



# Release Note for the Cisco Internet CDN Software Version 2.1

---

November 19, 2001



---

The most current documentation for this product is available on Cisco.com at <http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/cdnsp/index.htm>. The online documents may contain updates and modifications after the hardcopy documents were printed.

---

## Contents

This release note contains information about the Cisco Internet Content Delivery Network (CDN) Software version 2.1. It describes the following topics:

- [Introduction](#)
- [System Requirements](#)
- [Updating to a New Software Version](#)
- [Important Notes for Service Providers](#)
- [Important Notes for Content Providers](#)
- [Copyright Notices and Licenses](#)
- [Open Caveats](#)
- [Resolved Caveats](#)
- [Documentation Corrections](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)



---

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

Copyright © 2001. Cisco Systems, Inc. All rights reserved.

78-13558-01

# Introduction

The following features have been added to the Cisco Internet CDN Software version 2.1 since the release of Version 2.0:

- Support for streaming Windows Media files.
- HTTP redirect routing based on the client's source IP address. Both Domain Name System (DNS)-based routing and source IP address-based routing can be configured on a single CDN at one time.
- Content Services Switch and supernode improvements.
- Multiple levels of user access through the user interface, each with a single login account.
- Support for two Content Distribution Managers in separate locations using a replicated, distributed Oracle database.
- Routing visibility tools and new configuration options.
- Enhanced security through user interface timeouts and secure log transfer.
- Authentication of HTTP and WMT content.
- Removal of the requirement for cdn-tags in pre-positioned and live content URLs.
- Support for a CDN that comprises of devices using mixed versions of the Cisco Internet CDN Software.

## System Requirements

This section describes the devices and third-party applications that are supported on an Internet CDN, the media servers that are native to these devices, and the software and servers that are required for you to set up and manage an Internet CDN.

- [Cisco-Supported Hardware](#)
- [Software Compatibility](#)
- [Workstations that Access the Web-Based Interface](#)
- [Database Management System](#)
- [Domain Name System](#)
- [RealServer, Darwin Streaming Server, and WMT Server](#)
- [File Transfer Protocol Server](#)
- [SNMP Manager](#)

## Cisco-Supported Hardware

The Cisco Internet CDN Software Version 2.1 operates with the following Cisco hardware:

- Content Distribution Manager 4670 ICDN (model number CDM-4670-ICDN-K9)
- Content Router 4450 ICDN (model number CR-4450-ICDN-K9)
- AC and DC versions of the Content Engine 500 ICDN Series (model numbers CE-590-ICDN-K9 and CE-590-DC-ICDN-K9, respectively)

- AC and DC versions of the Content Engine 7320 ICDN Series (model numbers CE-7320-ICDN-K9 and CE-7320-DC-ICDN-K9, respectively)
- Content Services Switch 1115x and 1180x
- Cisco Catalyst switches (optional)
- AC and DC versions of the Storage Array 6 (model numbers SA6-SHF-6Disk-AC and SA6-SHF-6Disk-DC, respectively) for use with the Content Engine 590
- Storage Array 12 (model number SA12-SHF-12Disk-AC) for use with the Content Engine 7320

Refer to the Cisco documentation that came with each device for detailed, device-specific instructions on handling, installing, and configuring your Cisco CDN hardware.

## Software Compatibility

For version 2.1, the following upgrade sequences for the Cisco Internet CDN Software are supported:

- Version 2.0.2 → Version 2.1
- Version 2.0.1 → Version 2.1
- Version 2.0 → Version 2.1
- Version 1.0.2 → Version 2.0.1 → Version 2.1
- Version 1.0.1 → Version 2.0.1 → Version 2.1
- Version 1.0 → Version 1.0.2 → Version 2.0.1 → Version 2.1

The following downgrade sequences are supported:

- Version 2.1 → 2.0.1
- Version 2.0.2 → Version 2.0.1

## Workstations that Access the Web-Based Interface

You interact with the Cisco Internet CDN Software using the web-based graphical user interface that is installed on the Content Distribution Manager. The following minimum hardware and software requirements apply to each machine that is used as a workstation for accessing the graphical user interface.

### Network

- Ethernet connection
- Connection to the Internet

### Platform and Operating System

- Windows 95/98 Pentium-class system, 266 MHz, 64 MB of RAM
- Windows NT/2000 Pentium-class system, 266 MHz, 64 MB of RAM

### Software

- Microsoft Internet Explorer 4.x/5.0 (or later)
- Netscape 4.7 (or later)

## Database Management System

The Cisco Internet CDN Software requires that the Oracle 8i database management system (DBMS) be installed on your host network. The Cisco Internet CDN Content Distribution Manager uses an Oracle database for persistent storage of system information and statistics.

The Cisco Internet CDN *does not* require a dedicated Oracle database. If you already have an Oracle database in use within your organization, that database can also be used with your Internet CDN.

If you have not already done so, you must purchase Oracle 8i from Oracle. The DBMS requirement is Oracle 8i Version 8.1.6 or later.

For information about setting up the Oracle 8i database, refer to the Oracle documentation, and the *Cisco Internet CDN Software Configuration Guide* for version 2.1, Chapter 2, in the section “Setting Up the Oracle 8i DBMS”.

## Domain Name System

The Cisco Internet CDN Software Version 2.1 uses the Domain Name System (DNS) to route requests to Content Engines. To serve content in your CDN, you must configure DNS. For information on how to do this, see the *Cisco Internet CDN Software Configuration Guide* for version 2.1, Chapter 2, in the section “Configuring DNS.”

## RealServer, Darwin Streaming Server, and WMT Server

Content Engines that serve QuickTime media files using the Apple Computer Darwin Streaming Server, RealNetworks RealMedia files, or Windows Media files require that the server software be installed. Cisco Internet CDN Version 2.1 Content Engines ship with the Darwin Streaming Server, the RealNetworks RealServer, and the Starbak Windows Media Technologies (WMT) Server already installed.

If you wish to distribute RealMedia content over your CDN, you must also purchase a server license from RealNetworks in order to use the RealServer feature.

If you intend to serve live content using RealServer on the Cisco Internet CDN Software Version 2.1, you must upgrade the RealServer software on your origin server to RealServer Version 8.0 if you have not already done so.

If you wish to distribute WMT content over your CDN, you must purchase a WMT server license from Cisco Systems for each Content Engine that will be serving WMT content.

## File Transfer Protocol Server

You need a File Transfer Protocol (FTP) server configured to receive ACTIVE-mode transmissions if you want to enable remote logging. For information, refer to the Cisco Internet CDN Software online help or the *Cisco Internet CDN Software User Guide* for version 2.1.

## SNMP Manager

You need a Simple Network Management Protocol (SNMP) manager if you want to monitor system statistics using SNMP. For information about creating and registering an SNMP manager with your CDN, refer to the *Cisco Internet CDN Software User Guide* for version 2.1, Chapter 4, in the section “Maintaining the Cisco Internet CDN Software.”

The Cisco Internet CDN Software Version 2.1 implements the HOST-RESOURCES MIB (IETF standard RFC 2790) and the CISCO-CONTENT-NETWORK-MIB. The CISCO-CONTENT-NETWORK-MIB monitors statistics related to the operation of the CDN. You can find the definition of the CISCO-CONTENT-NETWORK-MIB at <ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CONTENT-NETWORK-MIB.my>. For information on traps and variables in this MIB, refer to the *Cisco Internet CDN Software User Guide* for version 2.1.

## Updating to a New Software Version

Review this entire section before beginning a software upgrade. It is important to have a clear view of the entire upgrade process before beginning.

To update your Internet CDN Software, you must follow this three-step procedure:

- Step 1—Determine the Current Software Version
- Step 2—Download the software update file
- Step 3—Update the software on your Internet CDN devices

In order to access and download your Cisco Internet CDN Software update, you need a registered username and password. If you are a Cisco customer and service contract owner, a Cisco reseller, Premier Certified Partner, the customer of a Cisco certified Partner Initiated Customer Access (PICA) partner, or a Cisco consultant, you can acquire a login directly from the Cisco.com website.

If you have questions or concerns about the upgrade, contact your designated Cisco Internet CDN Technical Support representative.

### Step 1—Determine the Current Software Version

To determine the version of the Cisco Internet CDN Software that you are using:

- 
- Step 1** In your web browser, enter the secure IP address or DNS name of the Content Distribution Manager (CDM). For example:
- ```
https://10.89.100.111
```
- Step 2** Log in to the CDM using the administrator username and password.
- Step 3** From the Cisco Internet CDN Software Version 2.1 user interface, click **Tools**.
- Step 4** From the System Tools drop-down list, choose **Software Update**.
- Step 5** For each component (CDM, Content Engine, and Content Router), refer to the Version column. The current version of the software installed on that device is displayed.
-

## Step 2—Download the Software Update File

You can download the software update file from either the Cisco.com website or the Cisco FTP server.

### Download from the Cisco.com Website

To connect to the Cisco.com website:

---

**Step 1** Launch your web browser and point it to the following URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/cdn-sp`

You are prompted to log in. Enter your Cisco.com username and password.



---

**Note** You need to have a Cisco.com username and password before attempting to download a software update from Cisco.com. In order to acquire a Cisco.com login, you need a service contract number, Cisco.com registration number and verification key, PICA registration number and verification key, or packaged service registration number.

---

**Step 2** Enter your Cisco.com username and password into the fields provided and click **OK**. The Cisco Internet CDN Software screen appears, listing the Internet CDN Software upgrades available for download.

**Step 3** Locate the update file for the version of the Cisco Internet CDN Software that you need. Version numbers are listed in the column labeled Release. Determine which version you need by referring to the [“Software Compatibility” section on page 3](#). Depending on the version that you currently have, you may have to go through more than one upgrade to get to version 2.1.

**Step 4** Click the link for the file that you need in the Filename column, for example, merlot-2.0.0.0.28.meta.

**Step 5** A page is displayed where you can verify the details of the file that you chose. If you are sure that this is the file you need, click the link for the file.

**Step 6** You are prompted to open the file or save the file to a location on your hard drive. Choose **Save File**.

**Step 7** Locate a directory on your hard drive or LAN to temporarily hold the update file and click **OK**.



---

**Note** You will use the update file later to update the Cisco Internet CDN Software on your CDN devices, so be sure to place the file in a location which is easy to remember and accessible.


---

**Step 8** Proceed to the section [Step 3—Update the Software on Your Cisco Internet CDN Devices](#) for instructions on using the update file to update the software on your Cisco Internet CDN devices.

---

## Download from the Cisco FTP Server

Instead of downloading Cisco Internet CDN Software updates from Cisco.com, you can use your web browser to download the updates from the designated Cisco FTP site: `ftp://ftp.cisco.com`.

- 
- Step 1** Launch a Netscape browser window.
- Step 2** Log in to the Cisco FTP server as a registered user or as a guest.
- To enter as a registered user, enter your Cisco.com user ID and password in the Location field in the following format:  
`ftp://userid:password@ftp.cisco.com`
  - To enter as a guest user, the URL is:  
`ftp://ftp.cisco.com`  
You are prompted to log on.
  - If you were given a special access code by e-mail or by a customer support representative, follow the instructions specified in the e-mail.
- Step 3** Navigate to the following download directory on the FTP server:  
`cisco/content-delivery/cdn/sp/`
- Step 4** Locate the .upg update file for the version of the Cisco Internet CDN Software that you need. Determine which version you need by referring to the “[Software Compatibility](#)” section on page 3. Depending on the version that you currently have, you may have to perform two upgrades to reach version 2.1.
- Step 5** Right-click the filename and choose the **Save Link As** or **Save Target As** option to save the target file to your local machine.
- If you are prompted to open the file or save it to a disk, choose to save the file to a disk. Locate a directory on your hard drive or LAN to temporarily hold the update file and click **OK**.
-  **Note** Because you will use the update file later to update the Cisco Internet CDN Software on your CDN devices, place the file in a location which is easy to remember and accessible.
- 
- Step 6** Proceed to [Step 3—Update the Software on Your Cisco Internet CDN Devices](#) for instructions on using the update file to update the software on your Cisco Internet CDN devices.
- 

## Step 3—Update the Software on Your Cisco Internet CDN Devices

The CDM will reboot at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the graphical user interface.

To update the Cisco Internet CDN Software on your devices, follow these steps:

- 
- Step 1** From the CDM user interface, click **tools**.
- Step 2** From the drop-down list, choose **Software Update**.
- Step 3** On the Software Update page, click the radio button next to the update file that you want to use.

**Step 4** Click the tab corresponding to the type of device that you want to upgrade, for example, **Content Routers**. The window refreshes, listing the devices of the selected type on your CDN.



**Note** When updating the software on your Content Engines, you need to ensure that all Content Engines in a single supernode are updated at the same time.

**Step 5** Refer to the column labeled Version to verify that the devices you are choosing are not already running the version to which you will be upgrading. Also verify that the current version has an upgrade path to the version to which you are upgrading.



**Note** If you have questions regarding upgrade paths, see the [“Software Compatibility” section on page 3](#) or contact Cisco Technical Support.

**Step 6** Select the check boxes next to the name of the device you will be upgrading, or select the box in the column header to select all devices.

**Step 7** Click **OK**. The update process begins on the selected devices and they go offline temporarily.

**Step 8** Repeat [Step 4](#) through [Step 7](#) for each device or group of devices that you wish to upgrade.

**Step 9** Click the **Refresh** button to see the status of your upgrade.

You have completed the software update procedure.

Allow 15 to 30 minutes for the devices to come online on the CDM user interface after the upgrade has been completed. The CE-7320-CDN takes longer to come online than the CE-590-CDN because of the number of drives on the device.

## Important Notes for Service Providers

This section describes the limitations on and the non-intuitive behavior of some features of the Cisco Internet CDN Software. The topics covered are:

- [Content Engine Log Files May Be Overwritten](#)
- [Configuration Script for the Content Services Switch Has Been Modified](#)
- [Content Engine Log Files May Be Overwritten](#)
- [Adding a Deleted Content Distribution Manager Back to the CDN](#)
- [Standby Content Distribution Manager Cannot Be Upgraded Through the User Interface](#)
- [Deployment of Standby Content Distribution Manager Requires Content Engines in Supernodes to Be Running Version 2.1](#)
- [Using RealServer’s RealSystem Media Commerce Suite](#)
- [Limitations on Coverage Zones](#)
- [Accessing System Logs Page May Cause Internal Server Error](#)
- [Large Content Engine Log Files May Be Transferred to FTP Host](#)



## Content Engine Log Files May Be Overwritten

Content Engine log files may be overwritten if they are not removed from the FTP server before new logs files are generated. This happens because of three processes on a Content Engine:

1. **Logrotate**—Every 10 minutes, the logrotate process on a Content Engine looks for new log files to rotate. At this stage, the filenames have the structure fileroot.N.
2. **Stream-logrotate**—Every hour, the stream-logrotate process on a Content Engine looks for newly-rotated log files. If there are rotated log files present, it processes and compresses them. When the files are compressed, their filenames are changed to the structure fileroot.N.gz. The filename change makes the previous filename, fileroot.N, available for re-use by the logrotate process.
3. **Logmover**—At an interval that you define on the Remote Logging page, the logmover process on a Content Engine looks for files of the form fileroot.N.gz and starts putting timestamps on them and moving them to the remote FTP server.

The logrotate, stream-logrotate, and logmover processes are not synchronized. If the setting for remote logging transfer, which activates the logmover process, is too high, the compressed files are still present on the Content Engine while new files are being rotated and compressed. Since the rate at which files are compressed may be faster than the rate at which they are transferred to the FTP server, newly compressed files may overwrite older files with the same filenames.

The frequency with which you need to move the files to the remote FTP server depends on how much time your log files take to reach their maximum size limit. This time depends on the load that your Content Engines experience. Bearing a load of 150 HTTP transactions per second, a single Content Engine, in one hour, has to send out about 10.8 MB of SQuID logs to the FTP server, which amounts to a sustained load of 0.024 MB per second. This figure scales linearly with the number of transactions.

To reduce the likelihood of log files being overwritten, you must:

- Ensure that the remote FTP server is always up and available, and that you have a high bandwidth connection to it.
- Set the remote logging transfer interval (on the Remote Logging page) to a low value. We recommend a value of 10 minutes. This will increase the likelihood of log files being transferred from the FTP server as soon as they are compressed.

## Configuration Script for the Content Services Switch Has Been Modified

The Content Services Switch (CSS) configuration script has been modified to allow you to add as many interfaces to a VLAN as are available on the CSS. Previously, you could not assign more than 32 interfaces to one VLAN. After you assign a number to the VLAN, you are asked to assign interfaces in increments of ten. For example:

```
What is the number [1-4095] of this VLAN? [default = 1] 821
```

```
Configuring interfaces bridged to this VLAN ...
```

```
How many interfaces are bridged to this VLAN? 56
```

```
Please input interfaces from 1 to 10: Separate them by space.
```

```
1/1 1/2 1/3 1/4 1/5 1/7 1/8 2/1 2/2
```

```
Please input interfaces from 11 to 20: Separate them by space.
```

```
2/3 2/4 2/5 2/6 2/7 2/8 3/1 3/2 3/3
```

Do not input fewer than 10 interfaces, unless there are no more to enter. The script will only ask you to input interfaces as many times as it would take for you to enter all the bridged interfaces in increments of ten. For example, if you entered 56 as the number of interfaces you would like bridged to the VLAN, the script will only ask you to input the interfaces 6 times. The script does not check to ensure that you input as many interfaces as you specified in your answer to “How many interfaces are bridged to this VLAN?”. If you fail to enter all the interfaces in this sequence of the script, you must re-run the script.

## Some Features Are Unusable Unless All Devices Are Running Version 2.1

A CDN comprising devices using mixed versions of the Cisco Internet CDN Software is supported. However, features that are new to version 2.1 are unusable in the CDN unless *all* devices are running version 2.1. Some of these features are:

- Windows Media Technologies (WMT) support—If you want to serve WMT for a hosted domain, you must ensure that all Content Engines serving that hosted domain are running version 2.1.
- Hybrid routing—To use the hybrid routing feature, all CDN devices need to be running version 2.1.
- Warm standby Content Distribution Manager (CDM)—CDN devices that are not running version 2.1 will not be aware of the standby CDM.

## Adding a Deleted Content Distribution Manager Back to the CDN

A Content Distribution Manager (CDM) can be deleted from the network. To add it back to the network, establish a Secure Shell connection with the device, determine if your CDM is configured as a standby or a primary, and follow the appropriate procedure:

If the CDM is configured as a standby:

- 
- Step 1** Enter **register**.
  - Step 2** Go to the primary CDM’s user interface.
  - Step 3** Activate the standby CDM through the user interface.
  - Step 4** Wait for the standby CDM to come online.
- 

If the CDM is configured as a primary and you want to add it back to the CDN as a standby, follow these steps:

- 
- Step 1** At the prompt, enter **setup** and, when prompted, specify that the CDM is a standby.
  - Step 2** Enter the current primary CDM name when asked for the DNS name of the active CDM.
  - Step 3** At the prompt, enter **register**.
  - Step 4** Go to the primary CDM user interface.
  - Step 5** Activate the standby CDM through the user interface.
  - Step 6** Wait for the standby CDM to come online.
-

When the user interface indicates online status, the CDM is back on the network and has synchronized its database with the other CDM.

The bug tracking number for this issue is CSCdv43131.

## Standby Content Distribution Manager Cannot Be Upgraded Through the User Interface

To upgrade a standby Content Distribution Manager (CDM):

- 
- Step 1** Log in as **admin** to a Secure Shell (SSH) session with the CDM.
- Step 2** Load the upgrade file onto the CDM by entering the following commands:

```
ftp
Host> open ftp.cisco.com
Host> username: CCO_user_account_name
Host> password: CCO_account_password
Host> passive
Host> cd/cisco/content-delivery/cdn/sp
Host> get upgrade_filename
Host> bye
Host> enable
Host# upgrade swupgrade
```

When the upgrade is complete, the CDM will reboot itself.

---

## Deployment of Standby Content Distribution Manager Requires Content Engines in Supernodes to Be Running Version 2.1

While version 2.1 of the Cisco Internet CDN Software supports CDNs in which some nodes are running earlier (2.0.x) CDN software releases, if you have deployed a failover Content Distribution Manager (CDM) and supernodes on the same CDN, it is necessary to update the software on *all* Content Engines and Content Routers in your supernodes to version 2.1 so that those supernodes can continue to communicate with the failover CDM.

## Using RealServer's RealSystem Media Commerce Suite

RealServer's RealSystem Media Commerce Suite (RSMCS) has not been integrated into the software. (bug number CSCdv66612). You must, instead, purchase the appropriate RealServer RSMCS plugin from Real Networks and then install it on a Content Engine running version 2.1 software. Once you have obtained the plugin, follow these steps to install it on your Content Engine:

- 
- Step 1** Verify that the plugin file you have is `rmffplin-linux.so.6.0`, the linux version that you need for the Cisco Internet CDN.
- Step 2** Log in to a Content Engine in bash mode.
- Step 3** Change the current directory to: `/cisco/merlot/real/Plugin` by entering the following command:
- ```
cd /cisco/merlot/real/Plugin
```

- Step 4** Change this directory to read/write mode by entering the **rw** command.
  - Step 5** Transfer the plugin to this directory by using SCP or FTP.
  - Step 6** Change the directory back to read-only mode by entering the **ro** command.
  - Step 7** Restart the Internet CDN software by entering **control restart**.
- 

For Real media content that you want protected by RSMCS, specify the `playserver` property as "real" in the manifest. For example, if you have an RSMCS file named `foo.rms`, and want the `cdn-url` to be `cdn_foo.rms`, the item in the manifest file should read:

```
<item playserver="real" src="/foo.rms" cdn-url="/cdn_foo.rms">
```

## Limitations on Coverage Zones

For coverage zones to work, all Content Routers must be running Cisco Internet CDN Software Version 2.1. Coverage zones for a particular hosted domain work only if all Content Engines serving that hosted domain are running Internet CDN Software Version 2.1.

## Accessing System Logs Page May Cause Internal Server Error

The user interface may display an "Internal server error" message when you go to the Tools > System Logs page because it tries to fetch a large set of system messages.

## Large Content Engine Log Files May Be Transferred to FTP Host

Content Engine log files that are in the process of being generated are transferred to the FTP host if they reach a size that is above the limit specified on the Tools > Remote Logging page. Files that are already generated are not affected in this way.

## Important Notes for Content Providers

This section describes guidelines that content providers need to follow when they CDN-enable their content. It also describes the behaviors that users accessing their CDN-enabled content can expect to see. The topics covered are:

- [Limitations on Using Windows Media Player](#)
- [Windows Media Player Plug-In Required for a Netscape Browser](#)
- [Uppercase Tags Should Not Be Used in Content URLs](#)


## Limitations on Using Windows Media Player

Windows Media Player 6.4 is supported only on Microsoft Internet Explorer for Windows Media Technologies (WMT) streams served through the CDN. To support Windows Media Player 6.4, Content Providers need to take the following steps:

- When editing the HTML source of their site, they should use mmst-style URLs for all content that will be served by the WMT server. The structure of the URL should have either of the following two structures:
  - mmst://hosted\_domain\_name/hosted\_domain\_name/cdn-wmt/cdn-url
  - mmst://hosted\_domain\_name/hosted\_domain\_name/cdn-url

Table 1 describes the components of the URL.

**Table 1** Components of the mmst URL

URL Component	Description
hosted_domain_name	Fourth-level domain name assigned to your hosted domain or the alias assigned to that hosted domain.   <b>Note</b> The hosted domain name must appear twice in the URL.
cdn-wmt (optional)	Specifies that you are designating the WMT server to handle the content item to which you are linking. Playservers can be specified in a number of locations, including the manifest file. Playserver designations in the URL of a content item override a content mapping in the manifest file.
cdn-url	Relative location of the content item on the CDN device. This value is supplied by the cdn-url or src attribute in the <item> tag in the manifest file for each piece of content.  Wildcard characters are accepted in the cdn-url attribute only when you link to live content. Actual content URLs must point to the actual content item.

- Content providers should use variable bitrate (VBR) encoding or some other form of low-bandwidth encoding when creating content files. VBR encoding enables the Windows Media Player to download a version of the content file that is appropriate for the bandwidth setting of the player. This is necessary because Windows Media Player 6.4 does not handle high-bitrate fixed encoded content sent over low-bandwidth connections. This problem does not exist with Windows Media Player 7.x or higher.
- Content providers should urge end users to upgrade their Windows Media Players to the latest version available for their operating system.

For a complete discussion of manifest file creation and URL publication for CDNs, see the *Cisco Internet CDN Software User Guide* for version 2.1, Chapter 2, in the section “Setting Up a CDN.”

## Windows Media Player Plug-In Required for a Netscape Browser

To open a Windows Media Technologies (WMT) file in a Netscape Version 7.x browser, end users need to install a Window Media Player plug-in. Otherwise, when the Netscape browser launches Windows Media Player, an error message appears, saying “Invalid or corrupt data was encountered.”

## Uppercase Tags Should Not Be Used in Content URLs

Browsers display a “Page Not Found” message and fail to stream content if the CDN tag in the content URL has uppercase letters. For example:

```
http://hosted_domain/CDN-MEDIA/filename.xxx.
```

## Copyright Notices and Licenses

This product contains copyrighted programs and license agreements that are used with permission and are the property of the following respective owners.

**TomCat** Copyright © 1999 The Apache Software Foundation. All rights reserved.

**OpenSSH** Copyright © 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

**Jama** Copyright Notice: This software is a cooperative product of The MathWorks and the National Institute of Standards and Technology (NIST) which has been released to the public domain. Neither The MathWorks nor NIST assumes any responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

**ModSSL** Copyright © 1998-2001 Ralf S. Engelschall. All rights reserved.

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod\_ssl project (<http://www.modssl.org/>).

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

**Apache-SSL Server, OpenSSL** Copyright © 1995,1996,1997 Ben Laurie. All rights reserved.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

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

### Java JRE

Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Except as specifically authorized in any Supplemental License Terms, you may not make copies of Software, other than a single copy of Software for archival purposes. Unless enforcement is prohibited by applicable law, you may not modify, decompile, reverse engineer Software. Software is not designed or licensed for use in on-line control of aircraft, air traffic, aircraft navigation or aircraft communications; or in the design, construction, operation or maintenance of any nuclear facility. You warrant that you will not use Software for these purposes. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

#### NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## Open Caveats

The following caveats are open (unresolved).

- CSCsp00588  
If a Content Engine or Content Router is shut down, the event may not be logged in the System Event Log on the Content Distribution Manager.
- CSCsp01022  
There is no visual indication whether or not passwords have been overridden on a Content Delivery Network device.
- CSCsp01245  
A "Page not Found" error message is displayed in the Add Update File window when the Content Distribution Manager cannot reach the device hosting the upgrade file.
- CSCsp01249  
The web browser times out, displaying a "Page Not Found" error when the Content Distribution Manager attempts to locate upgrade files on an unreachable server.
- CSCsp01372  
It is possible to add the same upgrade files multiple times to the same Content Distribution Manager. This does not impact the upgrade in any way.
- CSCdt96485  
The QuickTime server runs even if you disable it.
- CSCdu04445  
After you run netsetup on a Content Engine 7320, you see the following message:  

```
epro100: Device or resource busy rmmmod: module acenic is not loaded
```

  
You can ignore this message.
- CSCdu21113  
The Supernode page allows you to create multiple supernodes with one Content Services Switch (CSS), even though creation of multiple supernodes on a single CSS is not supported. If you erroneously create multiple supernodes on one CSS, you should delete all supernodes associated with that CSS, and then create only one supernode.
- CSCdu24791

The sort indicator on the View Supernode page does not appear after you click the Refresh button.

- CSCdu38518

To preserve security, FTP is disabled on the Content Services Switch (CSS) by default. To transfer upgrade files to a CSS, you need to enable FTP on the switch. After you have transferred the file, you should disable FTP again.

- CSCdu41069

When an inactive Content Engine or Content Router is registered, the Modify Content Engine or Modify Content Router page initially displays the fully qualified domain name (for example, ce590-1.canada.org). Once the Content Engine or Content Router reboots for the first time and comes online, only the host name (for example, ce590-1) is displayed on the user interface. This does not impact the routing capability of the CDN.

- CSCdu42467

The clock on a device is not updated if the Network Time Protocol (NTP) server is inaccessible while the device is booting. To avoid this, you should wait until the NTP server is available and then reboot the device.

- CSCdu44384

When a RealServer license expires on a Content Engine, an error message indicating the expiration is not logged. An expired RealServer license prevents the Content Engine from serving content through the RealServer.

- CSCdu45008

If you delete a Supernode from the CDM and then recreate the Supernode, identical to the deleted one, all Content Engines associated with the re-created supernode must be rebooted to function properly. If they are not rebooted, they fail to serve content.

- CSCdu50308

In the command line interface, if you run setup remotely through Secure Shell (SSH) using the Dynamic Host Configuration Protocol (DHCP) address, you are disconnected from the device when netsetup is completed. You can reconnect to the device by using the IP address you specified during setup.

- CSCdu53388

In Netscape, if you try to assign Content Engines to a hosted domain and fail to select a root location, the user interface does not display a warning message; it accepts the change when you click the Save button. If you do this using Internet Explorer, the user interface tells you that you must specify a root location.

- CSCdu56255

The system allows you surpass the limit on the number of content items you can assign to a Content Engine (CE). When you have reached the limit, the CE warns you that you have reached the limit but allows you to assign further items. By default, the limit is set to 500,000 items, but the CE 7320 can support up to 1 million.

- CSCdu57706

The **dnslookup** command in the command line interface does not function as documented; it fails to resolve the host name of an IP address that you enter.



- CSCdu57718

If you enter the show logs command line interface command during a period of high end user activity on the system, the log output gets stuck on the SQuID log (the squid log records HTTP requests for content). To break out of this command, press Ctrl-C. To view selected logs, use the **view path\_of\_log\_file** privileged level EXEC command. The following log files are available:

- /cisco/merlot/state/merlot.log
- /cisco/merlot/state/apache/log/\*\_log
- /cisco/merlot/state/squid/logs/\*.log
- /cisco/merlot/state/sysout/\*.log

- CSCdu60211

If you have assigned a Content Engine (CE) to a location, you must manually restart the CE if you later change it to a different location through the Content Engine Details page. Otherwise, your routing performance will not be optimal.

- CSCdu64147

While you modify a supernode cluster, an extra row is added to the Content Engine table.

- CSCdu66216

On the Software Update page, the file at the top of the list of upgrade meta files is selected by default. When you choose a different file, this choice is not perpetuated to all the other device tabs. Under the other device tabs, the file at the top of the list remains as the default. You must choose the upgrade file for each device individually.

- CSCdu69371

Content Engines fetch the manifest file from the origin server instead of the hosted domain leader Content Engine. This is by design.

- CSCdv69513

When you fetch the Coverage Zone file from a Content Router, you will see many warning messages in the merlot log file. These messages do not indicate disruption of hybrid routing.

- CSCdu70671

When you attempt to update a CDN password, the ! icon appears next to the wrong field after an incorrect value is entered into the Old Password field.

- CSCdu71747

Password verification is limited to the first eight characters of the password.

- CSCdv13330

If your Content Distribution Manager (CDM) fails to come online after a reboot, this may be due to a connectivity problem with the database. However, if you run the **node status** command, you may erroneously be told to run a database rollback. Before you run a database rollback, you should look at the CDM merlot log for a message that says, “DBupgrade records contain incomplete operation ... run rollback.” If you see this message, running the **upgrade rollback** in the command line interface fixes the problem. If you do not see this message, you should remove the DBUPGRADE-FAILED file from the merlot-state directory and restart the Cisco Internet CDN Software by entering the **node restart** command in the command line interface.

- CSCdv27477  
If you erroneously enter “http://” before the origin server name on the Hosted Domain Details page and click Save, the system rejects the whole transaction and requires you to start over. You also lose all information that you may have entered in the fields.
- CSCdv31624  
Content Engine performance drops briefly on an hourly basis because of usage log processing.
- CSCdv33683  
For .ram files, content providers must use a CDN tag in the manifest file. The syntax must use the cdn-http tag, for example: http://hosted\_domain\_name/cdn-http/path\_to\_file.ram.
- CSCdv38305  
If you are upgrading from Version 2.0.1 to 2.1, subsequent to running setup on a device, you should immediately change the device password through the Content Distribution Manager user interface. If you do not change it, the security of your system is compromised because somebody can access the device using default information. The password that you set during setup only protects your device temporarily following reboot.
- CSCdv44831  
If you use a browser that does not have cookies or JavaScript enabled, you receive a session timeout message. For the user interface to function, you must have both cookies and JavaScript enabled in your browser options.
- CSCdv47796  
Do not downgrade a Content Distribution Manager (CDM) from the user interface; doing so may corrupt your database’s table structure. Instead, downgrade your CDM through the command line interface using the upgrade command. For more information on using the command line interface, refer to the *Cisco Internet CDN Software Command Reference* for version 2.1.
- CSCdv49216  
When you create or modify a routed domain or SKCA/IMS settings, the newly created information may take up to 10 minutes to propagate to the Content Engines.
- CSCdv50195  
If you reset your Content Distribution Manager (CDM) password to the default using the reset-password script, you should change it immediately afterward through the CDM user interface.
- CSCdv52128  
In Internet Explorer, next-click failover does not work for Windows Media Technologies (WMT) 7.1 content requested through HTTP. If you send HTTP requests through an Internet Explorer browser, after a Content Engine failure behind a supernode, you need to take of the following actions:
  - Go back to the original HTTP URL and click it again.
  - Do a refresh for any URL you enter in the browser location field.
  - Publish the HTTP URL as a web link.

If you are using Internet Explorer 6.0, you can also get next-click failover by closing the WMT player, entering the HTTP URL directly into the browser location field, and then pressing Return.
- CSCdv62694  
The peekable interface is disabled by default on Content Engines and Content Routers. If you do not enable the peekable interface:

- You receive a “Page not found” error when clicking on a Content Engine on the Hosted Domains > Replication Status page.
- You cannot access the Java Monitor for Real Server.
- You cannot view the Tools > System Tools > Simple Peek page for the device, which you use to enable or disable Telnet and debugging.
- You cannot view manifest log files for hosted domains.

To enable the peekable interface, enter the **node peekable** command in the command line interface. For more information, refer to the *Cisco Internet CDN Software Command Reference* for version 2.1.

- CSCdv62704

In a single software upgrade transaction, you can upgrade only the devices on one page. When you select the check-all check box on the Upgrade Software page, all of the devices on that web page are selected. If you then go to the next page and choose all the devices, the devices on the first page are de-selected.

- CSCdv64154

When you are running setup on a Content Distribution Manager (CDM), you are prompted to enter the Oracle database username that you specified during Oracle configuration. You should not use the username of the database account to which you assigned administrator privileges. Doing so causes problems during upgrades and downgrades. If you only created one user account during database setup and gave it administrator privileges, you have to run the **dbsetup** command, through the command line interface, to create a second user without administrator privileges. Once you have done so, you can rerun setup on the CDM.

- CSCdv65761

If you have Content Engines with Version 2.0.1 and a Content Router that never rebooted after Version 2.0.1 was installed on it, you must reboot the Content Router before upgrading it to version 2.1. If you do not reboot prior to upgrading, Content Engines running Version 2.0.1 will lose contact with the Content Router until they are rebooted.

- CSCdv66612

The Media Commerce Suite for RealServer has not been integrated into the software.

- CSCdv67951

You should run Network Time Protocol (NTP) setup on a Content Services Switch (CSS) after you configure the IP address and default gateway. The reason is that the CSS configuration is clear before it starts, so the absence of an IP address or default gateway prevents the CSS from contacting the NTP server that you specify.

- CSCdv70049

The **no** command that appears in the command line interface configuration menu is nonfunctional.

- CSCdv70721

You must reboot a Content Router after removing the URL for its coverage zone file from the Content Distribution Manager user interface.

- CSCdv71374  
You are not given a message warning that making either of the following modifications to Windows Media Technologies (WMT) settings causes the device to restart:
  - On the Tools > Windows Media Server Configuration page, setting the maximum number of concurrent streams or the maximum amount of bandwidth to serve concurrently.
  - Checking the Enable WMT check box on a Hosted Domain page.
- CSCdv71468  
On the Tools > Routing Properties page, if you change the setting for the minimum number of name server records to fewer than three, the new setting does not take effect until the Content Routers are rebooted.
- CSCdv71769  
When you install a Content Engine and then attempt to activate it through the Content Distribution Manager user interface, the fully qualified domain name that you specified during setup is not propagated to the Content Engine page. Instead, the description that you specified for the Content Engine during setup appears in the Content Hostname field and you get an error message saying, “Transaction not completed! Content hostname must contain at least 1 dot.” The workaround for this is to enter the fully qualified content host name in the Content Hostname field and then click the Save button.
- CSCdv72380  
The **show build** command in the command line interface returns inaccurate information. To verify which build is installed, enter the **info** command, and check the “CDN SW Version” entry in the output.
- CSCdv80036  
If you reboot a Content Engine that has a missing hard drive, all cached content on that Content Engine becomes unavailable. If a hard drive fails, *always* replace the disk with a SCSI disk with the same SCSI ID as the failed drive before rebooting the Content Engine. Do not reboot the Content Engine with a drive missing, as this can potentially destroy data.
- CSCdv80269  
Your Content Engine may stall during a Version 2.0.1 —> Version 2.1 software upgrade. If this happens, you need to reboot the Content Engine and repeat the upgrade procedure.
- CSCdv82691  
End-users may be unable to play the Real live stream that they select.
- CSCdv84379  
When you change the status of a Content Distribution Manager from primary to standby, the change is not recorded in the system log.
- CSCdv84723  
Do not use the —cdn tag in a hosted domain name or a filename; doing so will cause the RealServer, Darwin, and Windows Media Technologies (WMT) servers to have trouble verifying requests for content.

- CSCdv88053

If you enter a Video On Demand (VOD) quota setting on a Content Engine by using the **node diskadmin** command line interface command, the change is not registered. Changes made through the Content Distribution Manager (CDM) user interface are registered. This may cause a discrepancy between the VOD quota value that the CDM user interface displays and the value that the command line interface **show disk** command displays.

## Resolved Caveats

The following caveats are fixed (resolved) in version 2.1.

- CSCdu03195

The RealServer Java Monitor is not fully implemented.

- CSCdu16048

Deployment of a standby Content Distribution Manager in the event of failover should be supported to allow for geographic diversity.

- CSCdu21104

During setup, it should be possible to specify a VLAN name for a Content Services Switch.

- CSCdu23464 F

The Distributed Licensing for RealServer feature does not work for live streams.

- CSCdu24818

On the Content Router details page, under the Management Information heading, the Content Router IP address appears where you should see the Content Router host name. This resolves itself after some time.

- CSCdu34339

The status message on the Replication Progress page identifies live content files as “live items” but pre-positioned content files as “items.”

- CSCdu37494

Manifest errors that appear in the logs are not displayed on the user interface.

- CSCdu39865

There is no inactivity timeout associated, by default, with the CDM user interface, which users can set through the Tools > System Configuration page. There is, however, a `cdm.session.timeout` property that you can set as a user interface logout interval. For instructions on how to modify this property, refer to the *Cisco Internet CDN Software User Guide* for version 2.1, Chapter 4, in the section “Modifying the System Timeout Value.”

- CSCdu45677

The sorting button on the user interface first sorts uppercase items and then lowercase items.

- CSCdu48305

There should be multiple levels of user access.

- CSCdu49531

If you connect to a Content Engine with only the Gigabit Ethernet interface connected, the device fails to register with the Content Distribution Manager.

- CSCdu52703  
It should be possible to distribute configuration scripts from the Content Distribution Manager to the Content Services Switch through the user interface.
- CSCdu53202  
There should be a command line interface command for creating optional static routes for a Content Router.
- CSCdu56623  
The **node restart** command in the command line interface does not work.
- CSCdu57678  
The **contentmask** command in the config menu of the command line interface is not implemented.
- CSCdu58508  
The **node update** command in the command line interface does not work.
- CSCdu59102  
The prompt that is visible when you are logged in to a Content Services Switch (CSS) should be identical to the name of the supernode that the CSS is a member of.
- CSCdu62385  
The system allows you to add Content Engines with insufficient free disk space to hosted domains. This results in pre-positioned content being dropped from the Content Engine.
- CSCdu67146  
When a Content Engine that is the last node in the root location changes its location, the assigned hosted domains using that root location must have their root location changed as well.
- CSCdu70447  
A supernode cannot come on line if the Content Distribution Manager is off line.
- CSCdu71733  
Servers stop notifications are not issued to the SNMP manager if you run **node stop**, **exit**, and **reboot** commands on a device.
- CSCdu73919  
The configuration script for each device should enable users to use their company name as a signature on certificates.
- CSCdu74015  
If you delete the location leader Content Engine and add it back, two Content Engines will take on the role of location leader.
- CSCdu74880  
Access logs for Content Engines that are behind a Content Services Switch need to be labeled with the primary IP address, not the hidden IP address. This is because the same hidden IP address may be used on different supernodes.
- CSCdu76981  
SNMP times out while scanning ghost drives on Content Engine-590 devices.
- CSCdu80912  
When configuring Content Services Switches in a redundant configuration, administrators receive the following message: "The script is in use by another session."

- CSCdu89261  
Content Engines report to Content Routers and their supernode leader while shutting down. This increases the period when Content Routers route requests to Content Engines that cannot serve them.
- CSCdu89276  
Content Engines and Content Routers report being on line even when they fail to serve content.
- CSCdv01319  
System time is not displayed on all pages of the user interface.
- CSCdv02380  
The IP address or location of the origin server should not be displayed in the error message you see when the origin server goes down while trying to retrieve content.
- CSCdv02431  
The gateway IP address that you assign to a Content Engine must be reverse-resolvable.
- CSCdv07620  
Generation of SNMP traps due to changes in run-mode level is not implemented.
- CSCdv12657  
Running the command line interface command **node stop** may prevent the system from restarting.
- CSCdv14297  
The Windows Media Technologies (WMT) server continues running on Content Engines even when Windows Media Server (WMS) is deactivated on the Tools > WMS Configuration page.
- CSCdv15182  
Content Engine statistics are not displayed correctly on a hosted-domain-by-hosted-domain basis.
- CSCdv15190  
To restore the default CLI or HTTP passwords on Cisco Internet CDN devices:
  - Reboot the device.
  - At the LILO prompt, enter **linux single**.
  - At the bash prompt, enter **/cisco/merlot/etc/reset-passwd**.
  - Reboot the device.
 You can now log in to the device using the default passwords. The passwords will remain reset until a new password is set using the Content Distribution Manager user interface.
- CSCdv17970  
Scroll bars are missing on the Routing Diagnostics > View Supernodes page.
- CSCdv19565  
The user interface does not always give a warning or require confirmation when an operation will result in a reboot or restart.
- CSCdv24460  
Telnet ports respond to probes even when they are disabled.
- CSCdv28773  
Sometimes you do not receive server stop traps because the SNMP agent shuts down early.

- CSCdv30542  
The system does not keep track of used WMT licenses or require acknowledgment of an end user license agreement.
- CSCdv30840  
The **node status** command line interface command does not give you information about the WMT server, as it does for the QuickTime and RealServer.
- CSCdv33958  
Scrollbars are missing on the Content Router peek page.
- CSCdv34752  
You cannot log in to the command line interface as admin after doing a manual upgrade. Instead, you have to log in to the bash shell and reboot the device.
- CSCdv34827  
The DNS statistics on the Content Engine Statistics page always show a value of 0. This is incorrect.
- CSCdv35138  
If the wildcard is removed from a manifest and the manifest file re-fetched, RealPlayer returns an error message stating that either the file cannot be found or “A General Error has occurred” when trying to access the live stream.

## Documentation Corrections

This section documents corrections to the following manuals:

- [Cisco Internet CDN Software Configuration Guide for Version 2.1](#)
- [Cisco Internet CDN Software User Guide for Version 2.1](#)
- [Cisco Internet CDN Software Command Reference for Version 2.1](#)

## Cisco Internet CDN Software Configuration Guide for Version 2.1

- This correction applies to the following sections in Chapter 2:
  - Configuring a Content Distribution Manager
  - Configuring a Content Router
  - Configuring a Standalone Content Engine
  - Configuring a Content Engine as Part of a Supernode

The first three steps in each of these sections should be replaced with the following:

- 
- Step 1** Boot the device.
  - Step 2** Log in as **admin** with the password **default**.
  - Step 3** At the prompt, enter **enable**. Press **Enter**.



**Step 4** At the prompt, enter **config**. Press **Enter**.

**Step 5** At the config prompt, enter **setup**. Press **Enter**.

Continue with Step 4 in the appropriate section of the *Cisco Internet CDN Software Configuration Guide* for version 2.1.

- On page 1—2, RealNetworks RealPlayer and Apple QuickTime player should not be listed as software required to access the Content Distribution Manager user interface.

## Cisco Internet CDN Software User Guide for Version 2.1

In Chapter 4, “Maintaining Cisco Internet CDN Software,” the “Setting Up Remote Logging” section contains inaccurate log file formats for the different servers. The correct log file formats for each server are shown below. Note that the time stamp in each of the above log filenames is not given in milliseconds.

- SquID cache log file format  
IPaddress~access.log.lognumber~timestamp.cdn.gz
- QuickTime server log file format  
IPaddress~StreamingServer.lognumber.log~timestamp.cdn.gz
- RealServer log file format  
IPaddress~rmaccess.log.lognumber~timestamp.cdn.gz
- Windows Media Technologies log file format  
IPaddress~mms\_export.xxxxx.log~timestamp.cdn.gz

## Cisco Internet CDN Software Command Reference for Version 2.1

Usage guidelines for the **shutdown** command should state “After entering the **shutdown** command, you need to boot up the device manually. You need physical access to the device, because you cannot access the device remotely until you physically reboot the device.”

## Related Documentation

This section lists documentation that provides additional information about the Cisco Internet CDN hardware and software.

- [Hardware Documents](#)
- [Software Documents](#)

## Hardware Documents

The following documentation provides additional information about the Cisco Internet CDN hardware:

- *Cisco Internet CDN Documentation Roadmap*
- *Cisco Content Distribution Manager 4670 Product Description Note*
- *Cisco Content Engine 500 Series Hardware Installation Guide*

- *Cisco Content Engine 500 Series Hardware Release Note*
- *Cisco Content Engine 7320 Product Description Note*
- *Cisco Content Router 4450 Product Description Note*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*
- *Cisco Catalyst Family Software Configuration Guide*
- *Cisco Content Services Switch Getting Started Guide*
- *Cisco Storage Array 6 Installation and Configuration Guide*
- *Release Notes for the Cisco Storage Array 6*
- *Storage Array 12 Installation and Configuration Guide*
- *Site Preparation and Safety Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

## Software Documents

The following documentation provides additional information about the Cisco Internet CDN software:

- *Cisco Internet CDN Software User Guide* for version 2.1
- *Cisco Internet CDN Software Configuration Guide* for version 2.1
- *Cisco Internet CDN Software Command Reference* for version 2.1

## Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems  
Attn: Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

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

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

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

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

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

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

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

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

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That’s Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

Copyright © 2001, Cisco Systems, Inc.  
All rights reserved.

