Release Notes for Cisco ECDS 2.5.6

Revised: May 14, 2013
OL-24532-03

These release notes support all Cisco Enterprise Content Delivery System (Cisco ECDS) 2.5.x releases and contain the most current system information.

Contents

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

New Features

The following sections contain new feature information:

Features in Software Versions

Table 1 lists Cisco ECDS software versions and feature support.

Table 1 Cisco ECDS Software New Feature Support

Software Version	New Feature
2.5.6 2.5.5 (S1) 2.5.3 (S5)	• Cisco MDE 1125, Cisco MDE 3125 - Next-generation ECDS Appliances (based on Cisco UCS C220 M3 rack servers).
2.5.5	• WCCP transparent caching with HTTPS support. You have a choice to use the Cisco ECDS with WCCP in Release 2.5.5 See WCCP for Request Routing. • Storage enhancement for the Cisco MDE 1100 Series adds support for 2 or 4 drives/disks. See the "Cisco MDE 1100 Series" section on page 15.
2.5.3 (S4)	• MDE 10XVB—Introduces support for generic, ESXi-based virtual machines. • MDE 50WVB—Extends WAAS VB support to the WAE 294, WAE 594, and WAE 694 platforms. • Support for Apple HTTP Live Streaming. See the *Cisco ECDS 2.5 Software Configuration Guide* to enable Apple HLS.
2.5.3 (S3)	Introduces support for MDE 50IVB.
2.5.3 (S2)	Introduces support for MDE 3100.
2.5.3 (S1)	Introduces support for MDE 50WVB.
2.5.3	Supports the MDE 1100 Series.

Cisco MDE UCS Chassis Support

The Cisco MDE 1125 and Cisco MDE 3125 are the next-generation ECDS appliances based on Cisco UCS rack servers.

Cisco MDE 1125

The MDE 1125 holds up to four 2.5 inch hard drives (small form factor, SFF drives).

Cisco MDE 3125

The MDE 3125 is delivered with eight 2.5 inch hard drives (small form factor, SFF drives).

See the following sections:

- Supported Software, page 3
- Unsupported Software, page 3
- Spare Support, page 4

Supported Software

The Cisco MDE 1125 and Cisco MDE 3125 are supported on Cisco ECDS Software Release 2.5.3 (S5), 2.5.5 (S1) and 2.5.6. Use the following part numbers when ordering:

- MDE-1125-K9
- MDE-3125-K9
- MDE-1125-K9= (Spare, without the hard drives)
- MDE-3125-K9= (Spare, without the hard drives)

The Cisco MDE 1125 and Cisco MDE 3125 use the following software images:

- 2.5.3 s5 b8xx
- 2.5.5 s1 b1xx
- 2.5.6 s1 b1xx

Unsupported Software

Prior versions of Cisco ECDS 2.5.3 and 2.5.5 are not supported on the new Cisco MDE platforms, for example:

- 2.5.3 images with b# where # is less than 800
- 2.5.5 images with b# where # is less than 100

Note The system does not block installation of unsupported images. For best results, do not install unsupported software versions. If installation of prior image versions occurs, recover your system with the *mfg-cdrom iso* or *rescue-cdrom iso* supported image version.

Spare Support

The Cisco MDE 1125 and Cisco MDE 3125 spare is only available with Cisco ECDS Software Release 2.5.3(S5). If your chassis shipped with Cisco ECDS Software Release 2.5.5, you must either re-image the flash drive to release 2.5.3(S5) or run the upgrade to release 2.5.3(S5). Contact your Cisco representative for support information.

WCCP for Request Routing

To address networking challenges for enterprises, traffic patterns content requests can be fulfilled locally using WCCP with transparent caching. In previous Cisco ECDS software releases, DNS changes were required and additional work was necessary to change existing URLs to fit into the Cisco ECDS service routing-based caching solution. Cisco ECDS Release 2.5.5 introduces WCCP and transparent proxy for all supported media protocols in Cisco ECDS.

WCCP can be used with Cisco content caching engines and third-party proxy servers, Web caching, and content filtering appliances. Cisco ECDS 2.5.5 works with WCCP Version 2 to support unmanaged video caching and Application and Content Networking System (ACNS) migration.

The following is supported:

- WCCP Services—HTTP, HTTPS, RTSP, RTMP, WMT, Custom Web-Cache, and Dynamic services
- WCCP Redirect—GRE and L2
- WCCP Assignment—Hash and Mask
- WCCP Bypass—Static, load, and port exception server
- FMS
  - Flash Media Server support
  - Application name changes: **vod-ecds** and **live-ecds**
- WMT—WMT proxy bypass

To enable WCCP in the Cisco Enterprise CDSM, choose **Devices > Request Routing > WCCP**.

See the following documents for complete information:

- *Cisco ECDS 2.5 Software Configuration Guide*
- *Cisco ECDS 2.5 Command Reference*

HTTPS Secure Delivery Service

When WCCP is enabled, HTTPS becomes an option in the delivery service content source URL configuration. The Content Acquirer fetches content using HTTPS and distributes ECDS content securely.

The following is supported:

- Web Engine
  - HTTPS certificate management
  - HTTP proxy bypass
  - IP spoofing
  - Max-min cacheable objects

- Cache-query string
- Cache-nonreachable
- Cache-fill-range

To access HTTP Connections in the Cisco Enterprise CDSM, choose **Devices > Application Control > Web > HTTP > HTTP Connections**.

HTTPS can only be enabled when WCCP service is enabled. Follow these steps to ensure proper configuration:

1. First, make sure WCCP is *not* enabled by entering the **show wccp status** command.
2. Create all the certificates, keys, and certificate groups on the same service engine in the Cisco ECDSM.
3. Enable the HTTPS server and check HTTPS server status on SE CLI by entering the **show https server** command.
4. Now enable WCCP service for the SE from the Cisco CDSM.

See the following documents for complete information:

- *Cisco ECDS 2.5 Software Configuration Guide*
- *Cisco ECDS 2.5 Command Reference*

New and Changed CLI Commands

Table 2 lists command support added in Cisco ECDS Release 2.5.5 and 2.5.6.

Table 2 Cisco ECDS 2.5.5 and 2.5.6 WCCP and Supported New and Changed Commands

Command	Description
New Commands	
alarm nic-shutdown-alarm	Generates an alarm when the NIC interface is shut down.
bypass	Configures the bypass functions.
https (EXEC)	Manages certificates, certificate groups, and private keys when using the Service Engine as an HTTPS server: **https cert—**Creates certificate objects with a given name, imports a certificate from external sources into a certificate object, or removes existing certificate objects. **https certgroup**—Creates or removes certificate groups or imports a certificate from an external source to add it to an existing certificate chain.
https server	Configures the Service Engine to act as an origin HTTPS server.
show bypass list	Determines whether the origin HTTPS server has been added to the WCCP accept list.
show https	Displays HTTPS proxy status and port policies.
show statistics wccp	Displays the WCCP statistics for the Service Engine.
show wccp	Displays Web Cache Communication Protocol (WCCP) information.
show interface all	Displays details of interfaces.

Table 2 Cisco ECDS 2.5.5 and 2.5.6 WCCP and Supported New and Changed Commands

Command	Description
wccp custom-web-cache	Enables the Service Engine to accept redirected HTTP traffic on a port other than 80.
wccp flow-redirect	Enables Web Cache Communication Protocol (WCCP) flow redirection
wccp https-cache	Enables Web Cache Communication Protocol (WCCP) flow redirection to a Service Engine configured as an HTTPS server
wccp port-list	Associates ports with specific Web Cache Communication Protocol (WCCP) Version 2 dynamic services.
wccp router-list	Configures a router list for Web Cache Communication Protocol (WCCP) Version 2.
wccp rtmp	Configures Web Cache Communication Protocol (WCCP) Version 2 Real-Time Messaging Protocol (RTMP) media stream transparent interception.
wccp rtsp	Configures Web Cache Communication Protocol (WCCP) Version 2 Real-Time Streaming Protocol (RTSP) protocol transparent interception.
wccp service-number	Enables up to eight dynamic Web Cache Communication Protocol (WCCP) redirection services on the Service Engine
wccp shutdown	Sets the maximum time interval after which the Service Engine will perform a clean shutdown of Web Cache Communication Protocol (WCCP)
wccp slow-start	Enables the slow-start capability of the caching service on the Service Engine with Web Cache Communication Protocol (WCCP).
wccp version	Specifies the version of Web Cache Communication Protocol (WCCP) that the Service Engine should use. The ECDS uses only Version 2.
wccp web-cache	Configures the router to run the web cache service with Web Cache Communication Protocol (WCCP) Version 2.
wccp wmt	Configures the router to run the web cache service with Web Cache Communication Protocol (WCCP) and Windows Media Technologies (WMT).
wccp wmt-rtspu	Configures Web Cache Communication Protocol (WCCP) Version 2 WMT Real-Time Streaming Protocol (RTSP) transparent interception.
wmt proxy outgoing	Configures outgoing bypass proxy lists: **wmt proxy outgoing http bypass**—HTTP Proxy Bypass list **wmt proxy outgoing rtsp bypass**—RTSP Proxy Bypass list
Changed Commands	

Table 2 Cisco ECDS 2.5.5 and 2.5.6 WCCP and Supported New and Changed Commands

Command	Description
service-router service-monitor	The **service-router service-monitor** command is changed to **service-monitor** in Cisco ECDS Release 2.5.5 and 2.5.6
flash-media-streaming	The **flash-media-streaming** command has changed for configuring the virtual-path for VOD applications. The new parameter is **vod-ecds**, as shown in the following example that maps a VOD folder to media: `SE(config)# flash-media-streaming application-virtual-path vod-ecds map media` The **live** keyword is changed to **live-ecds** in Cisco ECDS Release 2.5.5 and 2.5.6. This parameter manages the aggregated live stream in Live applications to Flash Media Streaming.

Configuration Changes Since Last Release

Table 3 describes hardware and software administration information that has changed since last release.

Table 3 Administration Changes

Topic	Description	Change
Cisco MDE spares replacement	A spare unit is intended to recover content on Cisco ECDS hard disks when the Cisco MDE unit itself is damaged but the hard disks are ok.	A new section has been added to the Cisco Media Delivery Engine 1100 Series and Cisco Media Delivery Engine 3100 Series hardware installation guides that describes how to configure a replacement unit. See the following documentation on Cisco.com: • *Cisco Media Delivery Engine 1100 Series Hardware Installation Guide* • *Cisco Media Delivery Engine 3100 Series Hardware Installation Guide*
NIC shutdown alarm management	By default, the minor alarm, Network Interface Controller (NIC) shutdown, is not displayed in either the **show alarms** command output or in CDSM reporting.	You can enable NIC alarm reporting through either the CLI on the SE or by using the CDSM administration GUI. Use the **alarm nic-shutdown enable** command. **Tip** After configuring the setting, you may need to wait a few minutes before the alarm is no longer shown in **show alarms** output. The CDSM administration GUI navigation has been changed: **Devices > General Settings > Notification and Tracking > Alarm Settings**. The "Alarm Overload Detection" check box is available on the Alarm Settings for Service Engine page.

Service Engine CLI Setup Wizard in Cisco ECDS Release 2.5.5 and 2.5.6

Typically when a device is first brought up, you would first run the Setup Wizard on the Service Engine CLI to configure basic settings. One of these settings is the device mode change where you can change the device mode to service-router or CDSM for example.

In Cisco ECDS Release 2.5.5 an 2.5.6, the device mode change in the Setup Wizard does not work. Instead, you must manually configure the device mode before running the Setup Wizard.

To manually configure the device mode on the SE upon first startup:

1. Enter the following command:

```
se(config)# device mode [device-mode]
```

2. Follow the directions in the prompts.
3. Restart the device when instructed.

   After restarting the device, the device mode should be correctly configured and you can run the Setup Wizard as normal.

Tip Any device-mode configurations should always be done manually.

Cisco ECDS Application Support and Recommended Software

Table 4 describes the Cisco ECDS application supported on each Cisco ECDS platform and the recommended software version.

For best results, the following is recommended:

- Use the most current version of the software. See Table 4 for recommendations per platform.
- You should use the same software release across your deployment.
- Generally, downgrade to a lower version is not required or necessary and can render your system unusable.

Note Downgrade from Cisco ECDS Release 2.5.5 and 2.5.6 to an earlier release is not supported.

- Cisco ECDS 2.5.5 and 2.5.6 is the current recommended version:
  - Supports WCCP/HTTPS
  - Applies to all Cisco ECDS platforms and can be used for device group upgrade with mixed platforms.
  - Supports the Cisco ECDS 2.5.5 and 2.5.6 rescue image if a device goes to a bad state and rescue is required.

Table 4 Cisco ECDS Application Support by Platform

Platform	Enterprise Content Delivery System Manager	Service Router	Service Engine	Content Acquirer	Supported Software
MDE 3125	Y	Y	Y	Y	2.5.6, 2.5.5 (S1) 2.5.3 (S5)
MDE 1125	Y	Y	Y	Y	2.5.6, 2.5.5 (S1) 2.5.3 (S5)

Table 4 Cisco ECDS Application Support by Platform

Platform	Enterprise Content Delivery System Manager	Service Router	Service Engine	Content Acquirer	Supported Software
MDE 3125 MDE 3100	Y	Y	Y	Y	2.5.6 2.5.5 2.5.3 (S5) (3125 only) 2.5.3 (S4) (3100 only) 2.5.3 (S3) (3100 only) 2.5.3 (S2) (3100 only)
MDE 1125 MDE 1100	Y	Y	Y	Y	2.5.6 2.5.5 2.5.3 (S5) (1125 only) 2.5.3 (S4) (1100 only) 2.5.3 (S3) (1100 only) 2.5.3 (S2) (1100 only)
MDE 10XVB	N	N	Y	N	2.5.6 2.5.5 2.5.3 (S4)
MDE 50WVB	N	N	Y	N	2.5.6 2.5.5 2.5.3 (S4) 2.5.3 (S3) 2.5.3 (S2)
MDE 50IVB	N	N	Y	N	2.5.5 2.5.3 (S4) 2.5.3 (S3)

Cisco ECDS Software Version Compatibility by Platform

Table 5 describes the Cisco ECDS software release versions and the applicable base minimum software for the applicable hardware platforms.

Table 5 Cisco ECDS Software Compatibility by Platform

Software Release	Media Delivery Engine							Base Platform Software
	10XVB	MDE 1100	MDE 3100	MDE 1125	MDE 3125	50WVB	50IVB (N)	
2.5.6 (N)	Y	Y	Y	Y	Y	Y	Y	• vECDS PCs running ESXi4.1 or ESXi5.0 • ISR29xx and ISR39xx: 15.1(4)M1 SRE-V Up to 2.0.0.10 • MDE 1100, MDE 3100, MDE 1125, MDE 3125 • WAVE294 / WAVE594 / WAVE694:4.4.1.12 • WAVE574 / WAE674:4.4.3.4
2.5.5	Y	Y	Y	Y	Y	Y	Y	• vECDS PCs running ESXi4.1 or ESXi5.0 • ISR29xx and ISR39xx: 15.1(4)M1 SRE-V Up to 2.0.0.10 • MDE 1100, MDE 3100, MDE 1125, MDE 3125 • WAVE294 / WAVE594 / WAVE694:4.4.1.12 • WAVE574 / WAE674:4.4.3.4
2.5.3 S4	Y	Y	Y	Y	Y	Y	Y	• vECDS PCs running ESXi4.1 or ESXi5.0 • ISR29xx and ISR39xx: 15.1(4)M1 SRE-V Up to 2.0.0.10 • MDE 1100, MDE 3100, MDE 1125, MDE 3125 • WAVE294 / WAVE594 / WAVE694:4.4.1.12 • WAVE574 / WAE674:4.4.3.4

Table 5 Cisco ECDS Software Compatibility by Platform

Software Release	Media Delivery Engine							Base Platform Software
	10XVB	MDE 1100	MDE 3100	MDE 1125	MDE 3125	50WVB	50IVB (N)	
2.5.3 S3	N	Y	Y	N	N	Y	Y	• ISR29xx and ISR39xx: 15.1(4)M1 SRE-V 1.5.1.0 • MDE 1100, MDE 3100 • WAVE574 and WAE674: 4.2.3.7
2.5.3 S2	N	Y	Y	N	N	Y	N	• WAVE574 and WAE674: 4.2.3.7 • MDE 1100, MDE 3100
2.5.3 S1	N	N	N	N	N	Y	N	• WAVE574 and WAE674: 4.2.3.7
2.5.3	N	Y	N	N	N	N	N	• MDE 1100, MDE 3100

Note The MDE 1100 and MDE 3100 hardware End-of-Life was announced in August, 2012 replaced by the higher performance MDE 1125 and smaller form factor MDE 3125. None of the above software releases are at End-of-Life and continue to be supported on the MDE 1100 and MDE 3100 as applicable.

Note Customers can elect to have either 2.5.3 or 2.5.5 software installed on the MDE1125 and MDE 3125 at the time of manufacturing.

Obtaining and Upgrading Software

To upgrade your Cisco ECDS platform to the latest software supported on the platform, contact the Cisco Technical Assistance Center (TAC). See the "Obtaining Documentation and Submitting a Service Request" section on page 22.

Refer to the *Cisco ECDS 2.5 Software Configuration Guide* on Cisco.com for upgrade instructions.

Unsupported Software Features

The following features may appear in the Cisco Enterprise CDSM or CLI interfaces or be supported in WCCP in general but are not supported in this release of Cisco ECDS software:

- Unsupported in Cisco ECDS, page 13

Unsupported in Cisco ECDS

- DVRCAST
- ICAP
- IP-based Redirection
- IP multicast routing
- Geo-Location Server integration
- Proximity Server
- PCMM
- RTMPT
- RTMPTE
- Session Shifting
- Show and Share over SSL
- URL Signing
- Wholesale licensing
- Windows Media Services Multi Bit Rate
- Access Control Lists with WCCP
- Bypass Error handling with WCCP
- Encrypted private keys for configuring the HTTPS server with WCCP
- HTTPS without WCCP
- IP ACL with WCCP
- IP multicast routing with WCCP
- IP Spoofing with non-HTTP protocols or multiple Service Engines with WCCP
- L4 Switch for the bypass gateway with WCCP
- Reverse proxy with WCCP
- RTMP unmanaged domain with WCCP
- Security proxy with WCCP
- WCCP CIF/FTP/DNS traffic caching with WCCP
- WCCP Web cache packet return with WCCP

Limitations and Restrictions

Observe the following limitations and restrictions in this release:

- Cisco ECDS-SRE9x0_RAID0.ova Deployment with vSphere, page 14
- HTTP Request Header Size, page 14
- NAT Devices, page 14

Cisco ECDS-SRE9x0_RAID0.ova Deployment with vSphere

Make sure that the system from which you deploy the RAID 0.ova file is running natively on hardware, or is controlled through a remote desktop. There is an issue with deployment if there are nested vSphere instances in which vSphere is running on the VM controlled through vSphere. In this case the Cisco SRE VM is deployed using vSphere from a Windows 2008 server VM. The Windows 2008 server VM is controlled from the console window of another vSphere client, therefore creating a nesting environment and the deployment fails.

HTTP Request Header Size

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.

NAT Devices

There is no network address translation (NAT) device separating the MDEs from one another.

Cisco ECDS does not support NAT configuration, where one or more MDEs are behind the NAT device or firewall. If your Cisco ECDS network is behind a firewall, workaround this issue by configuring each internal and external IP address pair with the same IP address.

Cisco ECDS 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 Cisco ECDS network and the client device. However, the NAT device or firewall must support RTP/RTSP.

Cisco ECDS Configuration Tips

Use the following configuration tips to help you manage your system. For more information, see the *Cisco ECDS 2.5 Software Configuration Guide* on Cisco.com.

Encoders with Variable Bit Rates

We recommend that customers with variable bit rates cap the bit rate at the encoder to avoid bit rate spikes, which may result in throughput exceeding the supported throughput allowed in the Cisco ECDS. Use the **show bitrate** [**movie-streamer** | **wmt**] command in Privileged EXEC mode to display the bit rate allocated to a particular device. Use the **bitrate** command in Global configuration mode to configure the maximum pacing bit rate for large files for the Movie Streamer and to separately configure WMT bit-rate settings.

Hybrid Ingest

In the current release, the origin server OFQDN is always used, and the hostname/port in the Manifest file is ignored.

NTP Configuration

When configuring network settings on your Service Engine, make sure that you configure NTP in **General Settings** > **Network** > **NTP** and enter the **ntp server** <*ntp-server-IP*> command. This enables the Service Engine to work properly with Flash Media Streamer and successfully sync with CDSM.

WCCP and Streaming Interfaces

WCCP always binds to the first interface. The streaming interface can still be configured for service routing.

Cisco MDE Support

Cisco MDE 3100 Series

Observe the following recommendations for the Cisco MDE 3100 Series:

CIMC RAID Support

CIMC RAID management is not supported. The appliance drives do not appear on the CIMC **Inventory** > **Storage** screen.

KVM Console Support

By default, console output is available on the KVM console connector on the front of the appliance and the serial connector on the rear of the appliance. Enabling Serial-over-LAN in CIMC disables the console output on the serial connector on the rear of the appliance. You can still obtain console output from a CIMC console session or from the KVM console connector on the front of the chassis.

Spares Support

A spare unit is intended to recover content on Cisco ECDS hard disks when the Cisco MDE unit itself is damaged but the hard disks are ok. For complete information about managing spares, see the Cisco Media Delivery Engine 3100 Series Hardware Installation Guide.

Cisco MDE 1100 Series

Observe the following recommendations for the Cisco MDE 1100 Series:

Cisco MDE Disk Drive Support

The Cisco MDE 1125 supports two, three or four 500 GB SATA 7.2 RPM 2.5" hard drives (HDDs), for a maximum storage of 1, 1.5 or 2 TB. This is a configurable option at the time of ordering. Additional HDDs can be added up to the four total. The part number for additional or spare HDDs is: MDE-HD2GC3-500GB=.

Table 6 Cisco MDE 1125 Hard Drives

Supported Drive	Part Number	Number of Disks	ECDS Software Release	Storage Space
500 GB SATA 7.2 RPM 2.5" HDD	MDE-HD2GC3-500GB=	2	2.5.3 (S5), 2.5.5 and 2.5.6	929.4 GB
		3	2.5.3 (S5), 2.5.5 and 2.5.6	1394.1 GB
		4	2.5.3 (S5), 2.5.5 and 2.5.6	1858.8 GB

Disconnect USB Devices

Disconnect any external USB devices (such as drives and keyboards) before powering on the appliance. Your appliance may not boot with devices connected to the external USB ports.

Maximum Content Delivery

To maximize the content delivery performance of an MDE 1100 Series appliance, do the following:

- Use port channel for the primary and streaming interface.

  Configure the gigabit Ethernet interfaces into a single port-channel interface. Use this interface for all client-facing and administrative traffic. Refer to the *Cisco ECDS 2.5 Software Configuration Guide* for detailed instructions.

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

  Assuming port-channel is used between the upstream router/switch and the SE for streaming real-time data, the port-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.

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

  If you have enough client WMT traffic to saturate the MDE capacity, we recommend that you provision a dedicated MDE to handle WMT; and likewise for HTTP. In such cases, we do *not* recommended that you mix the two traffic types on all MDE servers which could result in suboptimal aggregate performance and require more MDE servers than usual.

- 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 Cisco Enterprise CDSM.

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.

- 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.

NIC Settings

Do not change the Network Interface Controller (NIC) mode or NIC redundancy settings when configuring Cisco Integrated Management Controller (CIMC) network settings. The supported settings are:

- **NIC Mode**: Dedicated
- **NIC Redundancy**: None

Spares Support

Information about managing spares. See Configuration Changes Since Last Release.

Cisco MDE 50WVB

Portchannelling is not supported on the Cisco MDE 50WVB.

Cisco MDE 10XVB

Disk Space on the Virtual Machine

For best results, delete unused files and reduce unnecessary storage to conserve memory allocation on the Cisco ECDS running on the VM. If you have difficulty powering on the device or the system warns of no space left on the device, reduce the memory allocation then boot the device and delete files from the server.

Cisco MDE 50IVB

Portchannelling is not supported on the Cisco MDE 50IVB.

Caveats and Known Issues

Known Issues

Apple HTTP Live Streaming

Apple HLS may experience poor video quality when sending 50 Client requests using IxLoad client simulator on the Mac Mini. To work around this potential problem, use the Cisco Media Processor (formerly Spinnaker Inlet Encoder) to send Client requests. See the Cisco AS5100 Series Media Processor support page for more information. For information about configuring Apple HLS in Cisco ECDS, see the *Cisco ECDS 2.5 Software Configuration Guide* on Cisco.com.

FMS Allocated Cache Size

If the flash-media-streaming cache is near maximum, the system may be unable to cache completely. The **show flash-media-streaming cache content** command output may be missing content and the system will issue an error message. The problem occurs when a single file is greater than the size of the flash-media-streaming allocated cache.

Caveats in Cisco ECDS 2.5.6

Resolved Caveats

Table 7 lists the caveats that are resolved in the current release.

Table 7 Caveats Resolved in Cisco ECDS 2.5.6

Identifier	Description
CSCua37007	ECDS authentication configuration command information is not explained in detail in Configuration guide.
CSCuf81414	ECDS 2.5.5 documentation did not have the live code application name change mentioned.
CSCuf81445	Detailed documentation on Live Streaming for WCCP is missing in ECDS Configuration guide.
CSCuf51468	CDSM: WCCP Select Assignment Method field is disabled for RTSP and RTMP.
CSCuc44621	ECDS IfInOctet and IfOutOctet counters do not reset to 0 after reaching the maximum 32-bit number.
CSCtz94461	'Show interface' command is not available in the device to show all interfaces.
CSCtz94452	Password policy is too restrictive. The special character "@" is not allowed.
CSCua81791	TACACS user can login and is in config mode even with no auth config.
CSCua25394	'snmp-server access-list < name >' not listed in the CLI prompt.
CSCty45216	Tacacs key is displayed in clear text during startup-config.
CSCud95933	Windows Media Streaming Engine cannot handle streams with stream number greater than 32.

Note The above list does not include all the bugs resolved, but only the bugs which will affect the customer deployment.

Open Caveats

Table 8 describes open caveats in Cisco ECDS 2.5.6.

Table 8 Open caveats in ECDS 2.5.6

Identifier	Description
CSCuf78061	Liveness queries are collected in WE transaction logs in Acquirer. **Symptom** Liveness queries are seen in transaction logs. Only client-served request should be collected in transaction logs. **Conditions** In Acquirer service engine (SE), liveness queries are seen in transaction logs when enabling transaction logs in SE, sending request for small files and checking the transaction logs in Acquirer. **Workaround** None
CSCuf49783	TACACS user login behavior is inconsistent. **Symptom** After rebooting the service engine (SE), user is unable to login with TACACS username and password. **Conditions** User should be able to login without configuring TACACS key every-time after rebooting the SE. **Workaround** After rebooting SE, login with local user; go to configure mode and enter TACACS key, then TACACS user will be able to login.
CSCue44689	Error message is shown when crawl length is 1 and the directory is inaccessible. **Symptom** Receiving service failure error as “cannot replicate a particular directory” when crawl length is 1. **Conditions** Since only specific file types, i.e.,wmv/.wma can be cached and the directory is beyond the crawl depth, the error message “Error = Critical: Replication Status is Failed” is displayed when accessing the folder. **Workaround** None.
CSCuf89985	SNMP V3 authentication key is displayed in clear text during startup-config **Symptom** SNMP V3 authentication key is displayed in clear text during startup-config. **Conditions** The authentication key should be in encrypted text. **Workaround** None.

Table 8 Open caveats in ECDS 2.5.6

Identifier	Description
CSCuf73595	SNMP access-list feature need to be added in IP ACL Feature page. **Symptom** Configuring SNMP access-list via cli does not reflect in CDSM GUI. **Conditions** None. **Workaround** None.
CSCug01393	Cisco IT SR 625355611 running ECDS 2.5.5 Qualys vulnerability QID 38143 **Symptom** QID 38143 - SSL Server Allows Cleartext Communication Vulnerability which indicates that the server allows HTTPS/SSL connections without a cipher, i.e. no encryption. **Conditions** The customer has upgraded to 2.5.5 (from 2.5.3 for bugs that were fixed). The customer confirmed that ECDS 2.5.5 is vulnerable by the qualys security QID 38143 and was able to confirm this behavior in one of ECDS devices as shown below: openssl s_client -connect aer01-ecds-se1:443 -cipher eNULL. **Workaround** Based on the information given in the below Reports: http://forums.novell.com/novell-product-discussions/collaboration/groupwise/groupwise-6x/gw6-webaccess/93627-web-access-through-apache2-using-ssl-still-clear-text.html http://www.scribd.com/doc/92697163/Vulnerability-Remediation-Synopsis The following lines are added to either the httpd.conf or the ssl.conf config files. SSLProtocol: -ALL +SSLv3 +TLSv1 SSLCipherSuite: ALL:!ADH:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+ME DIUM

Caveats in Cisco ECDS 2.5.5 and 2.5.3

For more information on caveats in Cisco ECDS 2.5.5, refer the URL http://www.cisco.com/en/US/docs/video/ecds/2.5/release_notes/ecds253rn.html#wp74654

Related Documentation

For complete document support for the Cisco Media Delivery Engine appliances and the Cisco Enterprise Content Delivery System, see the *Documentation for the Enterprise Content Delivery System (Cisco ECDS)* document roadmap at the following link:

http://www.cisco.com/en/US/docs/video/ecds/documentation.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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.