



# Release Notes for Cisco TV CDS 2.4.2

---

These release notes cover Cisco TV CDS Release 2.4.2.

**Revised: October 2011 OL-24427-02**

## Contents

The following information is in the release notes:

- [New Features, page 2](#)
- [Enhancements, page 2](#)
- [Supported Environments, page 5](#)
- [System Requirements, page 5](#)
- [Limitations and Restrictions, page 6](#)
- [Important Notes, page 7](#)
- [Open Caveats, page 8](#)
- [Resolved Caveats, page 9](#)
- [Upgrading to Release 2.4.2, page 11](#)
- [Rollback from Release 2.4.2, page 16](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)



---

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

© 2010 Cisco Systems, Inc. All rights reserved.

# New Features

The following new features are supported in Release 2.4.2:

- CDE250-2G3 Cache Server Configuration
- New hardware:
  - CDE250-2S5, with 12 drive SSD
  - CDE250-2S6, with 24 drive SSD
  - CDE250-2G3, with 24 drive HDD

The new hardware platforms are all based on the same motherboard and have the same add-in cards and memory and cpu configurations.

# Enhancements

The following enhancements have been added in Release 2.4.2:

## CDSM and Platform Enhancements

2.4 brings a number of new screens and features to the CDSM. These changes are specifically targeted to managing the new features and deliverables in the 2.4 release. The 2.4 release is primarily a hardware only release with limited software changes to support the new hardware. It is expected at the initial rollout that CDSM and new streamers will run the 2.4 software, however, existing gen1 and gen2 will not be upgraded to the 2.4 release and they were need to interoperate until the 2.5 release is ready.

## Console Baud Rate

The console baud rate has been changed from 115200 to 9600. This change is only active on Merced platforms, previous systems will continue to have 115200 baud rate.

Two files on the system are changed as a result of this:

```
/etc/grub.conf  
/etc/inittab
```

The console baud rate in these files will be changed to 9600 when the cdsinstall in run on a merced device.

## Cdsinstall

There is no changes in the cdsinstall options or output. But when cdsinstall is run, it will check the Serial Number in demidecode output, and changes the console baud rate in /etc/grub.conf and /etc/inittab to 9600.

## cdsconfig

Cdsconfig is enhanced to support CDE250-2S5, CDE250-2S6 and CDE250-2G3. For the Merced Platforms, the Serial Number in the dmidecode output will be "CDE250-V01-01234567890-HVY". When the cdsconfig is run on a merced platform, user will be prompted to select a platform from a list that is valid for Merced. Once the user selects the platform, and the rest of the steps in cdsinstall, the selected platform will be written to /home/isa/.arroyorc as the part number.

## Part Number Selection

For the Merced Platforms, the Serial Number in the dmidecode output will be "CDE250-V01-01234567890-HVY". When the cdsconfig is run on a merced platform, user will be prompted to select a platform from a list that is valid for Merced.

## Rc.local changes for IPMI

Cdsconfig also adds the following line to the rc.local file on a Merced Platform :

```
#/usr/sbin/enable_ipmi.sh
```

This line should be uncommented and the server should be rebooted after the cdsconfig is completed. This will result in the script /usr/sbin/enable\_ipmi.sh be invoked to load all the additional IPMI drivers on a Merced box.

## Configuration Changes

### Interface Setup

The Configure > Server Level > Interface Setup page for all Merced servers is the same as depicted in the screen shot below. This page is configured the same way as previous generations of CDS hardware.

### Server Setup

Like the Interface Setup page above, the Configure > Server Level > Server Setup page is configured just as it has been for previous CDS platforms. However, due to the 10Gig ports supported on the Merced servers, the server map 15 table for the Merced servers gets written with the tportX value == 3 for the 10Gig ports, all other ports are set as previous. There is no user interaction required for this, it is done in an automatic fashion based on the part number.

### Setupfile Changes

When generating configurations on the system, additional parameters will be added specifically for Merced systems.

### 10G Adapters

The Merced system now supports 10 Gigabit Ethernet adapters. Therefore additional configuration in the setup file will be present to support those adapters. The format of the data is as follows:

```
ixgbe adapters: maxrate 9850
ixgbe 0: streaming 1 fill 1 ip 192.169.132.155 tport 0 cport 0 tgid 0
ixgbe 1: streaming 1 fill 1 ip 192.169.132.156 tport 0 cport 0 tgid 0
ixgbe 2: streaming 1 fill 1 ip 192.169.132.217 tport 0 cport 0 tgid 0
ixgbe 3: streaming 1 fill 1 ip 192.169.132.218 tport 0 cport 0 tgid 0
```

**Note**


---

The driver for the 10G is the ixgbe.

---

**Model Attribute**

The model will also be written to the setupfile. This is the same model that is present in the /home/isa/.arroyorc file and is used by the cserver to determine the number of disks present in the system. This model will be written to the setupfile for both Merced and Merrimack systems. It is not written on Lindenhurst or Serverworks systems.

The format of this new parameter is:

```
model CDE250-XXX
```

## CDSM Disk Monitor

The Disk Monitor page supports the 12 SSD, 24 SSD and 24 HDD versions of the Merced platform with the same graphic representation (see screen shot below). Note that the disk numbering starts at the right at disk 1, and continues to the left up to disk 24. If the user mouses-over the lighted disk status a breakdown of the stats for that particular disk is displayed. Note that these stats will update dynamically (at the selected "data refresh rate") if the user continuously holds their mouse over a disk.

**CDSM NIC Monitor Page**

The NIC Monitor page displays the same graphic for all Merced platforms, since they all have the same port layout and numbering. This page has no unique features for support of Merced. As with previous generations of hardware when the user mouses-over a specific port the stats for that port will be displayed. Note that these stats will update dynamically (at the selected "data refresh rate") if the user continuously holds their mouse over a port.

**Graph Ports Popup**

Clicking the Graph Ports button on the NIC Monitor page will generate a port graph specifically tailored to the Merced 10Gig capabilities. This popup is generated and populated dynamically with a refresh based on the poll time associated with the ports.

**CDSM Server Vitals Monitor Page**

The Monitor > Server Level > Server Vitals page shows the specific monitored health parameters for each Merced server. The data contained in this page is dynamically refreshed at the rate set in the "Data Refresh Rate" box.

## SNMP

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1294

**10G Interface Support**

Merced hardware includes 10G interfaces. SNMP agent now supports 10G interfaces and reports the ifHighSpeed for all interfaces in UNITS of Mbps. The following example shows four interfaces: 10 Mbps, 100 Mbps, 1000 Mbps and 10Gbps:

```
# /usr/local/bin/snmpwalk -v 2c -c public 172.22.102.189 ifX | grep Speed
IF-MIB::ifHighSpeed.1 = Gauge32: 10
IF-MIB::ifHighSpeed.2 = Gauge32: 100
IF-MIB::ifHighSpeed.3 = Gauge32: 1000
IF-MIB::ifHighSpeed.4 = Gauge32: 10000
```

## Software Version

The Maintain > Software > Software Version page support the new Merced part numbers, when the user selects a Merced server for display the current software version and and the servers PID, VID, Serial and Additional String will be displayed.

## External Specifications

This release contains the sdt utility from SuperMicro that allows for system health monitoring.

# Supported Environments

Cisco TV CDS 2.4.2 Software Release supports the following environments and associated backoffice integrations:

- ISA environment:
  - ISA (standard)
  - ISA with STUN handshake
- RTSP environment:
  - NGOD
  - Cisco

## System Requirements

The Cisco TV CDS Release 2.4.2 runs on the CDE250-2S5, CDE250-2S6, CDE250-2G3 and CDE110 (if the CDE110 is used as a CDSM to configure, manage and monitor the stream domain with CDE250-2S5 and CDE250-2S6). See the *Cisco Content Delivery Engine110 Hardware Installation Guide*, and the *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*.

Release 2.4.2 running on CDE250 interoperates with 2.2.x and 2.3.x running on CDE220 and CDE420 within a cluster.

Release 2.4.2 does not support the CDEs with the ServerWorks chipset. All CDEs with the ServerWorks chipset need to be replaced with the CDEs with the Lindenhurst chipset or the Next Generation Appliances (CDE110 and CDE250) before upgrading to Release 2.4.2.

See the [“Related Documentation” section on page 17](#) for links to the documentation online.

[Table 1](#) shows all the platforms and software releases that have been tested with the CDE250-2S6 and the Cisco TV CDS 2.4.2 Software Release.

**Table 1** *Compatible Platforms and Releases*

	<b>CDE250-2S5/ 2S6/2G3 Streamer</b>	<b>CDE250-2G3 Cache Server</b>	<b>CDE420-4A Vault</b>	<b>CDE420-4G Cache Server</b>	<b>CDE220-2C2/ 2S3 Streamer</b>	<b>CDSM</b>	<b>VVIM</b>
NGOD Environment	2.4.1 and 2.4.2	2.4.2	2.3.2-ES6 2.3.3	2.3.2-ES5 2.3.3 2.3.3-es1	2.3.2-ES5 2.3.3 2.3.3-es1	2.4.2 (upgraded from 2.3.x and 2.4.1)	2.4.2 (upgraded from 2.3.x)
ISA SHIM Environment	2.4.2	2.4.2	2.3.2-ES6 2.3.3	2.3.2-ES5 2.3.3 2.3.3-es1	2.3.2-ES6 2.3.3 2.3.3-es1	2.4.2 (upgraded from 2.3.x and 2.4.1)	2.4.2 (upgraded from 2.3.x)

## Limitations and Restrictions

Cisco TV CDS 2.4.2 Software Release has the following limitations and restrictions:

- This release can only be run on a CDE250-2S5, CDE250-2S6 or CDE250-2G3.
- When adding one or more CDE250-2S5/CDE250-2S6 modules to a deployment cluster, the CDE110 for CDSM also needs to run with release 2.4.2.
- The fill bandwidth limit is 2000 SD streams when using Standard Ethernet Frames; it is 5000 SD streams when using Jumbo Ethernet Frames.
- When a CDE250 fails, there must be enough capacity on other streamers to which streams can failover; otherwise, they will be dropped.

# Important Notes

There is a new driver for the new solid-state drives (SSDs) that also addresses an issue with the old SSDs.

## Old SSD Issue

When an abrupt power loss occurs on an older SSD while the SSD is under load, which can also happen when the SSD is being written to and a power-off shutdown occurs, the result is that the SSD may become corrupted and unusable. If an SSD becomes corrupted in this way it must be replaced.

This driver update provides a fix to prevent the corruption of the SSD when the system is being shutdown. When the system is being shutdown the driver sends a command to the SSD to stop all activity and therefore is protected from corruption.



### Note

---

We recommend that this driver update be installed on all systems with SSDs. The driver update is compatible with both the older PV SSDs and the newer PVR SSDs.

---

## New SSDs

New solid-state drives (SSDs) used in the following CDE models require a device driver update for the TV CDS software to recognize the drives:

- CDE220-2S1
- CDE220-2S3
- CDE250-2S5
- CDE250-2S6

A new Generation 2 SSD drive could occur in one of the above newly manufactured CDEs or as a returned merchandise authorization (RMA) SSD drive replacement.

The new SSDs replace the end-of-life (EOL) external 160 GB SSDs. A new SSD drive is a Generation 2 front-mounted SSD. The new SSD model is identified by the title “Intel SSD 320 Series” on the label and has the model number: SSDSA2BW160G3. For more information, see Field Notice 63438 at: [http://www.cisco.com/en/US/products/ps7126/prod\\_field\\_notices\\_list.html](http://www.cisco.com/en/US/products/ps7126/prod_field_notices_list.html).

The new driver prevents the corruption of the existing SSDs in the field when a system is shutdown. In the case of receiving any new model of SSDs, the driver must be installed.



### Note

---

The new driver is 100 percent backward-compatible with older, pre-existing SSD drives. We recommend that a proactive upgrade of the SSD driver is a good best-practice.

---

For more information, see the [“Updating the Device Drivers for new SSDs”](#) section on page 14.

# Open Caveats

This release contains the following open caveats:

## Cache Server

- CSCtk66303

Symptoms:

The cache server has a general protection fault in CM::LocalReadRate::checkAndFillHole+0x66c as can be seen in the back trace.

Conditions:

The crash was caused because an acknowledge packet sent from a streamer to the cache server has a bad length for the amount of data acknowledged. This causes the cache server to unlock the wrong amount of data associated with the fill and this causes the later protection fault.

Workaround:

Older streamers are known to cause this problem. Updating streamers to the latest release may resolve the issue.

## cs-drivers

- CSCtl88307

Symptom:

Server may enter kdb when a drive is pulled without first being logically removed with `/proc/cds/cdd/remove_device`.

Conditions:

Conditions are varied and relative to the state of the drive; active, inactive, failed, etc.

Workaround:

Always logically remove a drive, especially one that is not failed, before pulling it from its slot.

## cs-file-systems

- CSCtl89516

Symptoms:

The symptoms of this problem are that all fill streams are in cut-through mode (not being written to the local file system) and the disk channel is at a relatively low utilization. This results in a less than optimal caching efficiency since a local copy of the data will not be retained on disk.

Conditions:

This has only been seen when running a CDE 250 2G3 system as a streamer, and when running with a maximum fill load of around 5000 standard definition streams. If you are running with a lighter fill load or a different server, you should be able to avoid the problem.

Workaround:



This in no way prevents the system from functioning. The stream data is still available when filled from a remote cache or vault. No other work around is needed.

## Resolved Caveats

The following caveats have been resolved for Cisco TV CDS Release 2.4.2. Not all resolved issues are mentioned here. The following list highlights caveats associated with customer deployment scenarios.

### Cache Server

- CSCth87732  
A locate request to a cache server can fail because the cache server was unsuccessful at querying vaults for information about the requested content. The error message associated with the failure does not indicate the vault was queried by the cache server, which can make troubleshooting the failure more difficult.
- CSCti38148  
Video content transferring from a cache server to streamer using C2 protocol can become corrupted, and exhibit artifacts such as tiling during streaming.
- CSCti79834  
A cache server can crash and reboot itself. The core trace of the crash will show information such as “Unable to handle kernel paging request at ffff80ffffffffffc RIP: [<ffffff883cd811>] :avs\_cserver:iox\_nonstreamcomplete+0x31/0x340”.

### cs-cache-management

- CSCtj15913  
Paid to goid lookup request failed.

### cs-network

- CSCtj86813  
Each system (vault, cache node, or streamer) keeps track of all the other servers that is within its scope of visibility allowing the systems to communicate, transfer content, provide management communications, provide fault tolerance and resiliency and maintain general health of the system. A table is kept in memory called the remote servers table and is used for keeping track of all servers that are visible to each server. There is a corresponding table called the shared page table which has an entry for each remote server where the status of that server (reachable, database online, etc.) is stored for access from the user space programs. The shared page table size was smaller than the remote server table size. The shared page table had a limit of 125 entries, and had code to check that the table would not overflow and cause memory corruption. When the 126th server was brought up it became visible to all the vaults, therefore they all executed the shared page table overflow check logic in the code causing each of them to go to kdb.

- CSCtj87648

When a cache server has two vault groups that it could fill from and one of the vault groups has all the vaults offline so that they will not accept ingests, this triggers a situation where none of those vaults in that group will be selected to fulfill the fill request. Then most if not all fill request made by the cache server will go to the one vault group and the fill capacity is not balanced.

## cs-stream

- CSCti79602

If RTSP is having issues and the master is moved then the backup may crash.

## cs-vault

- CSCtj00762

Vault kdb when more than 20 copies are created.

## Database

- CSCti73302

AVSDB generates a core file when issuing the db\_shutdown command.

## FSI

- CSCti91796

When ingesting content's name contains characters "21", the response of "SIZE" FTP command is incorrectly processed by fsid.

## ISA

- CSCth91946

During the 2.3 integration, we found that with 150 simultaneous FTP push sessions, Master ContentStore will core dump and then is restarted though check\_ISA\_service thread, which resulted in some failed live recordings.

- CSCth98418

ISA ContentStore restarts because of network issues. If the network issues occur then it could cause multi-master. If multi-master occurs then content store or isa service monitor application might not get the reply back for its requests and could wait for-ever and so script times out and restart both monitor application and the content store.

## statsd

- CSCth26572  
Vault's DB cannot establish connections with other servers.
- CSCtk82042  
Allows for new (multiple) power supply fan, temp. and failure monitoring.

## Upgrading to Release 2.4.2

For new installation and upgrade procedures, see the *Cisco TV CDS 2.3 Installation, Upgrade, and Maintenance Guide*.

The CDE250-2S5 and the CDE250-2S6 streamers and the 2G3 streamer and caching node are only supported in the CDS-TV 2.4 release. The CDSM has to be upgraded to a 2.4 image to configure the 2S5 or the 2S6 streamer through the CDSM.

This section contains the following topics:

- [Upgrading the CDSM, page 11](#)
- [Upgrading a CDE250-2S5 or a CDE250-2S6 Streamer, page 13](#)
- [Updating the Device Drivers for new SSDs, page 14](#)

## Upgrading the CDSM

Download the 2.4.2 image from the Cisco ftp download server.

The upgrade usually starts from the slave CDSM, then the master CDSM if CDSM Redundancy is enabled. If CDSM Redundancy is enabled, statsd runs on each CDSM. If CDSM Redundancy is disabled and only one CDSM is in service, statsd does not run on that CDSM.

Perform the following steps to upgrade the CDS-TV Software on the CDSM:

- 
- Step 1** Log in to the slave CDSM server as *root*.
- Step 2** Shut down the avbdb process by entering the following command:

```
# db_shutdown
```

- Make sure “pgrep avbdb” returns no process ID (PID).
- Make sure “netstat -an | grep 9999” returns nothing.

- Step 3** Shut down the statsd process. Make sure “pgrep statsd” returns no process ID (PID).

- Step 4** Backup the CDSM by entering the following command:

```
[root@cdsm19 ~]# /home/upgrade/2_2/preupgrade
```

```
Starting Backup of configuration and database files
Checking that all processes are stopped on the system
Checking that cserver is not running on the system
Starting Backup of files to: /root/cdsm19
Backup of files completed.
Creating Tarball of backed up files
Tarball of backed up files created successfully
```

```
!! IMPORTANT : Make sure that the directory /arroyo/backup is created on the machine to
back up !!
IP Address of machine to backup configuration/database files?: 172.22.102.21
root@172.22.102.21's password:
cdsm19.tgz                                100% 3233KB   3.2MB/s   00:00
Tarball uploaded to 172.22.102.21

Scripts executed successfully !!!
Please reboot the server and run the script 'upgrade' when the server comes back up.
```




---

**Note** The Remote Server 172.22.102.21 will have the cdsm19.tgz file in the /arroyo/backup directory.

---

```
[root@cdsm21 backup]# ls
cdsm19.tgz
[root@cdsm21 backup]# pwd
/arroyo/backup
[root@cdsm21 backup]#
```

**Step 5** Run the cdsinstall script to upgrade to the ISO image from your current running version to release 2.4.2 by entering the following command:

```
[root@cdsm19 ~]# ./cdsinstall CDS-TV-PROD.iso
Select Deployment Type (ctrl-c to quit):
  1) CDSM
1
CDSM Selected
[Omitted]
```

**Step 6** Check the /arroyo/image/tags to verify the 2.4.2 ISO image is installed:

```
[root@mc_cdsm_ccdn 2_2]# cat /arroyo/image/tags
cdstv-2.4.2-b33
```

**Step 7** Reboot the CDSM with /etc/rc.local and follow the statements if you want to automatically start avsdB and the Apache Server:

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
# Lines below this one modified by cdsflavconfig (ISA):

su - isa -c "cd /home/isa"

sleep 30

/arroyo/www/bin/apachectl start

sleep 30

# statsd process should be running with CDSM Redundancy enabled only
/home/stats/statsd -i <virtual-ip> -s <network-mask> -d <eth0>
```




---

**Note** avsdB, statsd (applicable if CDSM Redundancy is enabled), and the Apache Server are running if a CDSM is in a working state.

---

- Step 8** To complete the software upgrade, log in to the CDSM GUI as a user with Engineering access level. The CDSM Setup page is displayed. Verify all settings on the CDSM Setup page and click **Submit**.
- Step 9** Repeat [Step 1](#) to [Step 8](#) to upgrade the master CDSM if CDSM Redundancy is enabled.

## Upgrading a CDE250-2S5 or a CDE250-2S6 Streamer

Download the 2.4.2 image from the Cisco ftp download server. At least 1.8 GB of space must be available on the / partition to perform the upgrade.

To upgrade a CDE250-2S5, CDE250-2S6 or CDE-250-2G3 streamer, do the following:

- Step 1** Log into the streamer as user *root*.
- Step 2** Ensure that there are no active streams on the streamer. Check the Active Streams line in the `protocoltiming` log.
- Step 3** Shut down the `avsd` process by entering the following command:
 

```
# db_shutdown
```

  - a. Make sure “`pgrep avsd`” returns no process ID (PID).
  - b. Make sure “`netstat -an | grep 9999`” returns nothing.
- Step 4** Copy the `2.4.2.iso` image to the `/root` directory on the streamer.
- Step 5** Verify that the streamer has the necessary space in the `/` directory and in the `/arroyo` directory.
 

```
# df -k
Filesystem      1K-blocks      Used Available Use% Mounted on
/dev/hde2        7329436      4826612    2124496   70% /
/dev/sda7        18557000     8112384    9486744   47% /arroyo
/dev/sda6         4061540         603732    3248164   16% /var
/dev/sda2         8123200         635304    7068600    9% /home
/dev/sda1        19840892     1114908    17701844    6% /arroyo/db
/dev/hde1         248895          19474     216571    9% /boot
/dev/sda3         4948548     141364     4551752    4% /boot_cds
tmpfs            24692112           0    24692112    0% /dev/shm
```
- Step 6** Verify the MD5 checksum value.
 

```
# md5sum cdstv-2.4.2-upgrade-kit.sh
```

Compare the output with the `md5reportfile.txt` file on the CDS software CD-ROM.
- Step 7** Run `/root/cdsinstall/2.4.2.iso` and choose either ISA or RTSP, depending on your environment.
 

The `cdsinstall` script backs up the current running system, expands new files onto the system, removes old RPMs, and installs new RPMs.
- Step 8** Reboot the streamer to restart all services.
- Step 9** Verify that the 2.4.2 image has been correctly installed. From the CDSM GUI, click **Maintain > Software > Software Version** and verify that the software version is set to 2.4.2.

Once the Streamers have been upgraded, verify using the CDSM GUI that the servers are online (that is, Offload is set to Disabled) and verify that only one primary setup exists in one stream group.

## Updating the Device Drivers for new SSDs

The SSD driver update is for new SSDs and to address an issue with older SSDs. For more information, see the “[Important Notes](#)” section on page 7.

If a CDE requires an SSD replacement, the device driver must be updated. The device driver must be updated before replacing the SSD. If a new CDE is being added to the CDS, after upgrading the TV CDS software, the device driver must be updated. New SSDs are not recognized with the proper attributes until the device driver is updated.



**Note** The new driver is 100 percent backward-compatible with older, pre-existing SSD drives. We recommend that a proactive upgrade of the SSD driver is a good best-practice.

To view a list of TV CDS software releases this device driver applies to see the defect, CSCtr29064, in the Bug Tool Kit (<http://tools.cisco.com/Support/BugToolKit/>).



**Note** When using the **cdsinstall** script to install the software image file, install the driver package after the **cdsinstall** script is complete.

To install the device driver update package, do the following:

**Step 1** Download the `cdstv_x.y.z_CSCtr29064.bin` driver update package to the `/root` directory of the CDE. The filename is `cdstv_x.y.z_CSCtr29064.bin`, where `x.y.z` denotes the software release.



**Note** The driver update package includes support for all applicable software releases, so any `cdstv_x.y.z_CSCtr29064.bin` file installs correctly and can be used to update the drivers for any applicable release.

Following is the md5 checksum for the `cdstv_x.y.z_CSCtr29064.bin` driver update package:

```
89684e2094d841b236ba1d83e958df9b cdstv_x.y.z_CSCtr29064.bin
```

The driver update package is a self-extracting, self-installing package.

**Step 2** Change the permissions on the CDE. As user `root`, enter the following command:

```
# chmod 755 /root/cdstv_x.y.z_CSCtr29064.bin
```

**Step 3** Install the device driver update. As user `root` user enter the following commands:

```
# cd /root
# ./cdstv_x.y.z_CSCtr29064.bin
```

The package installs the device driver.

**Step 4** To verify that the package has been installed on the CDE, view the `/etc/cisco-version-history` file, and verify that the string “`cdstv_CSCtr29064`” has been added to this version-history file.

**Step 5** To verify that the driver has been updated and will be used by the CDS server, enter the following commands:

```
cd /lib/module/`uname -r`
/sbin/modinfo -F version csd.ko cdd_sys.ko
```

The updated driver files report the same version for both driver files in the format of x.y.z.1, where x.y.z is the version of the TV CDS software (for example, 2.3.3.1).

**Step 6** Reboot the CDS server.

```
# reboot
```



**Note** Rebooting a Vault server does not interrupt stream services, but causes current ingests to fail. If your CDS does not have stream failover, rebooting a Streamer without offloading it interrupts all stream services. If possible, you should perform functions that require a system restart during times when the least number of users are actively connected to your system.

A new SSD drive is a Generation 2 front-mounted SSD. The new SSD model is identified by the title “Intel SSD 320 Series” on the label and has the model number: SSDSA2BW160G3. For more information, see Field Notice 63438 at:

[http://www.cisco.com/en/US/products/ps7126/prod\\_field\\_notices\\_list.html](http://www.cisco.com/en/US/products/ps7126/prod_field_notices_list.html).

The following command provides information on the external SSDs that are the new drive model:

```
# find /sys/devices -name "model" | xargs grep SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:7/end_device-3:7/target3:0:7/3:0:7:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:6/end_device-3:6/target3:0:6/3:0:6:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:5/end_device-3:5/target3:0:5/3:0:5:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:4/end_device-3:4/target3:0:4/3:0:4:0/model:INTEL SSDSA2BW16
/sys/devices/pci0000:80/0000:80:05.0/0000:87:00.0/host3/port-3:3/end_device-3:3/target3:0:3/3:0:3:0/model:INTEL SSDSA2BW16
```

To view all SSD models currently supported by the Cisco TV CDS software, enter the following command:

```
# find /sys/devices -name "model" | xargs grep SSDSA
```

The older SSD model is INTEL SSDSA2M160.

## Rolling Back the SSD Driver Update

If for any reason you need to revert to the older SSD driver, with the TV CDS software running on the CDS server, do the following:

**Step 1** Change to the drivers directory.

```
cd /lib/module/`uname -r`
```

**Step 2** To save the updated driver (optional), enter the following command:

```
cp csd.ko csd.ko.update
cp cdd_sys.ko cdd_sys.ko.update
```

**Step 3** Rename the backed up driver files to the driver filenames. The “previous\_version” is the version number of the driver update.

```
cp csd.ko_bkup_<previous_version> csd.ko
cp cdd_sys.ko_bkup_<previous_version> cdd_sys.ko
```

**Step 4** Verify the driver versions by using the following command:

```
/sbin/modinfo -F version csd.ko cdd_sys.ko
```

The drivers before the driver update have a version in the format of a.b.c and the two drivers do not necessarily have the same version number.

**Step 5** Reboot the CDS server.

---

## Rollback from Release 2.4.2

### Rollback a CDSM

To rollback a CDSM from Release 2.4.2 to an earlier release, do the following:

---

- Step 1** Log into the CDSM as user *root*.
- Step 2** Shut down the avsdB process by entering the following command:
- ```
# db_shutdown
```
- Make sure “pgrep avsdB” returns no process ID (PID).
  - Make sure “netstat -an | grep 9999” returns nothing.
- Step 3** Run `/root/cdsinstall/<previous iso image>` to rollback to the previous software image.
- Step 4** Reboot the CDSM to restart all services.
- Step 5** Verify that the database (avsdB) has restarted.
- Step 6** Verify that the apache server is running correctly.

### Rollback a CDE250-2S5, CDE250-2S6 or a CDE250-2G3 Streamer

To rollback a streamer from Release 2.4.2 to an earlier release, do the following:

---

- Step 1** Log into the Streamer as user *root*.
- Step 2** Shut down the avsdB process by entering the following command:
- ```
# db_shutdown
```
- Make sure “pgrep avsdB” returns no process ID (PID).
  - Make sure “netstat -an | grep 9999” returns nothing.
- Step 3** Run `/root/cdsinstall/<previous iso image>` to rollback to the previous software image.
- Step 4** Reboot the streamer to restart all services.
-



## Related Documentation

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

- *Cisco TV CDS 2.3 ISA Software Configuration Guide*  
[http://www.cisco.com/en/US/docs/video/cds/cda/tv/2\\_3/configuration/isa\\_guide/tv\\_cds\\_2\\_3\\_isa\\_config.html](http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_3/configuration/isa_guide/tv_cds_2_3_isa_config.html)
- *Cisco TV CDS 2.3 RTSP Software Configuration Guide*
- [http://www.cisco.com/en/US/docs/video/cds/cda/tv/2\\_3/configuration/rtsp\\_guide/tv\\_cds\\_2\\_3\\_rtsp\\_config.html](http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_3/configuration/rtsp_guide/tv_cds_2_3_rtsp_config.html)
- *Cisco TV CDS 2.1–2.3 API Guide*  
[http://www.cisco.com/en/US/docs/video/cds/cda/tv/2\\_2/developer\\_guide/tv\\_cds\\_2\\_2\\_apiguide.html](http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_2/developer_guide/tv_cds_2_2_apiguide.html)
- *Cisco TV CDS 2.3 Installation, Upgrade, and Maintenance Guide*  
[http://www.cisco.com/en/US/docs/video/cds/cda/tv/2\\_3/installation\\_guide/tv\\_cds\\_2\\_3\\_maint\\_guide.html](http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_3/installation_guide/tv_cds_2_3_maint_guide.html)
- *Cisco Content Delivery System 2.x Documentation Roadmap*  
[http://www.cisco.com/en/US/docs/video/cds/overview/CDS\\_Roadmap.html](http://www.cisco.com/en/US/docs/video/cds/overview/CDS_Roadmap.html)
- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*



### Note

---

This document will be provided by your Customer Support representative.

---

[http://www.cisco.com/en/US/docs/video/cds/cde/cde205\\_220\\_420/installation/guide/cde205\\_220\\_420\\_hig.html](http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html)

- *Cisco Content Delivery Engine 110 Hardware Installation Guide*  
[http://www.cisco.com/en/US/docs/video/cds/cde/cde110/installation/guide/cde110\\_install.html](http://www.cisco.com/en/US/docs/video/cds/cde/cde110/installation/guide/cde110_install.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](http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/CDE_RCSI.html)
- *Adding CDE250-2S5/2S6 Streamer Procedure (EDCS-884951)*



### Note

---

This document will be provided by your Customer Support representative.

---

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](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](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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.