Release Notes for Cisco Internet Streamer CDS 2.4.3

These release notes cover Cisco Internet Streamer CDS Release 2.4.3-b7.
Revised: August 2009, OL-20359-01

Contents

The following information is included in these release notes:

- Enhancements, page 2
- System Requirements, page 2
- Limitations and Restrictions, page 3
- Important Notes, page 3
- Open Caveats, page 5
- Resolved Caveats, page 8
- Upgrading to Release 2.4.3, page 10
- Documentation Updates, page 10
- Related Documentation, page 11
- Obtaining Documentation and Submitting a Service Request, page 12
Enhancements

Table 1 describes the enhancements to Internet Streamer CDS 2.4.3.

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL public key signing</td>
<td>Asymmetric key signing, also known as public key URL signing, always has a key pair made up of a public key and private key. The private key is used for signing and the public key is used for validation. New commands are added for configuring the public key and private key, and a C program is included for externally signing the URL.</td>
</tr>
<tr>
<td>Service Router cross-domain support</td>
<td>The Service Router supports crossdomain.xml and clientaccesspolicy.xml files for content access by remote domains.</td>
</tr>
<tr>
<td>SNMP enhancements</td>
<td>The following traps have been added:</td>
</tr>
<tr>
<td></td>
<td>• SE or SR goes offline</td>
</tr>
<tr>
<td></td>
<td>• Protocol engines reach their bandwidth threshold</td>
</tr>
<tr>
<td></td>
<td>• CPU, memory, or disk thresholds are reached on SE</td>
</tr>
</tbody>
</table>

Release 2.4.3 supports the CDE220 2G2 platform. See the “System Requirements” section for more information.

Note

The Proximity-Based Routing feature and the Flash Media Streamer DVR support are available as an early field trial release. For more information, contact your Cisco account representative.

Note

The Session Shifting feature is not supported in Release 2.4. For 3-Screen Session Shifting, use the Cisco Internet Streamer CDS 2.3 software.

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>
<thead>
<tr>
<th>Device Mode</th>
<th>CDE100</th>
<th>CDE200</th>
<th>CDE205</th>
<th>CDE220</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDSM</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SR</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SE</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Release 2.4.3 supports the CDE220 2G2 platform. There are a total of ten gigabit Ethernet ports in this CDE. 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 the CDE200 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 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.

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 recommend 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:

Windows Media Streaming

- CSCta25831
  Symptom:
  Windows Media Streaming core dumps during longevity testing.
  Conditions:
  When multiple bit-rates, live, VOD, and protocols are used and a server-side playlist (SSPL) is used as the live source.
  Workaround:
  None.

- CSCta04062
  Symptom:
  Some of the Windows Media files are partially cached during stress testing of cache misses for unique content.
  Conditions:
  When Windows Media Streaming Fast Cache is disabled.
  Workaround:

- CSCsx58932
  Symptom:
  Windows Media Streaming core dumps during testing of live streaming.
  Conditions:
  This happens when a server-side playlist (SSPL) source is used and automation scripts are used as clients.
  Workaround:
  None.

- CSCsq46063
  Symptom:
  Multiple stale outgoing sessions are displayed for the show statistics wmt streamstat command.
  Conditions:
  When an SSPL broadcast publishing point is stopped and a managed live Windows Media Streaming program is scheduled.
  Workaround:
  Stale sessions are removed periodically and do not impact streaming. Alternatively, you can enable the SSPL broadcast publishing point source.
Flash Media Streaming

- CSCta47619
  Symptom:
  The FMS core process generates a core dump file.
  Conditions:
  The core dump occurs once in awhile during high-stress scenarios (that is, when the CPU and disk thresholds are reached). The high-stressed scenario is coupled with both cache-hit and cache-miss traffic for MPEG-4 VOD Flash Media Streaming.
  Workaround:
  Set the disk and CPU thresholds to 80 percent, so that the system will not get overloaded (SR will not redirect any requests when threshold is reached) (Default is 80 percent).

  ```
  {config}# service-router service-monitor threshold cpu 80
  {config}# service-router service-monitor threshold disk 80
  ```
  Set all debug level to default.

  ```
  # no debug all set logging level to notice
  # sh logging
  Syslog to host is disabled.
  Syslog to console is disabled
  Priority for console logging is set to: notice
  Syslog to disk is enabled
  Priority for disk logging is set to: notice
  Filename for disk logging is set to: /local1/syslog.txt
  Syslog facility is set to *
  Syslog disk file recycle size is set to 10000000
  ```

- CSCsz75396
  Symptom:
  Flash Media Streaming edge server process keeps printing syslog message on console during SR RTMP performance test.
  Condition:
  Performance test conditions.
  Workaround:
  This syslog message occurs some times when Flash Media Server is not able to shutdown properly. This is not harmful message and only occurs during the fms disable command.

CDSM

- CSCtb24668
  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 negative it, a CLI with default value will still show in running config.

Workaround:
Configuring just works, please avoid to negative the configure before it is fixed.

- CSCsx19763
  Symptom:
  When an SE is reloading, the Flash Media Streaming Wholesale License page in the CDSM does not respond, the page is blank for several seconds, and a warning dialog box displays, “The creation/modification will not proceed.”
  Workaround:
  None. The issue does not impact the functionality of the CDSM. All pages except the Wholesale License page, are responsive.
  None. The CDSM recovers after about five minutes.

Platform

- CSCta27060
  Symptom:
  The link state of a switch port is always “up” when connected to a gigabit Ethernet over optical fiber interface on the SE. Depending on how the port channel and load-balancing are configured, this may cause the switch to send packets to a shut down interface on the SE.
  Conditions:
  When the shutdown command is manually entered on a gigabit Ethernet over optical fiber interface
  Workaround:
  Manually shut down the corresponding interface on the switch.

- CSCta22112
  Symptom:
  Changing the time zone to “daylight savings” (or “summer time”) does not take affect.
  Condition:
  Although the Internet Streamer CDS supports time-zone adjustments, changes to “daylight savings” (or “summer time”) do not occur “on-the-fly.”
  Workaround:
  To have the time-zone change for “daylight savings” (or “summer time”) take affect, reload the server.
Resolved Caveats

Acquisition and Distribution

- CSCta35923
  Symptom:
  CDNFS usage shows used storage on a Service Engine that has been unassigned from all delivery services.
  Condition:
  Content not removed from Service Engine that has been unassigned from all delivery services.
  Workaround:
  Use the `cdnfs cleanup start` command to remove the content that remained after unassigning the SE from all delivery services.

URL Signing

- CSCtb16478
  Symptom:
  RTSPD core dumps when url validation is done using private key signing when URL is signed using public key
  Condition:
  RTSPD core dump happens and requests are not served.
  Workaround:
  Validate the URL using the same method used when generating the signature.

Service Router

- CSCtb16643
  Symptom:
  Service router failed to redirect client request.
  Condition:
  When curl is used as the browser.
  Workaround:
  Use wget instead of curl.

Resolved Caveats

The following caveats have been resolved since Cisco Internet Streamer CDS Release 2.4.1 Not all the resolved issues are mentioned here. The following list highlights the resolved caveats associated with customer deployment scenarios.
Flash Media Streaming

- CSCsz14232
  Symptom:
  If the maximum bandwidth for Flash Media Streaming is reduced, Flash Media Streaming does not honor the configuration for first two minutes after the configuration change.

Web Engine

- CSCta60227
  Symptom:
  Web Engine replies with wrong cache-status for Flash Media Streaming request in corner case.
- CSCtb10115
  Symptom:
  Query string in multicast reference URL fails.

CDSM

- CSCta78893
  Symptom:
  Inconsistency between default values in CLI and CDSM for port channel configuration.
- CSCtb14034
  Symptom:
  Some SNMP settings are not compatible between Release 2.3 and Release 2.4.

Authorization Server

- CSCta85678
  Symptom:
  SE returning "403 Forbidden" for dynamically cached content.
Upgrading to Release 2.4.3

The only supported upgrade paths are Release 2.4.1 to Release 2.4.3 and Release 2.3.x to Release 2.4.3. If you are running a release prior to Release 2.3.x, you must upgrade to Release 2.3.x before upgrading to Release 2.4.3.

Note
An SR running the Release 2.4 software is not compatible with an SE running the Release 2.3.x software. We strongly recommend that you upgrade your CDS network devices in the following order:

1. Multicast sender Service Engines
2. Multicast receiver Service Engines
3. Non-Content Acquirer Service Engines
4. Content Acquirer Service Engines
5. Service Routers
6. Standby CDSMs (Upgrade before primary when using the GUI only.)
7. Primary CDSM

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>
<thead>
<tr>
<th>Release Used for URL Signing</th>
<th>Release Used for URL Validation</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.x</td>
<td>2.4.3, 2.4.5, or 2.5.x</td>
<td>Does not work because the Release 2.3.x URL signing uses the port and schema for signing, but the port is stripped off during validation by the current software release.</td>
</tr>
<tr>
<td>2.4.1</td>
<td>2.4.3</td>
<td>Works for URL signing version 0, 1, or 2. URL signing version 3 is the new version introduced in Release 2.4.3 for the public/private key signing.</td>
</tr>
</tbody>
</table>

Documentation Updates

The following documents have been updated for this release:

- Cisco Internet Streamer CDS 2.4 Software Configuration Guide

The following documents have been added for this release:

- Release Notes for Cisco Internet Streamer CDS 2.4.3

The following documents have no changes:
Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.4:

- Cisco Internet Streamer CDS 2.4 Software Configuration Guide
- Cisco Internet Streamer CDS 2.4 Quick Start Guide
- Cisco Internet Streamer CDS 2.4 API Guide
- Cisco Internet Streamer CDS 2.4 Command Reference Guide
- Cisco Internet Streamer CDS 2.4 Alarms and Error Messages Guide
- Cisco Content Delivery System 2.x Documentation Roadmap
- Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide
- Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide
- Regulatory Compliance and Safety Information for Cisco Content Delivery Engines

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

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


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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting