoWorks is installed.




---

**Note** 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.

---

**Step 5** Enter the location, or browse to the location using the Browse tab.




---

**Note** The destination location must have casuser write-permissions.

---

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

The Summary page appears. The Summary window shows a summary of your inputs.

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

---

## Installing CS 3.0 SP1

This section provides information on installing CS 3.0 SP1 on Windows and Solaris platforms.

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




---

**Note** If you install CS3.0 SP1 when AAA mode is set to ACS, all the custom roles you have created will be lost. This happens only with Cisco Secure ACS version 3.3.x. To preserve the custom roles you have created, you must ensure that the AAA mode is set to CiscoWorks Local before you install CS3.0 SP1. You will be prompted to continue installation after changing the AAA mode. While changing to ACS mode after installation, ensure that you have not selected the **Register all installed applications with ACS** checkbox.

---

## Installing CS 3.0 SP1 on Solaris

To install CS 3.0 SP1 on a Solaris platform:

---

**Step 1** Unzip the `cwcs_3_0_sp1_sol.zip` file by entering:

```
unzip cwcs_3_0_sp1_sol.zip
```

**Step 2** Verify the integrity of the image by entering:

```
sh checkPkgIntegrity.sh
```

- If there are no errors, go to Step 3.
- If there are errors, contact the Technical Assistance Center (TAC). TAC will guide you how to proceed installing the Service Pack.

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

```
./setup.sh
```

- If you have set the AAA mode to ACS, the following message appears:

```
The AAA mode of this CiscoWorks server is currently set to ACS mode.
```

```
If you proceed with the installation without changing the AAA mode to CiscoWorks Local, all the custom roles you have created will be lost.
```

```
To change the AAA mode, run
NMSROOT/bin/perl NMSROOT/bin/ResetLoginModule.pl
```

```
If you change the AAA mode to CiscoWorks Local, make sure that you revert the AAA mode to ACS, after completing the installation.
```

```
To continue with the installation without changing the AAA mode, enter y.
```

```
To abort the installation, enter n.
```

- Enter **y** to continue installation without changing the AAA mode.

If you continue installation without changing the AAA mode, all the custom roles you have created will be lost. This happens only with Cisco Secure ACS version 3.3.x.

If you want to preserve the custom roles you have created, you must set the AAA mode to CiscoWorks Local. For this you must stop the installation and reset the login module before you continue the installation.

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

If you enter **n** and stop the installation, run the following script to reset the login module:

```
NMSROOT/bin/perl NMSROOT/bin/ResetLoginModule.pl
```

You can change the login mode to ACS after the installation. While changing to ACS mode, ensure that you have not selected the **Register all installed applications with ACS** checkbox.

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 modifies the casuser privileges. The following message appears:

```
INFO: Checking user entry casuser.....
```

```
WARNING: User casuser already exists. The installation process will  
overwrite its privileges
```

```
Do you want to continue ? ? (y/n) [y]:
```

**Step 6** Enter **y** to continue installation.

The following message appears:

```
INFO: User attributes are updated.
```

```
INFO: casuser has no shell.
```

The installation program installs CS 3.0 SP1 in the same directory where you have installed CS 3.0.

---

## Installing CS 3.0 SP1 on Windows

To install CS 3.0 SP1 on a Windows platform:

**Step 1** Unzip the `cwcs_3_0_sp1_win.zip` file.

**Step 2** Double-click **`cw-common-services-3.0-sp1-win.exe`** file.

A dialog box appears with the following message:

Do you really want to install CiscoWorks Common Services 3.0 SP1

**Step 3** Click **Yes** to continue installation.

- If you have set the AAA mode to ACS, a dialog box appears with the following message:

The AAA mode of this CiscoWorks server is currently set to ACS mode.

If you proceed with the installation without changing the AAA mode to CiscoWorks Local, all the custom roles you have created will be lost.

To change the AAA mode, run  
`NMSROOT\bin\perl NMSROOT\bin\ResetLoginModule.pl`.

If you change the AAA mode to CiscoWorks Local, make sure that you revert the AAA mode to ACS, after completing the installation.

To continue with the installation, without changing the AAA mode, click **Yes**.

To abort the installation, click **No**.

- Click **Yes** to continue installation without changing the AAA mode.

If you continue installation without changing the AAA mode, all the custom roles you have created will be lost. This happens only with Cisco Secure ACS version 3.3.x.

If you want to preserve the custom roles you have created, you must set the AAA mode to CiscoWorks Local. For this you must stop the installation and reset the login module before you continue the installation.

- Click **No** to stop the installation.

If you click **No** and stop the installation, run the following script to reset the login module:

```
NMSROOT\bin\perl NMSROOT\bin\ResetLoginModule.pl
```

You can change the login mode to ACS after the installation. While changing to ACS mode, ensure that you have not selected the **Register all installed applications with ACS** checkbox.

The Welcome screen appears.

**Step 4** Click **Next** to continue.

The Software License Agreement dialog box appears.

**Step 5** Click **Accept** to accept the license agreement and proceed with the installation.

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

The installation program checks the system configuration and required space.

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

The installation program verifies the settings.

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

The installation program installs CS 3.0 SP1 in the same directory where you have installed CS 3.0.

**Step 9** Click **Finish** to complete the installation.

---

# Uninstalling CS 3.0 SP1

This section provides information on uninstalling CS 3.0 SP1 on Windows and Solaris platforms.

You can uninstall CS 3.0 SP1 alone. The installation program backs up the files that will be modified and deleted during the installation of SP1. The backup is done during SP1 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.

## Uninstalling CS 3.0 SP1 on Solaris

To uninstall CS 3.0 SP1 on Solaris:

---

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

```
cd /opt/CSCOpX/bin
```

**Step 2** Enter:

```
/opt/CSCOpX/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:

```
INFO: CS Service Pack Uninstall Completed!!!!!!!
```

Check the ciscouninstall.log for possible messages during uninstallation.

---

## Uninstalling CS 3.0 SP1 on Windows

To uninstall CS 3.0 SP1 on Windows:

---

**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 %System
Drive%\Ciscoworks_setupxxx.log
```

The uninstallation completes and the following message appears:

```
INFO: CS Service Pack Uninstall Completed!!!!!!
```

Check the Ciscoworks\_setupxxx.log for possible messages during uninstallation

---

### Notes on Uninstallation

- You cannot uninstall CS 3.0 SP1 if any of your CiscoWorks applications depends on CS 3.0 SP1.
- The uninstallation script for CS 3.0 SP1 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 SP1 will be reverted. However, any configuration change **done after the installation** of CS 3.0 SP1 will be retained.

- Uninstallation of CS 3.0 SP1 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 as a normal CS 3.0 server after uninstalling CS 3.0 SP1.
- The Metadata Framework (MDF) package version 1.2 that is installed as part of CS 3.0 SP1 will not be uninstalled.

## General Guidelines for Using CS 3.0 SP1

This section describes the general guidelines related to the following tasks, while using CS 3.0 SP1:

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

You must not restore the data backed up from a CS 3.0 SP1 server, on a server that has CS 3.0 installed. The database changes in CS 3.0 SP1, 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 SP1.

CS 3.0 SP1 does not support a DCR Master-Slave setup with a mix of CS 3.0 and CS 3.0 SP1 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 server and import them into a CS 3.0 SP1 server. You can also export devices and credentials from a CS 3.0 SP1 server and import them into another CS 3.0 SP1 server.

You must not import devices and credentials from a CS 3.0 SP1 sever into a CS 3.0 server. The changes in CS 3.0 SP1, 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 SP1. This section contains:

- [Adding Peer Server Certificates](#)
- [New Features and Enhancements in Device and Credential Repository](#)
- [New Features in Software Center](#)
- [Support for MDF Package 1.2](#)

## Adding Peer Server Certificates

In CS 3.0, you can add peer server certificate only through a non-SSL port. But, in CS 3.0 SP1, 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 server to CS 3.0 server and vice versa.

This disables features like 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 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 22](#)

To add peer CiscoWorks Server certificates in CS 3.0 SP1:

- 
- 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 SP 1, 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 and 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.




---

**Note** 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 the 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**.



---

**Note** 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

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

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

The Auto Update Server Credentials dialog box appears.

**Step 9** 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 10** Click **Next**.

The User Defined Fields dialog box appears.

**Step 11** 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 and 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.



---

**Note** 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

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

**Step 10** Click **Next**.

The User Defined Fields dialog box appears.

**Step 11** Enter your choices for user-defined fields and click **Finish**.

**Note**

---

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, domain name and 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**.



---

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

**Step 4** 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.

If you have completed editing and do not want to proceed, click **Finish**.

**Step 5** 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 6** 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 provided at **Server > Admin > Cisco.com User Account Setup** and **Server > Admin > Security > Proxy Server Setup**, respectively.

In CS 3.0 SP1 you have to provide 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**.



---

**Note** 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.

---

The Download Summary window 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**.



**Note** 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 have to 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 Software Updates.

### On Windows

Enter `NMSROOT\bin\PSUcli.bat -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. You should 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 User Name and Password. If you have configured Proxy settings, you will be prompted for Proxy Server User credentials.

### On Solaris

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. You should 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.

### On Windows

Enter `NMSROOT\bin\PSUcli.bat -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. You should 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 User Name and Password. If you have configured Proxy settings, you will be prompted for Proxy Server User credentials.

### On Solaris

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. You should 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.

## Support for MDF Package 1.2

Meta Data Framework (MDF) is used to define device types in a uniform way that can be used across all applications of CiscoWorks.

The MDF package version 1.2 contains the new device type definitions added after Common Services 3.0.

You can download MDF package either from Cisco.com or through the Software Center in CiscoWorks Common Services 3.0.

For more information on MDF package see the Readme for MDF package at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-cd-one>