Release Notes for Cisco Internet Streamer CDS 2.5.7

These release notes cover Cisco Internet Streamer CDS Release 2.5.7-b5.

Revised: May 2010, OL-20688-02

Note Release 2.5.7-b10 supersedes 2.5.7-b5.

Contents

The following information is included in these release notes:

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

New Features

Release 2.5.7 of the Cisco Internet Streamer CDS introduces the following features:

New Web Engine

In Release 2.5.7, the Web Engine has been enhanced and supports the following:

- Optimization for small content objects
- Optimization of Adaptive Bitrate Streaming for Move, Apple iPhone, and Smooth HD
- Move VOD streaming
- Move live streaming
- MP3 live streaming
- Cache on abort (content is cached if client request is aborted)
- Maximum concurrent connections is 30,000. Alarm is raised and CDSM and SR are informed when an SE reaches 29,000 connections, allowing time for the SR to redirect requests to other SEs

The Web Engine in Release 2.5.7 interoperates with Apple's media stream segmenter, as well as Microsoft's Internet Information Services 7.0 (IIS7.0) Smooth Streaming. Apple's media stream segmenter segments encoded media into separate files for streaming to iPhones. Microsoft's IIS Smooth Streaming offers adaptive streaming of high-definition (HD) content.

The new Web Engine does not support IP-based redirection, an SR routing method. The new Web Engine follows the RFC 2616 standard with regards to caching content; therefore a number of the configuration settings have been removed in Release 2.5.7.

The following features are not supported in the New Web Engine:

- IP-based redirection
- Syslog or alarm is not generated when number of concurrent sessions threshold is crossed
- PCMM and ICAP
- Outgoing proxy
- Maximum object size
- Cache on abort
- Cache cookie
- CLI commands:
  - http cache-cookies
  - http cache-on-abort
  - http reval-each-request all
  - http object max-size *maxsize*

  - http proxy outgoing
  - service-router redirect-mode ip-redirect

The new Web Engine does not support the following service rule actions:

- generate-url-signature
- no-cache (do not cache this object); therefore all Web Engine content is cached.
- refresh
- replace

CDN Selector

The CDN Selector provides a method of performing third-party streaming service selection. The third-party streaming service is selected based on the content type of the client request, the geographic location of the client request, or both. When CDN Selector is enabled, the Service Router uses the information in the CDN Selector file to determine which third-party streaming service is selected for servicing the client's request.

Note CDN Selector is an EFT feature for Release 2.5.7.

A CDN Selector file is an XML file containing the URL, including the directory path, of each third-party streaming service, and the content types and geographic locations criteria for redirecting client requests. If the geographic location is used as the selection criteria, the CDN Selector uses the Geo-Location server to map the client's IP address to the client's country.

The Service Router then sends a 302 redirect to the client with the translated URL for the selected third-party streaming service. If the Internet Streamer CDS is chosen, the request is handed over to the Request Routing Engine for further processing. If the client request does not meet any of the selection polices criteria and a default CDN is specified in the CDN Selector file, the client request is redirected to the default CDN.

Proximity Engine

The Proximity Engine has the following new features:

- Service Routing Protocol (SRP)
- BGP best path and redirect proximity
- IS-IS authentication
- Proximity statistics displayed in CDSM

Multi-Port Support

Multi-port support allows the configuration of multiple interfaces, each with a different IP address, all used for streaming traffic. An interface could be a gigabit Ethernet channel, a port channel, or a standby group. Multi-port support allows for utilization of the total bandwidth available on the CDE220-2S3i and is introduced solely to support the CDE220-2S3i platform in order to use all 12 gigabit Ethernet interfaces.

Note Multi-port support is only supported on the CDE220-2S3i platform.

The main reason Multi-port support is added is because a switch has a hard limit of 8 interfaces that can be grouped into a port-channel, so in order to fully utilize all 12 gigabit Ethernet interfaces, multi-port support was added.

Prior to Release 2.5 only a single streaming interface could be configured; the streaming interface was configured as the primary interface. In order to separate management and streaming traffic, the management interface was configured as a dedicated management interface by using the CDSM's Device Activation page. A port channel, as well as a standby group, could be created for the management interface in order to provide redundancy. In Release 2.5, the streaming interface is introduced for streaming content.

Configuring Multiple IP Address in a Private Network

If the CDE220-2S3i has multiple IP addresses and is configured in a private network address space, then each internal IP address needs an external NAT entry defined on the main core router or switch.

Configuring a Default Gateway for Multi-Port Support

The IP default gateway can only be configured when the physical network connection and VLAN is configured and active on the switch or router. If the VLAN is not ready when you configure the IP default gateway, you get an error message stating that the default gateway address is invalid.

Delivery Service-based Service Rules for Web Engine

The Service Rule file is an XML file used to specify the service rules for all the SEs in a delivery service. The Service Rule file is only supported for the Web Engine. All other protocol engines should continue to configure service rules by device.

Note For the Web Engine in Release 2.5.7, the Service Rule file must be used if service rules are to be confided.

You do not need to enable Service Rules on each SE for the Web Engine, just create a Service Rule file, upload it to the CDS, and select it through for the delivery service.

The Service Rule XML file supports the following service rule pattern lists in Release 2.5.7:

- Domain
- SrcIP
- UrlRegex

Note In Release 2.5.7, the Header pattern list is not supported in the Service Rule XML file for the Web Engine.

The Service Rule XML file supports the following service rule actions for the Web Engine (HTTP only) in Release 2.5.7:

- Allow
- Block

- Validate
- URL rewrite

Note In Release 2.5.7, the URL redirect and no cache service rule actions are not supported in the Service Rule XML file for the Web Engine.

Enhancements

Table 1 describes the enhancements to Internet Streamer CDS 2.5.7.

Table 1 New Features in Internet Streamer CDS 2.5.7

Enhancement	Description
Removed ability to deactivate primary CDSM	In the CDSM GUI, previous to Release 2.5.7, the user could deactivate the primary CDSM. In Release 2.5.7 only the standby CDSM can be deactivated. (CSCtd66502)
Configure minimum length of username.	The CDSM GUI now offers the ability to configure the minimum length allowed for the username log in to the CDSM GUI. (CSCte01727)
MTOD functional for SSH log in.	The message of the day (MTOD) is functional for SSH logins. (CSCtc56405)
Disable TCP timestamp.	New command to enable and disable TCP timestamp. Use the **tcp timestamp** command to enable the timestamp and **no tcp timestamp** to disable the timestamp. (CSCte16238)
Added IOS patch for SNMP	SNMP IOS patch for private community. (CSCte01703)
Detect PSU failure.	Detect power supply unit (PSU) failure and trigger alarm. (CSCtc82945)
Primary Authentication server rejects access; second Authentication server is not tried.	If the primary Authentication server rejects access to a CDS device because of incorrect password, the second Authentication server is not tried. The rejection is counted as one attempt; not two. (CSCtc97976)
The **disk erase** and **disk policy apply** commands are added.	In Release 2.5.1 and 2.5.3, use the **disk reformat** command followed by the **reload** command to erase the content on a disk. In Release 2.5.7 and later, use the **disk erase** command followed by the **disk policy apply** command. This command erases all the content on the disk. The sequence to erase a disk is to enter the **disk unuse** command first, then enter the **disk erase** and **disk policy apply** commands.

System Requirements

The Internet Streamer CDS runs on the CDE100, CDE200, CDE205, and the CDE220 hardware models. Table 2 lists the different device modes for the Cisco Internet Streamer CDS software, and which CDEs support them.

Table 2 Supported CDEs

Device Mode	CDE100	CDE200	CDE205	CDE220
CDSM	Yes	No	Yes	No
SR	Yes	Yes	Yes	Yes
SE	Yes	Yes	Yes	Yes

Release 2.5.7 supports the CDE220-2S3i platform. There are a total of 14 gigabit Ethernet ports in this CDE. The first two ports (1/0 and 2/0) are management ports. The remaining 12 gigabit Ethernet ports can be configured as two port channels. See the *Cisco Content Delivery Engine CDE205/220/420 Hardware Installation Guide* for set up and installation procedures for the CDE220-2S3i and the *Cisco Internet Streamer CDS 2.5 Software Configuration Guide* for information on configuring the Multi Port Support feature.

The CDE220-2G2 platform has a total of ten gigabit Ethernet ports. The first two ports (1/0 and 2/0) are management ports. The remaining eight gigabit Ethernet ports can be configured as one port channel. See the *Cisco Content Delivery Engine CDE205/220/420 Hardware Installation Guide* for set up and installation procedures for the CDE220-2G2.

The CDE100 can run as the CDSM, while theCDE200 can run as the Service Router or the Service Engine. See the *Cisco Content Delivery Engine CDE100/200/300/400 Hardware Installation Guide* for set up and installation procedures for the CDE100 and CDE200.

The CDE205 can run as the CDSM, Service Router, or Service Engine. See the *Cisco Content Delivery Engine CDE205/220/420 Hardware Installation Guide* for set up and installation procedures for the CDE205.

Note For performance information, see the release-specific performance bulletin.

Limitations and Restrictions

This release contains the following limitations and restrictions:

- There is a 4 KB maximum limit for HTTP request headers. This has been added to prevent client-side attacks, including overflowing buffers in the Web Engine.
- There is no network address translation (NAT) device separating the CDEs from one another.
- Do not run the CDE with the cover off. This disrupts the fan air flow and causes overheating.

Note The CDS does not support network address translation (NAT) configuration, where one or more CDEs are behind the NAT device or firewall. The workaround for this, if your CDS network is behind a firewall, is to configure each internal and external IP address pair with the same IP address.

The CDS does support clients that are behind a NAT device or firewall that have shared external IP addresses. In other words, there could be a firewall between the CDS network and the client device. However, the NAT device or firewall must support RTP/RTSP.

Note In Release 2.5.7, configuring Replication Bandwidth Scheduling is only supported on a per SE-basis; Device Group configuration of Replication Bandwidth Scheduling is not supported.

Important Notes

To maximize the content delivery performance of a CDE200, CDE205, or CDE220, we recommend you do the following:

1. Use port channel for all client-facing traffic.

   Configure interfaces on the quad-port gigabit Ethernet cards into a single port-bonding interface. Use this bonding channel, which provides instantaneous failover between ports, for all client-facing traffic. Use interfaces number 1 and 2 (the two on-board Ethernet ports) for intra-CDS traffic, such as management traffic, and configure these two interfaces either as standby or port-channel mode. Refer to the *Cisco Internet Streamer CDS 2.4 Software Configuration Guide* for detailed instruction.

2. Use the client IP address as the load balancing algorithm.

   Assuming ether-channel (also known as port-channel) is used between the upstream router/switch and the SE for streaming real-time data, the ether-channel load balance algorithms on the upstream switch/router and the SE should be configured as "Src-ip" and "Destination IP" respectively. Using this configuration ensures session stickiness and general balanced load distribution based on clients' IP addresses. Also, distribute your client IP address space across multiple subnets so that the load balancing algorithm is effective in spreading the traffic among multiple ports.

   Note The optimal load-balance setting on the switch for traffic between the Content Acquirer and the edge Service Engine is dst-port, which is not available on the 3750, but is available on the Catalyst 6000 series.

3. For high-volume traffic, separate HTTP and WMT.

   The CDE200, CDE205, or CDE220 performance has been optimized for HTTP and WMT bulk traffic, individually. While it is entirely workable to have mixed HTTP and WMT traffic flowing through a single CDE200 simultaneously, the aggregate performance may not be as optimal as the case where the two traffic types are separate, especially when the traffic volume is high. So, if you have enough client WMT traffic to saturate a full CDE200, CDE205, or CDE220 capacity, we recommend that you provision a dedicated CDE200 to handle WMT; and likewise for HTTP. In such cases, we do *not* recommended that you mix the two traffic types on all CDE servers which could result in suboptimal aggregate performance and require more CDE200, CDE205, or CDE220 servers than usual.

4. For mixed traffic, turn on the HTTP bitrate pacing feature.

   If your deployment must have Streamers handle HTTP and WMT traffic simultaneously, it is best that you configure the Streamer to limit each of its HTTP sessions below a certain bitrate (for example, 1Mbps, 5Mbps, or the typical speed of your client population). This prevents HTTP sessions from running at higher throughput than necessary, and disrupting the concurrent WMT streaming sessions on that Streamer. To turn on this pacing feature, use the HTTP bitrate field in the CDSM Delivery Service GUI page.

   Please be aware of the side effects of using the following commands for Movie Streamer:

   ```
   Config# movie-streamer advanced client idle-timeout <30-1800>
   Config# movie-streamer advanced client rtp-timeout <30-1800>
   ```

   These commands are only intended for performance testing when using certain testing tools that do not have full support of the RTCP receiver report. Setting these timeouts to high values causes inefficient tear down of client connections when the streaming sessions have ended.

   For typical deployments, it is preferable to leave these parameters set to their defaults.

5. For ASX requests, when the Service Router redirects the request to an alternate domain or to the origin server, the Service Router does not strip the .asx extension, this is because the .asx extension is part of the original request. If an alternate domain or origin server does not have the requested file, the request fails. To ensure requests for asx files do not fail, make sure the .asx files are stored on the alternate domain and origin server.

Open Caveats

This release contains the following open caveats:

API

- CSCth44836

  Symptom:

  UNS-related errors occur because the program name and reference URL had uppercase and lowercase characters, but the API only allows lowercase characters for both the program name and reference URL.

  Condition:

  Live programs with uppercase characters in the program name and reference URL (unicast or multicast) are not consistent with API calls, which expect only lowercase characters.

  Workaround:

Only use lowercase characters for the program name and reference URLs.

Windows Media Streaming

- CSCtf74656

  Symptom:

  After run a certain long time SE can not server any requests in Longevity test.

  Condition:

  In longevity tests with mixed heavy traffic and "cache revalidate for each request" enabled, after running a certain period of time (duration depends on the test profile), the SE cannot serve requests. The following is an example of the profile:

```
1200 all-unique 100kbps sessions -prepositioned    length : 30mins
1200 all-unique 300kbps sessions -prepositioned    length : 30mins
600 all-unique 700kbps sessions - cache hit           length :30mins
800 all-unique 1mbps sessions - cache hit              length :1hr
200 all-unique 2mbps sessions - cache hit              length :30mins
100 long url single-unique 700kbps sessions - prepositioned         length : 30mins
600 single-unique 1mbps sessions - cache hit         length : 1hr
Total : 4700 concurrent requests
```

  Workaround:

  Disable "cache revalidate for each request."

- CSCtf77234

  Symptom:

  The transaction log configuration from device group cannot apply to the SE in this special case.

  Condition:

  If configure any value from CLI and negate it, a CLI with default value still shows in running config.

  Workaround:

  None.

Flash Media Streaming

- CSCta44470

  Symptom:

  This issue is seen when the client requests a live stream to the SE and after about eight hours, the client stream is stopped and the connection gets closed.

  Condition:

  This issue occurs only when playing a live stream continuously for more than eight hours to a single client. If the clients keeps connecting to the live stream and disconnecting from the live stream, this issue does not occur.

  Workaround:

  No workaround, however the next click does work.

- CSCte65508

Symptom:

The Flash Media Streaming processes take 100 percent of the CPU usage after changing the local time or possibly a negative NTP change. Mostly this would occur when the SE is reloaded.

Condition:

The fmsadmin process and fmsedge process is at 100 percent of the CPU after the SE reloads.

Workaround:

Restart Flash Media Streaming resolves this issue.

- CSCtf94686

  Symptom:

  Cache miss request fails to stream, when the virtual application path map is configured. But the same request next click works fine, because it is cache hit.

  Condition:

  During the cache miss request, when the virtual application path map is configured, virtual path map is applied to cache fill requests. But the following HTTP range requests are still sent without the virtual path map, which results in the origin server replying with a 404 error message and the Flash Media Streaming cache miss request failing.

  Workaround:

  Do not use the virtual map command or create a vod folder case on the origin server.

CDSM

- CSCtb82518

  Symptom:

  In the **Services > Service Definition> Delivery Services> Replication Status** page, the replication status switches between "No Status Reported" and "Completed" even if the replicating is finished.

  Condition:

  The interval for the replication status reporting between the CDSM and SE is not consistent.

  Workaround:

  Need to reconfigure the interval for the replication status reporting. In the CDSM GUI, choose **System > Configuration > System Properties**, edit **System.repstatus.updateRateSec**, change the current value to another one, and click **Submit**. This should stabilize the interval between the CDSM and the SEs.

- CSCtf61997

  Symptom:

  On an SE, the delivery service related information stored in the /state/perdsvc.xml file cannot be removed as expected even if the SE is deregistered from the CDSM.

  Condition:

  If the SE is assigned as the Content Acquirer of any delivery service, the perdsvc.xml file is not changed after the SE deregistered.

  Workaround:

Make sure the SE is not assigned as the Content Acquirer for any delivery service before running the **cms deregister force** command on the SE.

Web Engine

- CSCth28650

  Symptom:

  The device reloads when the **debug http service-router** or **undebug all** commands are entered.

  Condition:

  When the **debug http service-router** or **undebug all** commands are entered.

  Workaround:

  Do not enter the **debug http service-router** or **undebug all** commands. If you encounter this problem, contact Cisco customer support.

- CSCtc39891

  Symptom:

  Playback fails for Windows Media Streaming request.

  Condition:

  When the origin server is a Windows Media Server, and the SE tries a progressive download for the client .wmv request.

  Workaround:

  Make sure that client request is handled by the Windows Media Streaming engine and have the request streamed from the Windows Media origin server.

- CSCtd43011

  Symptom:

  Web Engine request to the origin server fails when request from client.

  Condition:

  When the origin server has authentication configured, the HTTP request from the client fails.

  Workaround:

  Disable authentication on the origin server. Instead, use the URL signing mechanism to make sure only genuine requests are allowed.

- CSCtf62311

  Symptom:

  Windows Media request fails for live programs.

  Condition:

  There are two delivery services configured for Live and VOD, and **Enable streaming over HTTP** is not configured for VOD delivery service. Then Windows Media live request fails.

  Workaround:

  Check the **Enable streaming over HTTP** check box for the delivery service to have the Windows Media live program work.

URL Manager

- CSCte42043

  Symptom:

  Windows Media request fails in particular scenario.

  Condition:

  When a badly formed URL request is sent for Windows Media content.

  Workaround:

  None. Do not use badly formed URLs in client requests.

Acquisition and Distribution

- CSCtf67983

  Symptom:

  Content with a bad MD-5 sum does not get removed and reingested on one of the SEs. It replicated fine to all other SEs, except the one SE where the content was not removed.

  Condition:

  In Release 2.4.3, an SE gets a bad copy of content and the MD-5 sum fails. The bad copy is not removed, so MD-5 sum is repeated in acquisition and distribution logs.

  Workaround:

  Delete the asset from the SE, wait for the replication to run again without errors, reingest the content, then have the replication run again.

Resolved Caveats

The following caveats have been resolved since Cisco Internet Streamer CDS Release 2.5.3 Not all the resolved issues are mentioned here. The following list highlights the resolved caveats associated with customer deployment scenarios.

Platform

- CSCtd16093

  Symptom:

  CDS-IS software does not currently support the lowering of SMART alarms. Should an event which triggers a SMART alarm clear, the SMART alarm will remain raised until the CDS-IS system has been reloaded.

  For a CDS-IS system, the typical SMART alarm pertains to drive failure prediction, and will be raised whenever a hard drive predicts its own imminent failure. The nature of this type of alarm is persistent. Once the prediction is made, it will not be cleared. Once more, because CDS-IS only supports replacing failed drives across reboot, the consequence of not lowering the alarm will go largely unnoticed.

Condition:

Unlike the typical 'failure prediction' alarm, other SMART conditions, namely the temperature alarm, are intermittent, and can be raised and lowered over time. This style of alarm is effected by the current bug, and will not be lowered once they have been raised.

CDSM

- CSCtf86279

  Symptom:

  When updating the software for a device through the CDSM GUI, the device status shows as pending rather than showing the progress of the software update. The new image is flashed five minutes later, which can be verified by the **show flash** command.

  Condition:

  Switch the role of the primary CDSM and standby CDSM. The device that is being updated cannot communicate with the old primary CDSM.

- CSCte74664

  Symptom:

  Removing content using the Content Removal page in the CDSM GUI or the URL Management API does not work shortly after the management IP address is changed using the CDSM GUI.

  Condition:

  From the CDSM GUI, choose **Devices > Devices > Device Activation**, change the Management Communication settings, and click **Submit**. The Content Removal in the CDSM GUI and the URL Management API may fail because of the DCF agent service is restarting.

- CSCtd28332

  Symptom:

  Multicast-in-multicast-out (MIMO) Movie Streamer live programs do not work, because the Unicast URL and Multicast URL fields in the CDSM GUI are exactly the same.

  Condition:

  This happens when creating a Movie Streamer live program with the multicast-out option.

- CSCtf54291

  Symptom:

  After selecting a Device Group in CDSM under **Devices > General Settings > Notification and Tracking > Service Monitor,** Submit button does not work.

Service Monitor

- CSCte10655

  Symptom:

  The major alarm for disk failure count is not cleared although the disk failure count threshold is cleared.

Conditions:

Enter the **show running-config** command, displays two port channels configured on the device and the **show service-router service-monitor** command displays disk failure count threshold enabled.

Network

- CSCtf81925

  Symptoms:

  When removing port channel load-balance at by using the **no portchannel load-balance** command, default-gateway route is removed and impacts network connectivity.

  When using the CDSM to change the port channel load balance it may not occur.

- CSCtf01052

  Symptom:

  After upgrading from Release 2.4.x to Release 2.5.3, static routes may be lost.

  Condition:

  Upgrade from Release 2.4.x to Release 2.5.3.

- CSCte76934

  Symptom:

  Static IP routes are appended with interface x.0.0.0 after upgrading from Release 2.4.x to Release 2.5.1 or Release 2.5.3.

  Condition:

  This only happens when you have existing static IP routes configured and you upgrade to Release 2.5.1 or Release 2.5.3.

- CSCte05421

  Symptom:

  Network connectivity is intermittent. Use the **show ip route** command to verify the routes. All default gateway and IP routes are listed.

  Condition:

  The **port-channel load-balance** command toggles the interface down and up, and causes the Linux OS to remove the route table for each interface. Restoration of the route tables is not handled properly by the CLI. Sometimes this command is sent by the CDSM when the device is registering to the CDSM.

Web Engine

- CSCtf94980

  Symptom:

  MP3 live streaming fails.

  Condition:

  Because Shoutcast does not have content length or transfer encoding as part of its headers, the connection to the origin server is closed after reading the headers.

- CSCtf24840

  Symptom:

  TRACE command is exposed and can be used to get more details of the server.

  Condition:

  Use of TRACE command to the SE.

Flash Media Streaming

- CSCsz23407

  Symptom:

  Minor alarm is generated in the SE stating that the fmsadmin process is down. Syslog reports the following:

  ```
  "%SE-UNKNOWN-3-899999: Failed to create listener for adaptor, IP 127.0.0.1, port
  11110: TCCommBridge::createListener 127.0.0.1:11110/v4: bind failed!!!."
  ```

  The **show statistics flash-media-streaming** command does not work.

  Condition:

  This issue happens randomly once Flash Media Streaming is restarted or the SE is restarted. This issue happens because the fmsadmin process port was taken by some other process.

Upgrading to Release 2.5.7

The only supported upgrade paths are Release 2.4.x to Release 2.5.7, and Release 2.5.x to Release 2.5.7. If you are running a release prior to Release 2.4.x, you must upgrade to at least Release 2.4.x before upgrading to Release 2.5.7.

After the upgrade procedure starts, do not make any configuration changes until all the devices have been upgraded.

Note Upgrading to Release 2.5.7 includes SHA-256-encrypted user passwords. If the config file contains users with SHA-256 encrypted passwords, and if you downgrade to an earlier release, the user information will be lost because the older software cannot recognize the new method of encrypting passwords.

When upgrading to Release 2.5.7 from Release 2.4.x, configuring the Proximity Server port number field is no longer required for the Proximity-Based Routing feature. The port number for all Proximity servers is 7003.

Release 2.5.7 only supports one IGP (IS-IS or OSPF) for the Proximity Engine. When upgrading to Release 2.5.7 from Release 2.5.1 or Release 2.5.3, if both IGPs (IS-IS and OSPF) were configured for the Proximity Engine, then one of the configurations must be removed.

Note Downgrading from Release 2.5.7 to Release 2.4 is not supported on the CDE220-2S3i because this CDE was introduced in Release 2.5.7

Because the functionality of having the SR act as both the Request Routing Engine and the Proximity Server was not part of Release 2.4.x, downgrading from Release 2.5.x to Release 2.4.x results in losing the configuration of 127.0.0.1 (SR loopback address) as the Proximity Server. All other Proximity Servers are still configured.

The new Web Engine in Release 2.5.7 cannot be removed during downgrade to Release 2.5.3 because this configuration is still valid in Release 2.5.3 (the new Web Engine was supported as an EFT feature in Release 2.5.3). Therefore, both CLI commands are present after downgrading.

URL Public Key Signing

Table 3 describes the compatibility and results when using a prior CDS software release to perform URL signing and the current software release to perform URL validation.

Table 3 Release Compatibility of URL Signing and URL Validation

Release Used for URL Signing	Release Used for URL Validation	Results
2.3.x	2.4.3, 2.4.5, or 2.5.x	Not supported because the Release 2.3.x URL signing uses the port and schema for signing, but the Release 2.5.7 URL validation removes the port.
2.4.3	2.5.7	Supported for all URL signing versions, except version 3 (CSCtb99898).
2.4.5	2.5.7	Supported for all URL signing versions, except version 3 (CSCtb99898).
2.5.1 or 2.5.3	2.5.7	Supported for all URL signing versions.

Documentation Updates

The following documents have been added for this release:

- *Release Notes for Cisco Internet Streamer CDS 2.5.7*

The following documents have changed:

- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
- *Cisco Internet Streamer CDS 2.5 Software Configuration Guide*
- *Cisco Internet Streamer CDS 2.5 Command Reference Guide*
- *Cisco Internet Streamer CDS 2.5 Alarms and Error Messages Guide*

Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.5:

- *Cisco Internet Streamer CDS 2.5 Software Configuration Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/configuration_guide/is_cds25-cfguide.html
- *Cisco Internet Streamer CDS 2.4–2.5 Quick Start Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/quick_guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 2.4–2.5 API Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/developer_guide/is_cds_24_apiguide.html
- *Cisco Internet Streamer CDS 2.5 Command Reference Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/command_reference/Command_Ref.html
- *Cisco Internet Streamer CDS 2.5 Alarms and Error Messages Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/message_guide/Messages.html
- *Cisco Content Delivery System 2.x Documentation Roadmap*
  http://www.cisco.com/en/US/docs/video/cds/overview/CDS_Roadmap.html
- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
  http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html
- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide*
  http://www.cisco.com/en/US/docs/video/cds/cde/installation/guide/CDE_Install_Book.html
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*
  http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/CDE_RCSI.html

The entire CDS software documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps7127/tsd_products_support_series_home.html

The entire CDS hardware documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps7126/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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