



Release Notes for Cisco ACNS Software, Release 5.1.11

August 4, 2005

ACNS Build 5.1.11b6



Note

The most current Cisco documentation for released products is available at Cisco.com at <http://www.cisco.com>. The online documents may contain updates and modifications made after the hardcopy documents were printed.

Contents

These release notes contain information about Cisco Application and Content Networking System (ACNS) software, Release 5.1.11. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Important Notes, page 3](#)
- [Caveats, page 5](#)
- [Documentation Updates, page 20](#)
- [Related Documentation, page 40](#)
- [Obtaining Documentation, page 41](#)
- [Documentation Feedback, page 42](#)
- [Cisco Product Security Overview, page 43](#)
- [Obtaining Technical Assistance, page 44](#)
- [Obtaining Additional Publications and Information, page 45](#)



Corporate Headquarters:

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

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

Introduction

ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media; ACNS software runs on Cisco Content Engines, Content Distribution Manager, and Content Router hardware platforms.


Note

The ACNS software 5.1.11 release is a maintenance release.

These release notes are intended for administrators who will be configuring, monitoring, and managing devices that are running ACNS 5.1.11 software. These release notes describe the open and resolved caveats regarding ACNS software, Release 5.1.11.

New and Changed Information

This section describes new and changed features in the ACNS 5.1.11 release. It also lists the supported hardware.

Changes to the Downgrade Script

The ACNS software downgrade script was updated to support downgrades from ACNS software, Release 5.1.11 to Release 5.0.

Hardware Supported

ACNS software, Release 5.1.11 supports the same hardware platforms that were supported in the ACNS 5.1, 5.1.3, 5.1.5, 5.1.7, and 5.1.9 releases. The following hardware platforms are supported:

- NM-CE-BP-SCSI
- NM-CE-BP-80G
- NM-CE-BP-40G
- CDM-4630
- CDM-4650
- CE-507
- CE-507AV
- CE-510-K9
- CE-510A-80GB-K9
- CE-565-K9
- CE-565A-72GB-K9
- CE-565A-144GB-K9
- CE-590
- CE-590-DC
- CE-7320
- CE-7305-K9
- CE-7305A-K9
- CE-7325-K9

- CE-510A-160GB-K9
- CE-560
- CE-560AV
- CE-7325A-K9
- CR-4430

Important Notes

This section emphasizes important information regarding ACNS 5.1.x software.

- [Media File System Issues When Downgrading to ACNS 5.0 Software](#)
- [Websense Issues When Downgrading to ACNS 5.0 Software or ACNS 5.1 Software](#)
- [Scheduling Live Events for Multiple Content Engines](#)
- [Multicast Sender Nonretroactive Scheduling Rule](#)

Media File System Issues When Downgrading to ACNS 5.0 Software

If you have configured the media file system (mediafs) with ACNS 5.1 software or later, and then downgrade to ACNS 5.0 software, the mediafs disk space assignment is lost and it reverts to ACNS network file system (cdnfs) disk space. (The mediafs is used for on-demand content that is fetched through the two streaming protocols [RTSP and WMT]. The cdnfs is used for pre-positioned content in the ACNS network.)

This situation occurs because of a design change that was implemented in ACNS 5.1 software. Because ACNS 5.0 software is not compatible with this change, the disk space becomes assigned to cdnfs instead of mediafs. To work around this problem, follow these steps:

1. After you downgrade to ACNS 5.0 software, use the CLI (**disk config EXEC** command) or the GUI to assign the mediafs disk space.

Use the Content Distribution Manager GUI for Content Engines that are registered with a Content Distribution Manager. Use the Content Engine GUI for standalone Content Engines (that is, Content Engines that are not registered with a Content Distribution Manager and are being managed through the Content Engine GUI or CLI).

2. Reboot the Content Engine for the disk configuration changes to take effect.

Websense Issues When Downgrading to ACNS 5.0 Software or ACNS 5.1 Software

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to ACNS 5.0 software or ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. Note that the ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed.

To avoid this problem when downgrading from ACNS 5.2.x software to ACNS software 5.1 or ACNS 5.0 software, follow these steps:

1. Disable the local (internal) Websense server on the Content Engine.
2. Deactivate the Websense services on the Content Engine.
3. Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.

Scheduling Live Events for Multiple Content Engines

When you schedule a program for a live event, we strongly recommend that you use Greenwich Mean Time (GMT) instead of the local time of the Content Engine that is delivering the program. If you are transmitting the live event across multiple Content Engines that span different time zones, and you schedule local time on each Content Engine instead of GMT, the live transmission is likely to fail.

Multicast Sender Nonretroactive Scheduling Rule

In ACNS 5.1 software, a primary multicast sender automatically schedules the first carousel pass, which sends multicast content to receiver Content Engines. However, ACNS software enforces a nonretroactive scheduling rule, which states that a multicast sender cannot send any files that arrived 10 minutes before it became a multicast sender. Thus, in ACNS software, Release 5.1, when a Content Engine becomes the active primary sender, it does not automatically schedule the first carousel pass to include content that is over 10 minutes old. If you want the old content sent, you must use the **distribution multicast resend** EXEC command *without* the **on-demand-only** option specified. (The **on-demand-only** option triggers a resend only when a negative acknowledgement [NACK] is issued. In this instance, you want to trigger the resend without a NACK from the receiver.)

After the first multicast carousel pass is complete (whether you manually triggered the resend using the **distribution multicast resend** command or whether the primary sender completed the pass automatically), the primary sender then determines whether the next carousel pass for content will follow a fixed schedule or whether it will be triggered by NACKs from receiver Content Engines.

In ACNS 5.1 software, you can configure the primary sender to disregard NACKs from receiver Content Engines and send content based on a fixed schedule of carousel passes. To enable this behavior, use the **multicast fixed-carousel enable** global configuration command. In contrast, a backup multicast sender cannot be enabled for fixed carousel passes; on backup senders, carousel passes must always be triggered by NACKs from receiver Content Engines.



Note

When the **multicast fixed-carousel** option is used, the **on-demand-only** option of the **distribution multicast** command is not available. The system displays an error message when the **on-demand-only** option of the **distribution multicast resend** command is issued in conjunction with the **multicast fixed-carousel enable** command.

The **multicast fixed-carousel enable** command is only available for the ACNS 5.1 software primary multicast sender. The default is no fixed carousel; the first carousel pass is automatic and future carousel passes are ondemand only, that is, they are triggered by NACKs.

Caveats

This section lists and describes the open and resolved caveats in ACNS software, Release 5.1.11. Caveats describe unexpected behavior in ACNS 5.1.11 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Open Caveats - ACNS Software, Release 5.1.11

This section lists caveats that have not been resolved in ACNS software, Release 5.1.11. The open caveats are grouped into two categories:

- [Open ACNS-IP/TV Software Integration Caveats, Release 5.1.11](#)
- [Other Open ACNS Software, Release 5.1.11 Caveats](#)

Open ACNS-IP/TV Software Integration Caveats, Release 5.1.11

This section lists and describes caveats that are open in ACNS software, Release 5.1.11, and are related to ACNS-IP/TV software integration.

- CSCec52492

Symptom: Requests for on-demand programs from clients in an ACNS network are sent to IP/TV Program Manager. IP/TV Program Manager treats these requests as standalone IP/TV on-demand program requests and directs them to the IP/TV Broadcast Server that can serve the request. This causes bandwidth issues and affects the functioning of IP/TV Server.

Condition: This problem occurs when IP/TV has been integrated in an ACNS network. It occurs when requests for on-demand programs that are exported to the ACNS network reach IP/TV Program Manager instead of being routed to the Content Engine that has the programs. This problem is related to routing failure or a routing error.

Workaround: Configure routing correctly in ACNS networks so that on-demand requests are directed to the nearest Content Engine that is capable of serving the program. Alternatively, you can change the proximity settings in IP/TV Program Manager so that it does not redirect the on-demand program requests to IP/TV Broadcast Servers. However, the second approach can also affect the serving of standalone on-demand programs.

- CSCec65255

Symptom: The audio stream sounds discontinuous when you listen to a rebroadcast or video on demand (VOD) of a recorded MP4 file.

Condition: The symptom occurs with IP/TV-generated MP4 files that are streamed from a Cisco Streaming Engine. The problem only occurs with MP4 files that contain an MP3 audio track sampled at 8000 Hz. Streaming the file directly from IP/TV Server does not result in this problem.

Workaround: Use a sampling frequency of 11025 Hz or 22050 Hz while creating a live program with MP3 audio if the recorded file is to be deployed in an ACNS network. Alternatively, use the AAC codec instead of MP3.

- CSCee35120

Symptom: When you are upgrading IP/TV Version 3.5 to Version 5.1, the functionality of the IP/TV Archive Server is replaced by Content Engines in the ACNS network. The Content Engines need to have the content present on a broadcast server but broadcast servers often have limited disk space.

Condition: This problem is only applicable if you are planning to upgrade from IP/TV Version 3.5 to Version 5.1 software, which will require that you use broadcast servers that have limited disk space.

Workaround: Import this data into your ACNS network by moving the media to a web server (origin server), and then creating a manifest file and an associated channel.

- CSCin70882

Symptom: For ACNS-based IP/TV scheduled programs that use live-split-only content delivery mode, IP/TV Program Manager allocates multicast addresses to individual streams that are never used along the content delivery path.

Condition: The problem is observed with live-split-only programs.

Workaround: There is no known workaround.

Other Open ACNS Software, Release 5.1.11 Caveats

This section lists and describes caveats that are open in ACNS software, Release 5.1.11 and are not related to ACNS-IP/TV software integration.

- CSCdy82311

Symptom: Content cannot be acquired using strong authentication from secure origin servers that use certificates from nonstandard certificate authorities (CAs). If strong authentication was chosen for content acquisitions from such a site, the acquirer error statistics will contain a 401 (Unauthorized) error code, and the acquirer error log contains the following error message:

```
Strong Cert Authentication rejects certificate due to error: ssl error code
```

Condition: This problem occurs if the origin server uses a certificate that is not known as a standard certificate to the ACNS software acquirer. For content acquisition from secure sites over HTTPS using strong authentication, only sites with certificates from standard certificate authorities are supported.



Note With strong authentication, if any errors occur during certificate verification by the ACNS acquirer, then content from that site will not be acquired. With weak authentication, certain errors (for example, a certificate has expired, certificate is not yet valid, and a subject issuer mismatch has occurred) are allowed during certificate verification.

Workaround: Use one of these workarounds:

- Use weak authentication.
- On the secure server, use a certificate that was generated by one of the standard certificate authorities. ACNS network administrators should refer to the following information to determine which CA certificate to install on their origin servers. Note that the certificate list differs based on the version of the ACNS software. For the ACNS 5.1.x software release or later, refer to the certificate list in the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*.

- CSCea51815

Symptom: When a Content Engine model CE-565 is attached to a Storage Array SA-7 device, if too large a cache file system (cfs) partition is configured, and a combined streaming and caching workload is used, then a lower HTTP performance is observed.

Condition: This problem occurs when the CE-565 has Windows Media Technologies (WMT) enabled; a combined streaming and caching workload is used, and the Content Engine is attached to an SA-7 device.



Note The Storage Array device is used for the cache file system (cfs).

Workaround: Allocate less space to the cfs if a Storage Array is attached to the Content Engine.

- CSCec52221

Symptom: Windows Media Technologies (WMT) is enabled with no media file system (mediafs) after you downgrade from ACNS 5.1b300 software to ACNS 5.0.7b8 software.

Condition: This occurs if you upgrade from ACNS 5.0.7b8 to ACNS 5.1bx software, configure the disk, and then downgrade to ACNS 5.0.7b4 software.

Workaround: Reconfigure the disk with a mediafs partition and reload the software.

- CSCec52319

Symptom: Using FTP inside the .meta file to have the Content Engine obtain the .bin file for a Content Distribution Manager GUI-initiated upgrade is unsuccessful if the user's home directory differs from the FTP root.

Condition: This problem occurs in either of the following situations:

- If you create the definition for the upgrade and the user's home directory does not contain a .bin file, then the Content Distribution Manager GUI displays an error message.
- If the FTP root directory does not contain a .bin file, then the Content Engine displays an error message.

Workaround: Copy the .bin file to both the FTP root and the user's home directory, or use a user whose home directory is the FTP root.

- CSCed00466

Symptom: The following error is reported when the ceApiServlet is called:

```
type Exception report
message
description The server encountered an internal error () that prevented it from
fulfilling this request.
exception
java.lang.NullPointerException
```

Condition: This problem occurs if the Content Engine does not have an explicit management IP address configured.

Workaround: Configure a management IP address for the Content Engine's Activation page.

- CSCed34718

Symptom: If you edit a file-based scheduled program and the Quality of Service (QoS) feature is configured, the revised program retains the QoS configuration even if you disable the QoS feature.

Condition: This problem occurs only with file-based scheduled programs; it does not occur with live programs.

Workaround: The only known workaround is re-creation. To remove the QoS configuration, delete the program and then re-create the program without configuring the QoS feature.
- CSCed46150

Symptom: The API program is created with multicast settings, with no multicast address ports specified within the program file. The program address pool is configured, including the pool TTL.

Condition: This problem occurs if the program multicast TTL is set to 255 instead of the address pool TTL value.

Workaround: Set the required TTL value within the program file.
- CSCed68360

Symptom: A constant stream of bandwidth error messages (one about every 2 seconds) is reported in the syslog. As the following sample messages indicate, these messages are not very useful.

```
Feb 11 13:24:26 webcache01 bandwd: %CE-BANDWD-3-115002: BANDWD: Trying again in two seconds
Feb 11 13:24:28 webcache01 bandwd: %CE-BANDWD-3-115003: BANDWD: verification registration failed, err=30
```

Condition: None.

Workaround: There is no known workaround.
- CSCed77655

Symptom: The Content Engine stops spoofing the client IP address, and uses its own IP address to fetch content from the origin server.

Condition: The **http i4-switch spoof-client-ip enable** global configuration command turns on IP spoofing on a Content Engine that is functioning as a caching engine. When a **rule action user-server** global configuration command is used, the Content Engine stops spoofing the client IP address and instead uses its own IP address to fetch the content.

Workaround: There is no known workaround.
- CSCed84227

Symptom: The network management system (NMS) host does not know where SNMP traps are coming from.

Condition: This problem occurs if there are two interfaces and you configure interface redundancy using both interfaces. You must use a dummy address for the physical addresses. You then configure a real address that floats between the two interfaces. If you then configure SNMP traps, the traps are being sourced from the dummy address and not the routable address. Therefore, the NMS host does not know where the trap is coming from.

Workaround: There is no known workaround.
- CSCee01453

Symptom: You experience problems when trying to add rules that have the pipe character (|).

Condition: You cannot add rules that contain the pipe character (|).

Workaround: To achieve the OR functionality, add multiple rules that do not contain the pipe character (|).

- CSCee19716

Symptom: The cache process restarts when the ICAP feature is enabled.

Condition: The problem occurs if the ICAP functionality is in an unstable state.

Workaround: Reboot the Content Engine to restart the ICAP daemon and bring it back to its normal state.

- CSCee40593

Symptom: Syslog messages contain the following text:

```
uns-server: %CE-CDNFS-0-480000: uns_read_meta: WOW! url mismatch: wanted '<URL>', swaw
'^C'
```

Condition: This problem occurs because of an apparent file system corruption; the cdnfs metadata files have the wrong content (the content is internally consistent but in the wrong file). This happens infrequently. For example, in this case, cdnfs content was being updated and a crash occurred because of a kernel panic (which occurs infrequently).

Workaround: Although there is no known workaround to stop the syslog messages shown above, lookups for the target URL listed in the syslog message may succeed if the ACNS software has created a new cdnfs entry for the target URL.

A way to test this is to use the **cdnfs lookup url EXEC** command and see if the URL is found. If the URL is not found, a way to force it to be replicated is to modify the file on the origin server (for example, by using the **touch** command on a UNIX-based origin server).

Alternatively, you can enter the **acquisition-distribution database-cleanup start** command on the affected Content Engine; this queries the cdnfs for all the objects that are supposed to be on the Content Engine. Missing objects should be detected and replicated.

- CSCee68339

Symptom: Proxy requests to the Content Engine proceed to allow mode (if allow mode is enabled) or are blocked (if allow mode is disabled) when the Websense URL filtering mechanism is configured to use the local Websense server.

Because the connections from the Content Engine to the Websense server time out, all requests go to allow mode until all 40 connections are exhausted. (This makes it appear as if the Websense server is not responding.) After all 40 connections are attempted, the Content Engine successfully connects to the Websense server and works properly thereafter.

Conditions: This problem can occur under the following conditions:

- The Content Engine is configured to use the local (internal) Websense server for URL filtering.
- The local Websense server is running on the Content Engine.
- There are long periods of inactivity.
- The cache process has difficulty connecting to the local Websense server.

Workaround: Reconfigure Websense URL filtering on the Content Engine so that the Content Engine will attempt to establish new connections to the Websense server.

- CSCef95723

Symptom: The local (internal) Websense server gets enabled on the Content Engine unexpectedly.

Condition: This problem occurs if the local Websense server is disabled and the IP address of the Content Engine is changed.

Workaround: Issue the **no websense-server enable** command to disable the local (internal) Websense server on the Content Engine.

- CSCei62672

Symptom: When you click links from the table of contents or the index of the ACNS Content Distribution Manager online help, the links open in the same pane, that is, the left pane, which contains the table of contents and the index, instead of opening in the right pane, which contains the help topics.

Condition: This problem occurs after you install Microsoft security update MS05-026. This security patch disables cross-frame navigation features that are based on HTML Help ActiveX control (HHCTRL).

Workaround: To reenabte cross-frame navigation features that are based on HHCTRL, modify your Windows registry as explained in Microsoft Knowledge Base article 896905, which is available at this URL:

<http://support.microsoft.com/kb/896905/>

- CSCin54434

Symptom: Websense Manager cannot connect to the local Websense server (the Websense server runs as a separate process on the Content Engine instead of running on a separate system).

Condition: This problem occurs if an external IP address is used from the Websense Manager to connect to the local Websense server (Version 5.0.1) that is running on the Content Engine.

Workaround: There is no known workaround.

- CSCin58464

Symptom: The Websense policy server and user server generate core files.

Condition: This problem occurs when the Websense server is running on ACNS 5.1.x software with a version of the Websense Manager that is earlier than Version 5.0.1 build 20030722. This problem does not exist when the Websense server is running on ACNS 5.0.3 software.

Workaround: Download Websense Manager Version 5.0.1 build 20030722.

- CSCin59084

Symptom: If there is a WCCP transparent proxy between the ACNS network root Content Engine and the content origin server, and the proxy requires NTLM authentication, then the ACNS network acquirer may fail to acquire content in the following scenario:

1. You specify the WCCP transparent proxy authentication information by using the **acquirer proxy authentication transparent** global configuration command. Content acquisition works correctly.
2. You remove the proxy authentication through the **no acquirer proxy authentication transparent** command. Content acquisition stops working, which is expected.
3. You restore proxy authentication using the **basic-auth-disable** option of the **acquirer proxy authentication** command. Content acquisition should work, but it does not. Content acquisition results in a 401 error message.

Condition: This occurs with ACNS 5.1.x software.

Workaround: Restart the acquirer through the **acquisition-distribution stop** and **acquisition-distribution start** commands.

- CSCin59100

Symptom: In ACNS 4.2 software, rules are configured only for HTTP and not for streaming protocols. If a Content Engine that is configured with rules and is running ACNS 4.2 software is upgraded to ACNS 5.1.x software, then these rules are configured with the protocol type “all.”

Condition: This occurs when the software is upgraded to ACNS software Release 5.1.x from ACNS software Release 4.2.

Workaround: If you do not want the rule to be applied for some of the rule actions, you can change the rule configuration as required.

- CSCin59462

Symptom: An FTP client application stops receiving data for a data transfer operation such as a directory listing (ls) or file transfer (GET). The same symptom can occur for FTP-over-HTTP data transfers from the FTP server to the Content Engine.

Condition: For FTP client applications, the Content Engine must be using the FTP proxy through WCCP redirection, configured for following the FTP client’s mode for establishing a data connection. The FTP client application must have also been set to use active mode to the FTP server.

```
ContentEngine(config)# wccp ftp router-list-num number
ContentEngine(config)# wccp version 2
ContentEngine(config)# ftp proxy active-mode enable
```

For FTP-over-HTTP data transfers, the Content Engine must be configured for an FTP incoming proxy and configured to use active mode to the FTP server. The client browser must be configured to use the Content Engine FTP proxy for FTP URLs.

```
ContentEngine(config)# ftp proxy incoming port
ContentEngine(config)# ftp proxy active-mode enable
```

The symptoms can occur with the configurations described above and when the FTP server starts sending data packets that are received out of order by the Content Engine before the Content Engine sends the TCP connection establishment SYN-ACK packet to the FTP server.

Workaround: Remove the Content Engine active mode configuration by issuing the following configuration command:

```
ContentEngine(config)# no ftp proxy active-mode enable
```

When this symptom occurs on an FTP client application, press **Ctrl-C** simultaneously to stop the partial data transfer operation.

When this symptom occurs on a browser configured for FTP-over-HTTP, click the **STOP** button to stop the partial data transfer operation.

- CSCin59581

Symptom: In ACNS 5.0 software, only “AND” is allowed between group of patterns with the same pattern list number. When you downgrade from ACNS 5.1 software to ACNS 5.0 software, the ORing of patterns configuration is not supported and is converted to ANDing of patterns. For example:

- Rule configuration in ACNS 5.1 software:

```
rule action block pattern-list 3 protocol http
rule pattern-list 3 url-regex sen
rule pattern-list 3 domain cisco
```

In ACNS 5.1 software, the default behavior is ORing of patterns.

- Rule configuration in ACNS 5.0 software:

```
rule action block pattern-list 3 protocol http
rule pattern-list 3 url-regex sen
rule pattern-list 3 domain cisco
```

In ACNS 5.0 software, the only behavior is ANDing of patterns.

Condition: The problem occurs when the configuration on the Content Engine has many pattern lists that are configured (ORed together) in ACNS 5.1 software and the Content Engine is downgraded to ACNS 5.0 software. Then only the first pattern-list configuration is used.

Workaround: There is no known workaround.

- CSCin59582

Symptom: After a Content Engine is downgraded from ACNS 5.1 software to ACNS 4.2 software, some patterns in the pattern list are lost. For example:

- Rule configuration in ACNS 5.1 software:

```
rule action block pattern-list 3 protocol http
rule pattern-list 3 url-regex sen
rule pattern-list 3 domain cisco
```

- Rule configuration in ACNS 4.2 software:

```
rule block url-regex sen
```

Condition: This problem occurs when the configuration on the Content Engine has many pattern lists that are configured (ORed together) in ACNS 5.1 software, and the Content Engine is downgraded to ACNS 4.2 software. Then only the first pattern-list configuration is used. All other pattern lists are lost.

Workaround: There is no known workaround.

- CSCin59781

Symptom: The cache process crashes while passing traffic for both the standard and the dynamic HTTPS service.

Condition: This problem can occur when heavy HTTPS traffic is passing through the Content Engine. Using standard and dynamic WCCP services and having the debug function enabled when HTTPS traffic is heavy may contribute to this problem.

Workaround: There is no known workaround. However, the cache process will restart and work normally after such a crash.

- CSCin60029

Symptom: When a rule with the **redirect** action is configured with a URL of 0 and with a matching pattern, the cache process crashes if the request matches the pattern.

Condition: This occurs when you configure a numeric value of 0 for the redirected URL (for example, if *www.yahoo.com* is redirected to 0). If you want the Content Engine to redirect URL *x* to URL *y*, then you can configure the **rule redirect** action. While doing so, you must configure URL *x* and URL *y*.

Workaround: There is no known workaround.
- CSCin65344

Symptom: When MPEG-2 is specified as the preferred format in a channel, programs cannot be created in that channel.

Condition: This problem occurs only if MPEG-2 is the preferred format.

Workaround: When MPEG-2 is chosen as the preferred format for a channel-based program, the default bandwidth is set to 1150 (the default for non-MPEG-2 programs). The default bandwidth for MPEG-2-based programs should be 2000 for MPEG-2 half duplex, and 3000 for MPEG-2 full duplex. Manually set the bandwidth while creating the program as follows:

 - If the preferred format is MPEG-2 half duplex, set the bandwidth to 2000.
 - If the preferred format is MPEG-2 full duplex, set the bandwidth to 3000.
- CSCin65854

Symptom: If Quality of Service (QoS) for MP2T audio-only programs is set, QoS parameters are not included in the Session Description Protocol (SDP) information for the program. Consequently, the MP2T stream is streamed without the intended QoS characteristics.

Condition: The problem is observed with MP2T audio-only programs and when the audio QoS option is specified.

Workaround: There is no known workaround.
- CSCin67818

Symptom: The manifest validator fails to fetch the XML file if the source is authenticated.

Condition: This problem occurs only if the file is located at an authenticated location.

Workaround: Put a copy of the manifest file in a nonauthenticated location to use the manifest validator.

Resolved Caveats - ACNS Software, Release 5.1.11

This section lists caveats that have been resolved in ACNS software, Release 5.1.11.

- CSCea40786
The status of a content item on the root Content Engine appears as “Error-Valid” when the object is initially acquired. The status should be “Pending.” Eventually the status is reported as either “Complete” or as a “Error -”, followed by an error description.
- CSCec52034
Clients are unable to access a program during its scheduled playback time. The cms_CE service logs an error indicating a failure to create a unified name space (UNS) entry. This problem occurs if a program is configured either through the Content Distribution Manager GUI or the API.
- CSCec66169
If you remove an active ICAP service while there are active connections to the ICAP server for this service, the ICAP daemon on the Content Engine generates a core file and restarts.
- CSCed44027
The **dns enable** command does not turn on the DNS service on a routing Content Engine.
- CSCed67142
If the Content Engine is running ACNS software, Release 5.1, and error logging is enabled on it, the log files in the error log can contain junk entries.
- CSCee19712
When the ICAP service is running on the Content Engine, clients can receive “502 Bad Gateway” error messages. The burst of errors continues for approximately 10 to 12 seconds, stops, and then recurs within a few hours.
- CSCee29257
If you execute the **show** and **clear EXEC** commands for a registered Content Engine from a Content Distribution Manager, these commands can fail and report a “Transaction not completed” error on the Content Distribution Manager. This problem occurs if Websense URL filtering or N2H2 URL filtering is enabled on the Content Engine.
- CSCee31443
On a slow link (for example, 11 kbps), when the load monitor is in load bypass because of other HTTP traffic, the FTP control connections are handled correctly; however, the FTP data connections experience a 20-second delay before rejecting the data connection.
- CSCee49434
The Content Distribution Manager only has a blank SNMP configuration for a device (that is, no settings for the SNMP configuration or no setting for its children class) because the device configuration that you had performed through the Content Distribution Manager GUI in the Device window is removed by local central management (LCM).
- CSCee50470
Proxy requests that include the request header “Expect: 100-continue” fail and a “417 Expectation Failed” response code is generated.

- CSCee82855

The cms_ce service fails to start up. The local1/service_logs/cms_ce_start_log_latest file shows a message such as the following:

```
Jun 11 15:18:59 iop-cdm-ce1 java: %CE-CMS-0-700003: java.net.BindException: Address
already in use:
  java.net.BindException: Address already in use at
  java.net.PlainSocketImpl.socketBind(Native Method)
  at java.net.PlainSocketImpl.bind(PlainSocketImpl.java:331)
  at java.net.ServerSocket.bind(ServerSocket.java:309)
  at java.net.ServerSocket.<init>(ServerSocket.java:183)
  at unicorn.RpcTcpServer.<init>(RpcTcpServer.java:31)
  at com.cisco.unicorn.dbvacuum.DbVacuum.<init>(DbVacuum.java:153)
  at com.cisco.unicorn.dbvacuum.DbVacuum.<clinit>(DbVacuum.java:52)
  at com.cisco.unicorn.director.Server.init(Server.java:287)
  at com.cisco.unicorn.server.AServer.main(AServer.java:990)
```

- CSCee83867

Objects that are protected with basic authentication are served from the Content Engine cache without being queried for authentication credentials. This problem can occur if all the following conditions exist: (1) the Content Engine is configured to use the basic authentication method to authenticate HTTP requests, (2) server-side persistent connections are enabled, and (3) the origin server is a Microsoft IIS 4.0 or IIS 5.0 server.

- CSCee89688

When you use the Content Distribution Manager GUI to remove device group settings (**Streaming/Caching > Client Proxy Auto Configuration**), any devices that had these settings applied through the CLI retain the enabled setting.

- CSCef08399

The Java monitor in the Content Engine GUI does not show statistics of all of the Content Engines that are using the same WCCP-enabled router. The Content Engine GUI only shows statistics for the Content Engine from which you accessed the Content Engine GUI.

- CSCef08806

With WMT proxy caching, an incorrect video on demand (VOD) could be served if it is accessed through a fixed URL that actually points to dynamically changed content. This problem only occurs when a dynamically changed content referred by a static URL is involved and the content has already been cached.

- CSCef09244

The Content Engine may not set the Don't Fragment (DF) bit in the IP header even though by default discovery of the Path MTU should be enabled. This problem can occur if the Content Engine is reloaded and the **ip path-mtu-discovery enable** global configuration command is not used.

- CSCef09719

The cache process restarts while mixed traffic (HTTP and HTTPS traffic) is being directed to the Content Engine.

- CSCef11301

The **show statistics distribution mcast-data-sender detail EXEC** command shows that the multicast sender is not making any progress even though several files are ready to be sent. This problem occurs if multicast is enabled on a multicast sender and the Content Engine clock has been changed.

- CSCef12284

When you have issued the **http cache vary-user-agent enable** command on the Content Engine, certain websites that do not behave consistently with regard to HTTP responses for the “Vary:” HTTP header can cause the HTTP caching application on the Content Engine to abort and restart.
- CSCef12507

The Content Engine does not clear WMT cached content and reports an error message.
- CSCef12939

The ICAP service restarts on the Content Engine. This problem can occur if there is a heavy load on the Content Engine and an ICAP server error occurs.
- CSCef13631

The CMS service fails to start, and the syslog.txt file contains messages such as the following:

```
Tue Jul 13 01:57:32 UTC 2004 [E] main: java.net.BindException: Address already
in use: java.net.BindException: Address already in use
    at java.net.PlainSocketImpl.socketBind(Native Method)
    at java.net.PlainSocketImpl.bind(PlainSocketImpl.java:331)
    at java.net.ServerSocket.bind(ServerSocket.java:309)
    at java.net.ServerSocket.<init>(ServerSocket.java:183)
    at unicorn.RpcTcpServer.<init>(RpcTcpServer.java:31)
    at com.cisco.unicorn.consumerAdaptor.ConsumerAdaptorImp.<init>
(ConsumerAdaptorImp.java:606)
    at com.cisco.unicorn.consumerAdaptor.ConsumerAdaptorImp.only
(ConsumerAdaptorImp.java:101)
    at com.cisco.unicorn.director.Server.init(Server.java:201)
    at com.cisco.unicorn.server.AServer.main(AServer.java:990)
```
- CSCef16964

When a web page is NTLM-protected and the links on the page point to a different origin server than the one from which the web page is retrieved, clients receive a 400 Bad Request error message when they attempt to access such links on the page.
- CSCef17473

The multicast cloud information for the sender Content Engine, which was configured through the Content Distribution Manager GUI, is not correctly reflected on the sender Content Engine. This problem occurs if the Content Engine was previously configured as the backup sender and then reconfigured as the primary sender for this cloud.
- CSCef20981

The Content Engine cannot serve MPEG-4 content to a Mood Player, which is a set top-based media player.
- CSCef21539

The CMS service cannot start on the standby Content Distribution Manager. This problem can occur if there are a large number of system messages in the Centralized Management System (cms) database table.
- CSCef21995

If you downgrade a Content Distribution Manager from ACNS software, Release 5.1 to Release 5.0, the Content Distribution Manager keeps sending full updates to all registered Content Engines.

- CSCef22597
The output of the **show rule action use-icap-service EXEC** command displays incorrect information about the ICAP service. This problem occurs if you configure more than one **rule action use-icap service** that uses the same pattern list number and if one of these rules is unconfigured.
- CSCef23273
Certain Windows Media files that contain markers with or without embedded scripts cannot be acquired through the MMS streaming protocol.
- CSCef24057
The ICAP service on the Content Engine restarts. This problem can occur if you remove or add numerous ICAP servers to an ICAP service.
- CSCef25496
The CMS process does not update the stream scheduler if the parent location is changed. This problem only occurs if you edit the parent location through the Content Distribution Manager GUI.
- CSCef27105
When you display the detailed Replication Status window in the Content Distribution Manager GUI, a null pointer exception occurs that causes the CMS process to restart.
- CSCef27367
If the HTTP persistent-connections timeout is set so high that the maximum number of file descriptors is exhausted, then no additional files can be opened. If no additional files can be opened, file errors occur if you perform such basic operations as showing the running configuration (using the **show running-config EXEC** command).
- CSCef27419
When the Content Engine is part of a device group, the Content Engine configuration partially disappears. In the Content Distribution Manager GUI, the Content Engine configuration window indicates that the Content Engine is being managed locally as opposed to being managed centrally through the device group.

This problem occurs if the Content Engine exhausts file descriptors, which results in incomplete output of the **show running-config EXEC** command. This causes local central management to think that the configuration of the Content Engine has been changed locally, and it sends that change to the Content Distribution Manager, where it is recorded as a local override.
- CSCef28214
The ICAP service on the Content Engine restarts. This problem can occur after you add or remove a number of ICAP servers for an ICAP service.
- CSCef29584
If the Content Engine is operating in proxy mode, it can stop accepting connections, or if the Content Engine is operating in WCCP mode, it can go in and out of overload bypass mode. If this problem occurs, syslog messages such as the following are reported:


```
Thread 1 really low memory
or
Thread 2 really low memory
```
- CSCef30460
The CPU consumption on the Content Engine is at 100 percent. The problem only occurs when artificially generated malformed packets resemble the patterns of fragmented generic routing encapsulation (GRE) packets.

- CSCef30670
The ICAP process crashes on the Content Engine. This problem can occur if the ICAP process that is running on the Content Engine receives some bad data from the external ICAP server. However, the ICAP process automatically restarts on its own.
- CSCef33557
The RTSP proxy fails to serve the content for RTSP links (rtsp://). This problem can occur if the Content Engine is acting as the RTSP proxy and RealMedia files are being played.
- CSCef34798
Certain TN3270 applications (that is, “green screen” applications) time out and hang. This problem can occur if the TN3720 application is going through a Content Engine.
- CSCef35485
Persistent server and client HTTP connections are terminated prematurely. This problem occurs if the server responds to an HTTP revalidation request (If-modified-since) with a 304 Not modified response and does not provide the object length.
- CSCef35559
If an HTTP request must be authenticated by a remote server and a Content Engine is being used, the Citrix client application fails to launch.
- CSCef39962
With HTTP authentication enabled on a Content Engine, there might be problems with authenticating users. This problem can occur if there is a hierarchy of Content Engines and the upstream Content Engine includes the X-Forwarded-For header. In this case, the downstream Content Engine indexes the HTTP authentication cache correctly. The Content Engine indexes the HTTP authentication cache through the client’s IP address in transparent mode but when the X-Forwarded-For header is present, the Content Engine does not save the correct IP address.
- CSCef42949
End users experience slowness in their HTTP requests.
- CSCef44042
Broken links and images or an error message is returned, indicating that the server is busy.
- CSCef50009
The status of the disk drive on the Content Engine is reported as “Problematic.” The drive firmware is sending a reset to the drive and the ACNS software is not restarting the drive after the reset.
- CSCef55480
The WMT process crashes and generates a core file when the WMT proxy receives a malformed packet over MMS-over-HTTP.
- CSCef58506
The Content Engine Network Module can report disk errors over time. These errors indicate that the “ECC Uncorrectable” error message is the most commonly reported error message.
- CSCef60023
The message “Unsolicited _Ftp_Ipc CloseDataSess_Cb cb_err -1” appears in the FTP error log file, which is in the errorlog/ftp-ctlproxy-errorlog.current directory. This problem occurs because of an error condition on the socket connection between the FTP process and the cache process.

- CSCef60602

The output of the **show statistics EXEC** commands shows error messages such as the following:

```
Internal Error: item not found in dataserver
Http requests are not served.
Unit recovers only by reload.
```

This problem can occur if you have configured URL filtering with a custom blocking message on the Content Engine.

- CSCef60783

After you upgrade from ACNS software, Release 5.0 to Release 5.1, in a large installation (over 1000 Content Engines) the Content Distribution Manager GUI is slow to respond. It can take approximately 30 seconds to display the complete list of devices in the Content Distribution Manager GUI, or to switch between device configuration windows.

- CSCef61952

TV-out functionality does not work on newer properly equipped CE-510 and CE-565 models because a newer revision of the audio video (AV) hardware is used. The **show hardware** or **show tvout EXEC** commands identify the affected units:

```
[***Revision not supported in this version of software***]
or
[***Hardware revision level not supported in this version of software***]
```

- CSCef65579

When HTTP authentication is enabled, the syslog.txt file receives an error message indicating that servers are dead. This problem occurs if an HTTP request is authenticated by LDAP or TACACS+ servers.

- CSCef66019

Rebroadcast programs may not play the list of files in the sequence desired. This problem can occur with all rebroadcast programs, because the media index attribute is not currently being.

- CSCef66974

After the time on the Content Engine has been changed, WCCP communication for the Real-Time Streaming Protocol (RTSP) WCCP service does not work. This problem occurs if you set the time on the Content Engine to a time that is earlier than the current time.

- CSCef71971

MMS-over-HTTP requests with proxy authentication can fail if there is a proxy chain and proxy authentication with LDAP is enabled on the Content Engines in the proxy chain.

- CSCef72422

The Content Distribution Manager GUI is slow, and thousands of syslog messages appear in the Content Distribution Manager GUI. This problem can occur if a Content Engine is sending an enormous number of syslog messages to the Content Distribution Manager, which forces the Content Distribution Manager to handle and log all of these messages.

Documentation Updates

This section describes documentation updates.

- [TACACS+ Enable Password Attribute](#)
- [Pre-Positioned Content](#)
- [Configuration Requirements for Managed Live Events](#)
- [cdn-url Attribute Description](#)
- [Multicast Sender Interoperability](#)
- [FTP Caching Support](#)
- [Group-Type Patterns in Rule Pattern Lists](#)
- [SmartFilter Software and the rule action no-auth Command Rule Interaction](#)
- [Bandwidth Configuration for Interfaces and Content Services](#)
- [pace Command](#)
- [pre-load Command](#)
- [NTLM Preload Support](#)
- [show statistics icap Command](#)
- [Default Port of the Content Engine GUI](#)
- [Playing Nonhinted IP/TV On-Demand Programs over an ACNS Network](#)
- [Restriction on IP/TV Program Manager Configuration](#)

TACACS+ Enable Password Attribute

This documentation update applies to the following three ACNS Release 5.1 software guides:

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*
- *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*
- *Cisco ACNS Software Command Reference, Release 5.1*

The ACNS software CLI EXEC mode is used for setting, viewing, and testing system operations. It is divided into two access levels, user and privileged. To access privileged-level EXEC mode, enter the **enable** EXEC command at the user access level prompt and specify a privileged EXEC password (superuser or admin-equivalent password) when prompted for a password.

In TACACS+ there is an “enable password” feature that allows an administrator to define a different enable password for each user. If an ACNS user logs in to the Content Engine with a normal user account (privilege level of 0) instead of an admin or admin-equivalent user account (privilege level of 15), the user must enter the admin password in order to access privileged-level EXEC mode.

```
ContentEngine> enable
Password:
```

This caveat applies even if these ACNS users are using TACACS+ for login authentication.

Pre-Positioned Content

This documentation update applies to the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.

In ACNS 5.1.x software earlier than Release 5.1.5, pre-positioned content is served only on ports that are standard for the protocol. If the incoming URL contains a port number other than the standard port for that protocol (for example, HTTP uses port 80, RTSP uses port 554, and WMT uses port 1755), then the Content Engine does not attempt to serve the content from the pre-positioned file system (cdnfs). Instead, the Content Engine tries to serve the content from the cache file system (cfs) or tries to fetch the content from the origin server, depending on the existing configuration of the Content Engine.

In ACNS software, Release 5.1.5, the *ignoreOriginPort* attribute was added to support the playback of pre-positioned content using nonstandard ports. The *ignoreOriginPort* attribute controls content playback and allows the use of nonstandard ports to play back pre-positioned content. In releases of ACNS software prior to Release 5.1.5, playback of pre-positioned content using nonstandard ports was not supported.

The *ignoreOriginPort* attribute is supported under the following tags in the manifest file:

- <options> tag
- <item> tag
- <crawler> tag
- <item-group> tag

The *ignoreOriginPort* attribute is optional. Valid values for the *ignoreOriginPort* attribute are *true* or *false*. The default is *false*. In the following example, the *ignoreOriginPort* attribute is specified in the <item> tag and is set to *true*.

```
<item src="<http://10.77.155.211/abc.html>http://10.77.155.211/abc.html"
ignoreOriginPort="true" />
```

If an item is acquired with the attribute set to *true* (*ignoreOriginPort=true*), then the content is played back even if the incoming URL that was used to request the content contains a nonstandard port. For example, if content is acquired as:

```
<http://www.foo.com/abcd.xml>http://www.foo.com/abcd.xml
```

then the content can be played back as:

```
<http://www.foo.comXXXX/abcd.xml>http://www.foo.comXXXX/abcd.xml
```

where XXXX is the port number.

For more information about using a manifest file to acquire and distribute content in an ACNS 5.1 network, refer to Chapter 7, “Creating Manifest Files,” in the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.

Configuration Requirements for Managed Live Events

This documentation update applies to the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.

If you have channels for live programs configured in your ACNS 5.1 network, make sure that there are no external proxy servers physically located between your ACNS 5.1 receiver Content Engines and your ACNS 5.1 root Content Engine that require proxy authentication. Also, make sure that proxy authentication is not enabled on any receiver Content Engines that might be in the logical, hierarchical path between the root Content Engine and the receiver Content Engine that is going to serve the live stream to the requesting clients. If a live stream encounters any device that requires proxy authentication, the stream will be dropped before it reaches its destination.

If your network is set up with intermediary devices that require proxy authentication, you can work around the problem by configuring rules to bypass authentication on these devices.

For example, to enable the formation of a unicast splitting tree and, in turn, enable live broadcasting from all receiver Content Engines, you can specify the following rule on all of the parent Content Engines in the channel:

```
ContentEngine(config)# rule pattern-list 1 downstream-CE-ipaddress
ContentEngine(config)# rule no-auth pattern-list 1
```

cdn-url Attribute Description

This documentation update applies to the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.

With ACNS software, you can use *cdn-url* as an optional attribute of distributed content. This option only works when the media is pre-positioned on the Content Engine and the origin server does not have to be contacted for any reason to fulfill the request. You cannot use the *cdn-url* attribute if the origin server needs to be contacted to fulfill the request, for example, in such situations as the following:

- Authenticated requests for pre-positioned content
- Redirection to an origin server (for example, if the pre-positioning is incomplete)
- Live streaming and splitting



Note

Do not use the *cdn-url* attribute in the specified situations.

On page 7-44, replace the bulleted item under the “Item” section with the following.

- *cdn-url*

The *cdn-url* attribute is optional and is used when content needs to be acquired from one URL (the content acquisition URL) and published using another URL (the publishing URL). The *cdn-url* attribute is the relative ACNS network URL that end users use to access this content. If no *cdn-url* attribute is specified, then the *src* attribute is used as the relative ACNS network URL.

In the following sample manifest file, the content item being acquired contains the file path `/RemAdmin/InternalReview/firstpage.htm`. By specifying a new file path (`RemAdmin/Production/firstpage.htm`) using the `cdn-url` attribute, the publishing URL disguises the fact that the content originated from an internal review.

```
<CdnManifest>
<server name="ultra-server">
  <host name="http://ultra-server" />
</server>
<item src="RemAdmin/InternalReview/firstpage.htm"
cdn-url="RemAdmin/Production/firstpage.htm" />
</CdnManifest>
```

In the preceding example, `src` is the content acquisition URL and `cdn-url` is the publishing URL.



Note The content item file path (`RemAdmin/InternalReview/firstpage.htm`) is controlled by the manifest file. The `cdn-url` attribute associates a file path with the content item in the manifest file. The manifest file allows the file path for the `cdn-url` attribute to be specified independently of the file path from which the content items are to be acquired from the origin server (`src` attribute), allowing the publishing URL to differ from the content acquisition URL. (Refer to the “Generate the Publishing URL” section on page 6-9 in the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.)

If the content is live or requires playback authentication, the origin server from which the content is acquired must be contacted. Therefore, two URLs must exist for the same content item, and the URL specified in the `cdn-url` attribute must exist on the origin server at all times.

For example, if the content item “`RemAdmin/Production/firstpage.htm`” requires playback authentication, this content must exist on the “ultra-server” origin server. Otherwise, pre-positioned content playback will fail.

In general, you should not use the `cdn-url`, `cdnPrefix`, or `srcPrefix` attributes if playback authentication is required or if the content is live.

If you use FTP to acquire content and the content type is not specified in the manifest file and the `cdn-url` attribute is used to alter your publishing URL, the `cdn-url` attribute must have the correct file path extension (for example, `.jpg`). Otherwise, the incorrect content type will be generated and you cannot play the content.

The following example correctly shows the publishing URL with the same file path extension (`.jpg`) as that of the origin server URL.

```
<item src="ftp://ftp-server.abc.com/pictures/pic.jpg" cdn-url="pic.jpg" />
```

The following example is incorrectly written, because it does not specify the file path extension (`.jpg`) in the `cdn-url` attribute.

```
<item src="ftp://ftp-server.abc.com/pictures/pic.jpg" cdn-url="pic" />
```

Multicast Sender Interoperability

This documentation update applies to the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*. The following is additional information regarding multicast sender interoperability.

- Condition 1: The ACNS network is set up for multicast distribution with Content Engines subscribed to multicast-enabled channels. Multicast sender and receiver Content Engines are running mixed versions of ACNS software. All Content Engines have been successfully enabled for multicasting. The Content Distribution Manager is running ACNS 5.1.x software.

Symptom:

- Only senders running ACNS 5.1.x software support failover to a backup sender. Only receivers running ACNS 5.1.x software can send negative acknowledgements (NACKs).
- If both the primary sender and the backup sender are actively sending the same file, the receiver Content Engine locks out one of the two and receives one copy of the file from the first sender.



Note Cases 1 through 6 assume that you are using a Content Distribution Manager that is running ACNS 5.1.x software.

Case 1: The primary sender is using an ACNS software release earlier than ACNS 5.1.x. The backup sender is using ACNS 5.1.x software, as is the receiver.

- The backup sender considers the primary sender inactive and becomes active after the configured failover period.
- The primary sender periodically sends multicast files as configured in the carousel pass and multicast-out bandwidth settings.
- The receiver tries to send a NACK to the primary sender, but receives NACK failures and begins sending NACKs to the backup sender. The backup sender responds to the NACK.

Case 2: Both the primary sender and the backup sender are using ACNS 5.1.x software. The receiver is using an ACNS software release earlier than ACNS Release 5.1.x.

- Failover works between the primary and backup senders, but neither the primary sender nor the backup sender ever receives a NACK response from the receiver.
- The primary sender sends out the first carousel pass for content without the need for a NACK, so the receiver might be able to obtain content if it joins the group promptly. If it does not, the receiver is not able to obtain content.

Case 3: Both the primary sender and the receiver are using an ACNS software release earlier than ACNS Release 5.1.x. The backup sender is using ACNS 5.1 software.

- The backup sender considers the primary sender inactive and becomes active after the configured failover grace period. The backup sender continues to wait for a NACK response from the receiver before sending the multicast, but the receiver is unable to send a NACK.
- The primary sender periodically sends multicast files as configured in the carousel pass and multicast-out bandwidth settings.
- The receiver should be able to obtain content from the primary sender.

Condition 2: Although you may have received a warning message from the Content Distribution Manager, you can still configure a Content Engine as a backup sender if the Content Engine is registered with a Content Distribution Manager running ACNS 5.1.x software and the Content Engine is running ACNS software earlier than ACNS Release 5.1.x. Cases 4 through 6 discuss the backup sender operating under these conditions.

Symptom: The Content Distribution Manager does not send related configuration information and configuration changes to the Content Engine running the earlier software version. This results in the the Content Engine not being able to identify itself as the multicast backup sender. This scenario might also occur if a backup sender using ACNS 5.1.x software is downgraded to an earlier software version through the Content Engine CLI.

Case 4: Both the primary sender and the backup sender are using an ACNS software release earlier than ACNS Release 5.1.x. The receiver is running ACNS 5.1 software.

- The receiver alternates attempts to send NACKs between the primary sender and the backup sender but is unsuccessful.
- The primary sender periodically sends multicast files as configured in the carousel and multicast-out bandwidth settings.

Case 5: The primary sender and the receiver are using ACNS 5.1 software. The backup sender is using an ACNS software release earlier than ACNS Release 5.1.x.

- The primary sender considers the backup sender inactive after the configured failover grace period.
- The receiver can successfully send NACKs only to the primary sender. If the primary sender fails, the receiver sends the NACKs to the backup sender, and when it receives a NACK failure as expected, the receiver retries the primary sender. The receiver alternates sending NACKs between the senders until the primary sender becomes active again.

Case 6: The primary sender is using ACNS 5.1.x software. Both the backup sender and the receiver are using an ACNS software release earlier than ACNS Release 5.1.x.

- The primary sender considers the backup sender inactive and becomes active after the configured failover grace period. The primary sender sends the first carousel pass of content without needing to receive a NACK. The primary sender then waits for the receiver's NACK to trigger further carousel passes if more than one carousel pass is configured.
- The receiver never sends a NACK to the primary sender or the backup sender.

Condition 3: The Content Distribution Manager is using an ACNS software release earlier than ACNS Release 5.1.x. In software releases earlier than ACNS Release 5.1.x, only one sender is configurable for each multicast cloud.

Case 7: The sender is using ACNS 5.1.x software. The receiver is using a software release earlier than ACNS Release 5.1.x.

The sender behaves like a primary sender running ACNS 5.1.x software. That is, it sends the first round of content without requiring a NACK to trigger the carousel pass. However, the sender is unable to continue making carousel passes because the receiver is unable to send NACKs.

Case 8: Both the sender and the receiver are using ACNS 5.1.x software.

The sender is able to perform carousel passes and the receiver is able to send NACKs for missing content; however, there is no support for a backup sender or for configuring the NACK interval multiplier.

Case 9: The sender is using an ACNS software release earlier than ACNS Release 5.1.x. The receiver is using ACNS 5.1.x software.

- The sender periodically sends multicast files as configured in the carousel pass and multicast-out bandwidth settings so that the receiver can obtain content.
- The receiver tries to send NACKs to the sender but continually fails and retries.

Workaround for Cases 1 through 9: Upgrade both senders and receivers to ACNS 5.1.x software. Upgrade the sender first, and then upgrade the receivers.

Workarounds for Case 7 only:

- Use the **distribution multicast resend** EXEC command on the sender Content Engine to trigger a multicast carousel pass manually.
- Upgrade both senders and receivers to ACNS 5.1.x software. Upgrade the sender first, and then upgrade the receivers.

FTP Caching Support

This documentation update applies to the following three ACNS 5.1 software guides unless otherwise stated:

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*
- *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*
- *Cisco ACNS Software Command Reference, Release 5.1*

A Content Engine that is running ACNS 5.1 software can be configured for FTP caching in either of the following two usage modes:

- **FTP-over-HTTP mode.** The Content Engine (nontransparent proxy server) caches the contents of the specified FTP URLs that are sent to it directly by clients that are using the HTTP protocol. This allows users to use their browsers (HTTP protocol) to access files (to send and receive files) on remote FTP servers.
- **Native FTP mode.** The Content Engine (transparent proxy server) caches the contents of the FTP requests that are sent from clients in the native FTP protocol.

In both of these usage modes, the Content Engine uses the FTP protocol to retrieve and locally cache the content of the FTP requests. These two usage modes differ in the protocol used by the client to issue the FTP request. In FTP-over-HTTP mode, clients use their browsers (the HTTP protocol) to issue FTP requests. In native FTP mode, clients use the native FTP protocol to issue FTP requests, as shown in the following example:

```
ContentEngine# ftp server.cisco.com
```



Note

In ACNS 5.1 software, native FTP caching is only supported in transparent proxy mode; it is not supported in nontransparent proxy mode. In ACNS 5.1 software, transparent redirection of FTP requests is supported only by WCCP Version 2; transparent redirection through a Layer 4 switch is not supported.

Native FTP requests are logged in the HTTP transaction log on the Content Engine.

FTP-over-HTTP Caching Support

The ACNS 5.1 software supports proxying and caching of FTP URL client requests using proxy-mode HTTP requests when URLs specify the FTP protocol (for example, *ftp://ftp.mycompany.com/ftkdir/ftp_file*). For instance, the following is an example of an FTP-over-HTTP request that allows the end user to use a browser to access public files from an FTP server:

```
ftp://ftp.funet.fi/pub/cbm/crossplatform/converters/unix/
```

For these requests, the client uses HTTP as the transport protocol with the Content Engine, whereas the Content Engine uses FTP with the FTP server. When the Content Engine receives an FTP request from the web client, it first looks in its cache. If the object is not in its cache, it fetches the object from an upstream FTP proxy server (if one is configured), or directly from the origin FTP server.

The FTP proxy supports anonymous as well as authenticated FTP requests. Only base64 encoding is supported for authentication. The FTP proxy accepts all FTP URL schemes defined in RFC 1738. In the case of a URL in the form `ftp://user@site/dir/file`, the proxy sends back an authentication failure reply and the browser supplies a popup window for the user to enter login information.

The FTP proxy supports commonly used MIME types, attaches the corresponding header to the client, chooses the appropriate transfer type (binary or ASCII), and enables the browser to open the FTP file with the configured application. For unknown file types, the proxy uses binary transfer as the default and instructs the browser to save the downloaded file instead of opening it. The FTP proxy returns a formatted directory listing to the client if the FTP server replies with a known format directory listing. The formatted directory listing has full information about the file or directory and provides the ability for users to choose the download transfer type.

Native FTP Caching Support

On page 2-8 of the *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*, and on page 2-120 (“Usage Guidelines”) of the *Cisco ACNS Software Command Reference, Release 5.1* publication, replace the information about native FTP caching with the following information.

The Content Engine operating as an FTP proxy supports passive and active mode for fetching files and directories. In native FTP caching mode, if the **ftp proxy active-mode enable** global configuration command is used, then the Content Engine uses the same mode with the FTP server for the data connection as the client used to reach the Content Engine, which can be either active or passive. If the **ftp proxy active-mode enable** command is not used, the Content Engine uses passive mode with the FTP server for the data connection.

As the following partial output of the **show ftp** command shows, if you have used the **ftp proxy active-mode enable** command, the Content Engine (the nontransparent proxy server that is functioning as a native FTP proxy server) adheres to the client’s mode (active or passive):

- The Content Engine (the native FTP proxy server) performs an active-mode data transfer to or from the FTP server if the FTP client issues an active-mode data transfer request.
- The Content Engine performs a passive-mode data transfer to or from the FTP server if the FTP client issues a passive-mode data transfer request.

```
ContentEngine# show ftp

FTP Configuration
-----

WCCP FTP service status:           ENABLED
Maximum size of a FTP cacheable object: 204800 KBytes
FTP data connection mode with Server: Adhere to Client's mode (active or passive)
```

Note that the format of the URL that the Content Engine (nontransparent proxy server that is functioning as a native FTP proxy server) creates for a native FTP request depends on the FTP login name and the transfer mode (binary or ASCII file transfer mode).

- If the FTP login name is an actual username instead of “anonymous,” then the string “*user*:*password*@” is included in the URL before the host.

- If the mode used to transfer the file is binary mode, then the string “;type=i” is included at the end of the URL. The following is an example of the URL format that the Content Engine creates for a specific user when binary mode is being used.

```
ftp://*user*:*password*@10.100.200.5/home/myhome/mybinfile.obj;type=i
```

The URL for an “anonymous” user login and an ACSII file transfer mode will not have any fields embedded in the URL, as shown in the following example:

```
ftp://10.100.200.5/home/myhome/mytextfile.txt
```

The following two examples demonstrate the use of native FTP with a Content Engine. In the first example, the user logs in with an actual username name (“huff”) and is able to retrieve the requested file (test.c) from the FTP server. Note that in this case, the current directory for the user named “huff” is “/home/huff.”

```
ContentEngine# ftp server.cisco.com
Connected to server.cisco.com.
220 server.cisco.com FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.
Name (server:huff): huff
331 Password required for myserver.
Password:
230 User huff logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/huff" is current directory.
ftp> get /tmp/test.c
200 PORT command successful.
150 Opening BINARY mode data connection for /tmp/test.c (645 bytes).
226 Transfer complete.
645 bytes received in 0.00077 seconds (8.2e+02 Kbytes/s)
ftp> quit
ContentEngine#
```

In the second example (shown below), the user logs in as an anonymous user and cannot retrieve the requested file (test.c) because the file is not located in the document root directory of the FTP server (“/”), which is the current directory for any anonymous user.

```
ContentEngine# ftp server.cisco.com
Connected to server.cisco.com.
220 server.cisco.com FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.
Name (server:huff): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password: test@cisco.com
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is current directory.
ftp>
ftp> passive
Passive mode on
ftp> get
(remote-file) /tmp/test.c
(local-file) test.c
local: test.c remote: /tmp/test.c
227 Entering Passive Mode (172.31.255.255)
550 /tmp/test.c: No such file or directory.
ftp>
ContentEngine#
```

In ACNS 5.1 software, the **wccp ftp router-list-number** and **wccp ftp mask** global configuration commands were added to support native FTP caching on a Content Engine that is operating in transparent proxy mode.

The **wccp ftp** command is used to configure the WCCP interception of FTP protocol traffic from FTP clients to FTP servers.

```
ContentEngine(config)# wccp ftp ?
  mask                Specify mask used for CE assignment
  router-list-num     Router list number
ContentEngine(config)# wccp ftp mask ?
  dst-ip-mask        Specify sub-mask used in packet destination-IP address
  src-ip-mask        Specify sub-mask used in packet source-IP address
ContentEngine(config)# wccp ftp router-list-num ?
  <1-8>              Router List Number
```

The following example shows how to configure native FTP caching on a WCCP Version 2 router:

1. Turn on native FTP caching. The service group number for this service is 60.

```
Router(config)# ip wccp 60
```

2. Specify an interface on which the native FTP caching service will run.

```
Router(config)# interface type number
```

3. Configure the router to use the outbound interface for the FTP caching service.

```
Router(config-if)# ip wccp 60 redirect out
```

The associated **show wccp services EXEC** command was modified in ACNS software, Release 5.1 to show the configuration information associated with the FTP proxy.

```
ContentEngine# show wccp services
Services configured on this Content Engine
  Web Cache
  Custom Web Cache
  FTP Cache
  RTSP
```

The **show wccp modules EXEC** command was modified in ACNS software, Release 5.1 to include an entry for the FTP caching service:

```
ContentEngine# show wccp modules

Modules registered with WCCP on this Content Engine

ModuleSocketExpire(sec)NameSupported Services
-----
5   6   3FTP ProxyFTP Cache

1   7   3RTSP ProxyRTSP

0   8   3HTTP ProxyWeb Cache
Reverse Proxy
Custom Web Cache
WCCPv2 Service 90
WCCPv2 Service 91
WCCPv2 Service 92
WCCPv2 Service 93
WCCPv2 Service 94
WCCPv2 Service 95
WCCPv2 Service 96
WCCPv2 Service 97
```

```
ContentEngine# show wccp masks ?
  custom-web-cache Custom web caching service
  ftp              FTP Proxy caching service
  reverse-proxy   Reverse Proxy web caching service
  rtsp            Media caching service
  web-cache       Standard web caching service
```

For more information about these commands, refer to the *Cisco ACNS Software Command Reference, Release 5.1*.

Restrictions Regarding Native FTP Caching in ACNS 5.1 and 5.1.x Software

Restrictions regarding native FTP caching support in ACNS 5.1 and 5.1.x software are:

- Maximum FTP object size of 200 megabytes
- No support for bandwidth control for FTP client requests and FTP server pulls
- No support for the Type of Service (ToS) bit for FTP client requests
- No support for pre-positioned files in the cdnfs
- No support for the Internet Content Adaptation Protocol (ICAP)
- No support for nontransparent proxy
- No support for proxy authentication
- No support for the Internet Cache Protocol (ICP)
- No support for healing mode
- No support for Layer 4 switch FTP redirection
- No support for FTP request proxy rules
- No support for MIN-TTL and AGING-HEURISTIC-TTL cache control knob configurations
- No support for any URL filtering schemes (good list, bad list, N2H2, Websense, and SmartFilter)
- No support for caching files from a Macintosh FTP server
- No support for “offline” operation for the FTP proxy server

FTP Caching Support in the *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*

Updates to the *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1* regarding FTP caching support are:

- On page 2-7, in the “FTP and Caching” section, the information about configuring FTP incoming ports and the Rules Template only applies to FTP-over-HTTP caching. It does not apply to native FTP caching.
- In the “FTP Proxy Configuration Examples” section on page 5-12, the examples of how to use the **ftp proxy** global configuration commands only apply to a Content Engine that is operating in FTP-over-HTTP mode. The **ftp object max-size** command applies to Content Engines that are operating in either FTP-over-HTTP mode or native FTP mode.
- The “Configuring FTP Connection Settings Using the Content Engine GUI” section on page 10-2 applies only to FTP-over-HTTP caching for nontransparent proxy mode. The FTP inbound and outbound proxy configuration apply only to FTP URLs over HTTP (FTP-over-HTTP).

- In the “Configuring FTP Connection Settings Using CLI Commands” section on page 10-3, the **ftp proxy incoming** and **ftp proxy outgoing** global configuration commands apply only to FTP-over-HTTP caching.

The **ftp proxy active-mode** global configuration command applies to FTP (native FTP) caching as well as to FTP-over-HTTP caching.

- In FTP-over HTTP caching mode, if the **ftp proxy active-mode** global configuration command is used, the Content Engine first attempts to use active mode with the FTP server for the data connection. If the active mode fails, the Content Engine attempts to use passive mode for the data connection. If this command is not configured, the Content Engine first attempts to use passive mode with the FTP server for the data connection, and then automatically switches to active mode if passive mode is not supported by the FTP server.
- In native FTP caching mode, if the **ftp proxy active-mode** command is used, then the Content Engine uses the same mode with the FTP server for the data connection as the client used to reach the Content Engine, which can be either active or passive. If this command is not configured, the Content Engine uses passive mode with the FTP server for the data connection.
- In the “Setting FTP Cache Freshness” section on pages 10-4 through 10-7, the **ftp object max-size** global configuration command is the only mentioned command that applies to both native FTP caching and FTP-over-HTTP caching. All of the other mentioned commands (for example, the **ftp age-multiplier** command, the **ftp max-ttl** command, the **ftp object** command, the **ftp proxy** command, the **ftp reval-each-request** command, and the **ftp min-ttl** command) apply only to FTP-over-HTTP caching.
- On page 10-7, replace the sample output of the **show ftp** EXEC command with the following sample output. The following example shows that the output of the **show ftp** command differentiates between the configuration that is applicable to FTP-over-HTTP client requests and the one that applies to FTP (native FTP) client requests:

```
ContentEngine# show ftp
FTP over HTTP Configuration
-----

FTP heuristic age-multipliers: directory-listing 30% file 60%
Maximum time to live in days: directory-listing 3 file 7
Minimum time to live for all objects in minutes: 30
Incoming Proxy-Mode:
  Configured Proxy mode FTP connections on ports: 80 8080
Outgoing Proxy-Mode:
  Not using outgoing proxy mode.
Active mode of FTP transfer is enabled
Maximum size of a FTP cacheable object is 204800 KBytes
No object is revalidated on each request

FTP Configuration
-----

WCCP FTP service status:           ENABLED
Maximum size of a FTP cacheable object: 204800 KBytes
FTP data connection mode with Server: Adhere to Client's mode (active or passive)
```

- On page C-4, replace the WCCP Service Groups table with the following table that has the WCCP FTP caching service (service group number 60) added to it. You can configure a router that is running WCCP Version 2 to run any of the cache-related services listed in the following table. WCCP Version 1 routers support only the web cache service (service group 0).

Service Group Number	Description of Services
0	Web caching
53	DNS caching
60	FTP caching
80	RTSP
81	MMST
82	MMSU
90–97	User-configurable
98	Custom web caching
99	Reverse proxy web caching

- On page C-9, add native FTP caching to the list of services that you can configure on a router that is running WCCP Version 2. The following is an example of how to configure native FTP caching on a router running WCCP Version 2.

- Turn on native FTP caching. The service group number for this service is 60.

```
Router(config)# ip wccp 60
```

- Specify an interface on which the native FTP caching service will run.

```
Router(config)# interface type number
```

- Configure the router to use the outbound interface for the native FTP caching service.

```
Router(config-if)# ip wccp 60 redirect out
```

FTP Caching Support in the *Cisco ACNS Software Command Reference, Release 5.1 Publication*

Updates to the *Cisco ACNS Software Command Reference, Release 5.1* publication regarding FTP caching support are:

- On pages 2-118 through 2-119, replace the syntax description of the options for the **ftp** global configuration command with the following revised description that indicates whether an option applies to FTP-over-HTTP caching only (FTP-over-HTTP only), or both native FTP caching and FTP-over-HTTP caching (FTP and FTP-over-HTTP):

age-multiplier	FTP caching heuristic modifiers. (FTP-over-HTTP only)
max-ttl	Sets the maximum Time To Live for objects in the cache. (FTP-over-HTTP only)
min-ttl	Sets the minimum Time To Live for FTP objects in the cache. (FTP-over-HTTP only)
object	Sets the configuration of FTP objects. (FTP and FTP-over-HTTP)
max-size	Sets the maximum size of a cacheable object. (FTP and FTP-over-HTTP)
proxy	Sets the proxy configuration parameters. (FTP and FTP-over-HTTP)

active-mode	Configures the FTP mode for establishing the data connection. (FTP and FTP-over-HTTP)
anonymous-pswd	Sets the anonymous password string (for example, wwwuser@cisco.com). (FTP-over-HTTP only)
incoming	Sets the incoming port for proxy-mode requests. (FTP-over-HTTP only)
outgoing	Sets the parameters to direct outgoing FTP requests to another proxy server. (FTP-over-HTTP only)
reval-each-request	Sets the scope of revalidation for every request. (FTP-over-HTTP only)

- On page 2-120, note the following new usage guideline regarding the **ftp proxy active-mode** global configuration command.

The **ftp proxy active-mode** command applies to FTP (native FTP) caching as well as FTP-over-HTTP caching.

- In FTP-over-HTTP caching mode, if the **ftp proxy active-mode** global configuration command is used, the Content Engine first attempts to use active mode with the FTP server for the data connection. If the active mode fails, the Content Engine attempts to use passive mode for the data connection. If this command is not used, the Content Engine first attempts to use passive mode with the FTP server for the data connection, and then automatically switches to active mode if passive mode is not supported by the FTP server.
- In native FTP caching mode, if this command is used, then the Content Engine uses the same mode with the FTP server for the data connection as the client used to the Content Engine, which can be either active or passive. If this command is not used, the Content Engine uses passive mode with the FTP server for the data connection.
- On page 2-121, the examples of how to use the **ftp proxy** global configuration commands apply only to a Content Engine that is operating in FTP-over-HTTP mode. The **ftp object max-size** global configuration command applies to Content Engines that are operating in either FTP-over-HTTP mode or native FTP mode.
- On page 2-331, replace the sample output of the **show ftp EXEC** command with the following sample output. As the following example shows, the output of the **show ftp** command differentiates between the configuration that is applicable to FTP-over-HTTP client requests and that for FTP (native FTP) client requests:

```
ContentEngine# show ftp
FTP over HTTP Configuration
-----

FTP heuristic age-multipliers: directory-listing 30% file 60%
Maximum time to live in days: directory-listing 3 file 7
Minimum time to live for all objects in minutes: 30
Incoming Proxy-Mode:
    Configured Proxy mode FTP connections on ports: 80 8080
Outgoing Proxy-Mode:
    Not using outgoing proxy mode.
Active mode of FTP transfer is enabled
Maximum size of a FTP cacheable object is 204800 KBytes
No object is revalidated on each request

FTP Configuration
-----

WCCP FTP service status:                ENABLED
Maximum size of a FTP cacheable object:  204800 KBytes
FTP data connection mode with Server:    Adhere to Client's mode (active or passive)
```

- On page 2-469, replace the sample output of the **show wccp services** EXEC command with the following:

```
ContentEngine# show wccp services
Services configured on this Content Engine
  Web Cache
  Custom Web Cache
  FTP Cache
  RTSP
```

- On page 2-469, replace the partial output from the **show wccp routers** EXEC command with the following:

```
ContentEngine# show wccp routers
Router Information for Service: FTP Cache
  Routers Configured and Seeing this Content Engine(1)
    Router Id      Sent To      Recv ID
    0.0.0.0        10.1.94.1    00000000
  Routers not Seeing this Content Engine
    10.1.94.1
  Routers Notified of but not Configured
    -NONE-
  Multicast Addresses Configured
    -NONE-
```

- In ACNS 5.1 software, the **debug ftp-proxy** EXEC command was added. On page 2-88 of the *Cisco ACNS Software Command Reference, Release 5.1* publication, add the following options to the **debug** command options table:

ftp-proxy	Debugs the native FTP functions (includes such functions as fetching and caching files from an FTP server, posting files to an FTP server, and performing directory listings on an FTP server).
all	Debugs all native FTP functions.
cache	Debugs the cache proxy that is used for native FTP caching (the cache proxy resides on the Content Engine that is operating in nontransparent proxy mode to support native FTP requests).
client	Debugs the native FTP client. In native FTP mode, clients use the native FTP protocol to issue FTP requests, as shown in the following example: ContentEngine# ftp server.cisco.com
control-proxy	Debugs the control proxy that is used for native FTP caching (the control proxy resides on the Content Engine that is operating in nontransparent proxy mode to support native FTP requests).
parser	Debugs the parser that is used for native FTP caching.
proxy-comm	Debugs the proxy communications used for native FTP functions.
server	Debugs the native FTP server.



Note All of the output of the **debug ftp-proxy** command is written to the file `/local1/errorlog/ftp-ctlproxy-errorlog.current` with the following exceptions. The output of the **debug ftp-proxy cache** command and portions of the **debug ftp-proxy proxy-comm** command output are written to the syslog at debug priority level.

- On page 2-88 of the *Cisco ACNS Software Command Reference, Release 5.1* publication, replace the description of the **debug ftp** EXEC command with the following:

ftp	Debugs the FTP functions for FTP-over-HTTP requests (includes fetching and caching files from an FTP server).
all	Debugs all FTP functions for FTP-over-HTTP requests.
cache	Debugs the FTP cache (the Content Engine that is operating in nontransparent proxy mode to cache the contents of the FTP-over-HTTP requests).
client	Debugs the FTP client (end users who are issuing the FTP-over-HTTP request from their browsers).
server	Debugs the FTP server (for FTP-over-HTTP requests).

Group-Type Patterns in Rule Pattern Lists

A group-type pattern is one of the types of rule patterns that you can add to a pattern list. The default operation for the group-type pattern is an OR operation.

In the “List of Rule Patterns” section on page 14-4 of the *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*, replace the syntax description for the group-type pattern with the following description:

group-type	Specifies whether the pattern list is an AND or OR type. The default is OR.
-------------------	---

In the “Patterns” section on page 2-281 of the *Cisco ACNS Software Command Reference, Release 5.1* publication, replace the bulleted description for the group-type pattern with the following description:

- **Group-type**—Specifies whether the pattern list is an AND or OR type. The default is OR.

SmartFilter Software and the rule action no-auth Command Rule Interaction

This documentation update applies to the following three ACNS 5.1 software guides:

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*
- *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*
- *Cisco ACNS Software Command Reference, Release 5.1*

The **rule action no-auth** global configuration command permits specific login and content requests to bypass authentication and authorization features such as LDAP, RADIUS, SSH, or TACACS+. In the following example, any requests from the source IP address (src-ip) 172.16.53.88 are not authenticated.

```
ContentEngine(config)# rule enable
ContentEngine(config)# rule action no-auth pattern-list 1 protocol all
ContentEngine(config)# rule pattern-list 1 src-ip 172.16.53.88 255.255.255.255
```

If ACNS 5.1 software is configured for authentication and SmartFilter URL filtering, requests that are allowed to bypass authentication will also bypass the SmartFilter URL filter.

Bandwidth Configuration for Interfaces and Content Services

On page 3-19 of the *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*, the tip states that Gigabit Ethernet interfaces run only at 1000 Mbps. This restriction only applies to a Content Engine CE-7320 model that has an optical Gigabit Ethernet interface; the speed of this interface cannot be changed.

For newer models of the Content Engine (for example, the CE-510, CE-565, CE-7305, and CE-7325) that have a Gigabit Ethernet interface over copper, this restriction does not apply; you can configure these Gigabit Ethernet interfaces to run at 10, 100, or 1000 Mbps. Note that on these newer Content Engine models, the 1000 Mbps setting implies autosense (for example, you cannot configure the Gigabit Ethernet interface to run at 1000 Mbps and half duplex). The ACNS 5.x software automatically enables autosense if the speed is set to 1000 Mbps.

pace Command

The **pace** global configuration command is no longer supported as a separate command in ACNS software, Release 5.1 and later. The functions of the **pace** command have been incorporated into the **bitrate** and **bandwidth** global configuration commands.

Updates to the *Cisco ACNS Software Command Reference, Release 5.1* publication are as follows:

- On page 2-6, ignore the description and cross-reference to the **pace** command in Table 2-1.
- On page 2-39, replace the syntax description in the “**bitrate**” section with the following revised description:

http	Configures the maximum pacing bit rate in kilobits per second (kbps) for large files sent using the HTTP protocol.
default	Sets the default bit rate in kbps for large files.
<i>bitrate</i>	Bit rate in kbps (0–2000000).
wmt	Configures the bit rate in kbps for large files sent using the WMT protocol.
incoming	Sets the incoming bit rate settings.
<i>bitrate</i>	Incoming bit rate in kbps (0–2147483647).
outgoing	Sets the outgoing bit rate settings.
<i>bitrate</i>	Outgoing bit rate in kbps (0–2147483647).



Note The aggregate bandwidth used by all concurrent users is still limited by the default device bandwidth, or by the limit configured using the **bandwidth** command.

- On page 2-223, ignore the entire “**pace**” command section.

pre-load Command

In the **pre-load url-list-file** *path* global configuration command, the value for *path* can be a URL as well as a local file path.

In the *Cisco ACNS Software Command Reference, Release 5.1* publication, in the “pre-load” section on page 2-238, replace the syntax description for *path* with the following description:

<i>path</i>	Path of the file containing the URL list or a URL.
-------------	--

In ACNS 5.1.5 software, the **pre-load depth-level-default** command was enhanced to support 0 as a preload depth level. Setting the depth level default to 0 would be useful if you have specified URLs in preload.txt files and you do not want the Content Engine to try to preload other URLs.

In the *Cisco ACNS Software Command Reference, Release 5.1* publication, in the “pre-load” section on page 2-236, replace the syntax description for *path* with the following description if you are using ACNS 5.1.5 or later software:

depth-level-default	Configures the default depth level.
<i>level_number</i>	Depth level of URL download (0–20). The default is 3.

For ACNS 5.1 or 5.1.3 software, the valid values for the preload depth level default are still 1 to 20; 0 is not supported.

NTLM Preload Support

This documentation update applies to the following ACNS 5.1 software guides:

- *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*
- *Cisco ACNS Software Command Reference, Release 5.1*

In ACNS 5.1 software, support for preloading NTLM authenticated objects was added. This feature allows NTLM authenticated objects (authenticated objects that reside on the servers that authenticate NTLM only) to be preloaded on a Content Engine.

An entry in a URL list file has the following format:

URL [depth] [domain-name:host-name:host-domain-name]

hostname and *host-domain-name* can be null; however, *domain name* is required if NTLM credentials have been configured. (The separator is required.)

`http://www.cisco.com 3 apac::`

If NTLM-related information is not present in the preload URL list file entry, the authentication scheme falls back to basic authentication.

To preload authenticated content on the Content Engine, you must specify the username and password in the URL list file as follows:

`http://username:password@www.authenticationsite.com/depth_level`



Note

To enable the Content Engine to fetch specified objects and to store these preloaded objects in its local cache, you must use the **http cache-authenticated ntlm** global configuration command.

show statistics icap Command

This documentation update applies to the *Cisco ACNS Software Command Reference, Release 5.1* publication.

In ACNS software, Release 5.1, the **show statistics icap** EXEC command was added. You can use this command to display ICAP related statistics for the Content Engine. This command has no arguments or keywords. There is no default behavior or values.

The following is an example of the output of the **show statistics icap** command.

```
ContentEngine# show statistics icap
ICAP-client statistics (http proxy)
-----

Total requests for V1 via RPC:          0
Time per ICAP request (last 1k reqs):  0
ICAP daemon connection error:         0
Bad packets from ICAP daemon:         0
Error parsing HTTP req hdr from ICAP:  0
ICAP daemon internal error:           0

Total requests via outgoing proxy:     0
ICAP daemon overloaded:                0
Other errors:                          0

ICAP Daemon statistics
-----

Total requests served:                  0
Total requests served:                  0
Average latency in milliseconds:       0.000000
ICAP Service statistics
-----

Service -- servforicap
Service Errors:      0
Service Bypasses:   0
  Server -- icap://1.2.3.4/servforicap
    Total Reqmods (0), Total Respmods (0)
    Modifications (Reqmod - 0), (Respmod - 0)
    No Modifications (Reqmod - 0), (Respmod - 0)
    Error Responses (Reqmod - 0), (Respmod - 0)
    Server Errors:          0
    Server Bypasses:       0
    Options Req Success:    0
    Options Req Failed:     8569
    Max Conn Available     0
    Used Connections:      0
    Total Bytes sent:      0
    Total Bytes received:  0
    Total BPS sent:        0.000000
    Total BPS received:   0.000000
    Server State:         DISCONNECTED
ContentEngine#
```

Default Port of the Content Engine GUI

On page 12-28 of the *Cisco ACNS Caching and Streaming Configuration Guide, Release 5.1*, replace the tip with the following:


Tip

To access the Content Engine GUI, enter the Content Engine IP address and append the default port number 8003 as the URL address in your browser of choice. For example, enter `https://CEIPaddress:8003` as the URL.

Playing Nonhinted IP/TV On-Demand Programs over an ACNS Network

This documentation update applies to the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.

The Cisco Streaming Engine supports only hinted files (MOV and hinted MP4 files) for streaming.


Note

Hinted files contain hint tracks, which store packetization information that tells the streaming server how to package the media data. The streaming server uses the packetization information in the hint tracks to stream the media data to the network.

If you are creating a file-based IP/TV program for streaming over an ACNS network, make sure that you use only hinted files such as those with .mov or .mp4 extensions. However, you can pre-position on-demand programs based on nonhinted files such as .mpg files on Content Engines in an ACNS network. Pre-positioned on-demand programs based on nonhinted files are not listed in the IP/TV Viewer program listings or in the web-based program guide.

To watch IP/TV on-demand programs based on nonhinted files when IP/TV is integrated with an ACNS network, use the TV-out feature of the ACNS software. For more information on enabling the TV-out feature and creating playlists, refer to Chapter 11 of the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.

Restriction on IP/TV Program Manager Configuration

This documentation update applies to the following ACNS 5.1 software guides:

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*.
- *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.1*

If a program that you want to deliver over an ACNS network uses live multicast mode, you must use the same multicast IP address for the audio, video, and SlideCast streams.

This restriction on IP/TV Program Manager configuration does not apply if the Content Engine used for live splitting is running ACNS 5.1.5 or later software. However, this restriction still applies if the Content Engine is running ACNS 5.1.1 software, even if you are running IP/TV 5.1.5 or later software on IP/TV Program Manager.

Related Documentation

Your product shipped with a minimal set of printed documentation. The printed documentation provides enough information for you to install and initially configure your product.

Product Documentation Set

In addition to these release notes, the product documentation set includes:

- *Documentation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Refer to the *Documentation Guide* for a complete documentation roadmap and URL documentation links for this product.

Hardware Documentation

- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Installing the Cisco Content Engine 7305 and 7325*
- *Installing Field-Replaceable Units in the Cisco Content Engine 7305 and 7325*
- *Cisco Content Engine 7320 Product Description Note*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Installing the Cisco Content Engine 510 and 565*
- *Installing Field-Replaceable Units in the Cisco Content Engine 510 and 565*
- *Cisco Storage Array Installation and Configuration Guide*
- *Release Notes for Cisco Content Delivery Manager 4630*
- *Cisco Content Distribution Manager 4650 Product Description Note*
- *Cisco Content Distribution Manager 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Release Notes for the Cisco Content Engine 500 Series*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*

Software Documentation

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.1*
- *Cisco ACNS Software Caching and Streaming Configuration Guide, Release 5.1*
- *Cisco ACNS Software Command Reference, Release 5.1*
- *Cisco ACNS Software Migration Guide, Release 5.1*
- *Cisco ACNS Software API Guide, Release 5.1*
- *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.1*

- *Release Notes for Cisco IP/TV, Release 5.1.5*
- *Release Notes for Cisco ACNS Software, Release 5.1.11* (the release notes you are reading now)

Online Help

- Content Distribution Manager GUI online help system for centrally managed ACNS networks
- Content Engine GUI online help system for locally deployed Content Engines

**Note**

The term “locally deployed Content Engine” refers to a Content Engine that was initially configured with the autoregistration feature turned off so that the Content Engine would not automatically register with the Content Distribution Manager. Because the Content Engine did not register with the Content Distribution Manager, it can be individually managed through the Content Engine CLI or GUI as a locally deployed device. The Content Engine GUI allows you to remotely configure, manage, and monitor locally deployed Content Engines through your browser.

The Content Distribution Manager GUI and the Content Engine GUI both have context-sensitive online help that can be accessed by clicking the **HELP** button.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:
http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)