Release Notes for Cisco TV CDS 2.2.1

These release notes cover Cisco TV CDS Release 2.2.1.
Revised: October 2011 OL-21788-02

Contents

The following information is in the release notes:

- New Features, page 2
- Enhancements, page 4
- Supported Environments, page 5
- System Requirements, page 6
- Limitations and Restrictions, page 6
- Important Notes, page 7
- Open Caveats, page 8
- Resolved Caveats, page 10
- Upgrading to Release 2.2.1, page 13
- Related Documentation, page 16
- Obtaining Documentation and Submitting a Service Request, page 17
New Features

Release 2.2.1 of the Cisco TV CDS introduces the following new features:

- Multi-Screen Video Support
- SNMP Traps
- Dual Conditional Access System Support
- Bulk Configuration

Multi-Screen Video Support

Release 2.2.1 offers Multi-Screen Video (MSV) support for ISA environments with VVI and Shared Content Store. An MSV Asset Deletion script runs periodically, nightly by default. The script identifies the VOD assets that were removed by the backoffice and deletes them from the Vaults. If the asset is found in any one of the video hub offices (VHOs), the asset is not deleted. Only when the asset is not found in all VHOs is the asset deleted from the Vaults. The MSV Asset Deletion script runs by way of a cronjob.

The cronjob needs to be manually entered after upgrading the software on the Vault. To add the cronjob, do the following:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to each Vault as root.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Edit the crontab.</td>
</tr>
<tr>
<td></td>
<td><code>crontab -e</code></td>
</tr>
<tr>
<td></td>
<td><code>30 05 * * * su - isa -c &quot;cd Asset;./clean_orphaned_contents &gt;&amp; run.log&amp;&quot;</code></td>
</tr>
<tr>
<td>Step 3</td>
<td>Make sure the job is printed out.</td>
</tr>
<tr>
<td></td>
<td><code>crontab -l</code></td>
</tr>
</tbody>
</table>

SNMP Traps

In previous TV CDS releases, there were minimal SNMP traps. In Release 2.2.1, the following SNMP traps have been added:
New Features

- cdstvServiceUp
- cdstvServiceDown
- cdstvDiskUsageHigh
- cdstvDiskUsageNormal
- cdstvLinuxFSUsageHigh
- cdstvLinuxFSUsageNormal
- cdstvPortLossHigh
- cdstvPortLossNormal
- cdstvSysHealthUp
- cdstvSysHealthDown

Dual Conditional Access System Support

Release 2.2.1 supports dual Conditional Access Systems (CASs) for ISA environments: Cisco/Scientific Atlanta Power Key Encryption System (PKES) and Motorola’s OffLine Encryption Station (OLES). A new field has been added to the Monitor Completed Ingests page that indicates whether the ingested content is encrypted or not. Both clear and encrypted content can be ingested.

Bulk Configuration

Bulk Configuration provides a method of configuring common parameters for all the servers at one time by using an XML file. Following are the CDSM GUI configuration pages that offer bulk configuration:

- QAM Gateway
- Headend Setup
- Stream Destination
- NTP Server
- Server DNS
- SNMP Agent
- Route Tables
- RTSP Setup
- FSI Setup
## Enhancements

Table 1 describes the enhancements to TV CDS 2.2.1.

### Table 1  New Features in TV CDS 2.2.1

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Play History report and Stream Monitor page Graph Stream option are now optional</td>
<td>Trick mode reporting and monitoring can now be disabled through the CDSM Setup page, thereby freeing up disk storage.</td>
</tr>
<tr>
<td>CDSM now supports 100,000 streams</td>
<td>CDSM supports the configuration, monitoring, and reporting of up to 100,000 provisioned streams.</td>
</tr>
<tr>
<td>CDSM now supports 120,000 ingests</td>
<td>CDSM supports the configuration, monitoring, and reporting of up to 120,000 provisioned ingests.</td>
</tr>
</tbody>
</table>
| NGOD C2 interface compliance | Compliance with the CD interface for NGOD deployments, which consist of the following:  
  - Rate of cache-fill between Caching Nodes and Streamers different than stream rate  
  - Persistent HTTP connections  
  - Encoding of transfer delay in Transfer ID and allow client to override with Transfer Delay header in transfer request. |
| Support for DVD on Demand content files up to 30 GB in size | Ability to differentiate between a DVD asset and a video asset and support ingest, trick-play creation, and streaming of content files up to 30 GB in size that could span multiple days. |
| Ability to add a server without shutdown existing servers | Adding a server into an existing system does not require shutting down existing servers in order to copy the database. |
| FSI Ingest resiliency | Previous TV CDS releases supported FSI ingest redundancy by creating two recording copies on separate Vaults. This allowed switching to the backup recording if there was an error on the primary recording. Adding to this functionality, the FSI monitors Vaults and detects problematic Vaults; if found, FSI switches to the backup. |
Release Notes for Cisco TV CDS 2.2.1

**Supported Environments**

Release 2.2.1 of the Cisco TV CDS supports the following environments and associated backoffice integrations:

- ISA environment
  - Tandberg OpenStream backoffice
  - OneWave backoffice
- RTSP environment
  - SeaChange Axiom backoffice (NGOD architecture)
  - EventIS

**Table 1  New Features in TV CDS 2.2.1 (continued)**

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDSM GUI enhancements</td>
<td>The CDSM GUI has the following enhancements:</td>
</tr>
<tr>
<td></td>
<td>- NTP configuration (System Level, Array Level, and Server Level)</td>
</tr>
<tr>
<td></td>
<td>- ISV Groups (known as SSV Groups in the GUI) that support ISV redundancy</td>
</tr>
<tr>
<td></td>
<td>- Scheduled automatic EPG import for Media Scheduler</td>
</tr>
<tr>
<td></td>
<td>- Server Vitals page that monitors server environment</td>
</tr>
<tr>
<td></td>
<td>- System Health Monitor page displays servers and groups, as well as Vitals column</td>
</tr>
<tr>
<td></td>
<td>- Disk and NIC Monitor pages dynamically updated</td>
</tr>
<tr>
<td></td>
<td>- Cache to Vault Map page allowing mapping between Caching Nodes and Vaults</td>
</tr>
<tr>
<td></td>
<td>- Thin Pipe Map page allows mapping for cache-fill and content mirroring</td>
</tr>
<tr>
<td></td>
<td>- Stream to Cache Map page allows mapping Streamers to Vaults</td>
</tr>
<tr>
<td></td>
<td>- Server ID added to Trick Play History report</td>
</tr>
<tr>
<td></td>
<td>- Assured Forwarding (AF) class assignment for cache priority per server</td>
</tr>
<tr>
<td></td>
<td>- Disable null MPEG files per Streamer</td>
</tr>
<tr>
<td>New API for Trick Play History</td>
<td>PlayServerHistory API added.</td>
</tr>
<tr>
<td>Supports different bit rates for streaming.</td>
<td>The VVI in Release 2.2.1 supports different bit rates for streaming than the bit rate of the asset. (CSCta54351)</td>
</tr>
<tr>
<td>Support timeout for HTTP connections</td>
<td>For VVI in an RTSP environment with HTTP Streamers. The HTTP connections times out after 60 seconds and the connection is closed, unless the client sends requests or heartbeat messages within the timeout interval. (CSCte72306)</td>
</tr>
<tr>
<td>Caching Node supports live streaming</td>
<td>The Caching Node in a VVI supports live streaming in Release 2.2.1. (CSCte26684)</td>
</tr>
</tbody>
</table>
System Requirements

The Cisco TV CDS Release 2.2.1 runs on the CDE110, CDE220, and CDE420. See the Cisco Content Delivery Engine110 Hardware Installation Guide, and the Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide.

The Cisco TV CDS Release 2.2.1 also runs on the CDE100, CDE200, CDE300, and CDE400 hardware models that use the Lindenhurst chipset. See the Cisco Content Delivery Engine CDE100/200/300/400 Hardware Installation Guide for set up and installation procedures.

Release 2.2.1 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, CDE220, and CDE420) before upgrading to Release 2.2.1.

See the “Related Documentation” section on page 16 for links to the documentation online.

Limitations and Restrictions

There are no limitations nor restrictions in Release 2.2.1.
**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.

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:

CDSM

• CSCsu65569
  Symptom:
  Some CDSM GUI commands are not processed properly. In this case the Reload Service Group command needs to reach the name server through DNS search.
  Conditions:
  If the resolv.conf file is not set up manually on the CDSM CDE100 hardware, the Reload Service Group command does not complete and streaming to service groups could be affected.
  Workaround:
  Make sure DNS search is setup in resolv.conf and resubmit the Reload Service Group command through the CDSM GUI.

Installation

• CSCtg10051
  Symptom:
  Reimaging a server to RHEL5 causes the first sector on the drive to be overwritten.
  Conditions:
  This issue happens when reinstalling the OS on a Streamer, Vault, or Caching Node.
  Workaround:
  Remove the front-mounted drives from the server before reimaging.

CServer

• CSCtf11533
  Symptom:
  Vault crashes when over 300,000 content objects are ingested.
  Condition:
  When ingesting more than 300,000 titles, the Vault crashes.
  Workaround:
  Do not ingest more than 300,000 titles.
• CSCtb79062
  Symptom:
  Server crashed because it could not list the details of an object.
Open Caveats

Condition: Because a drive was going in and out of repair mode, it caused the evaluators to abort and create multiple copies of some data.

Workaround:
Do not use the serverinfo log commands to dump detailed file map of a GOID.

- CSCtd42965
  Symptom: RTSP server hangs because it has not received a response.
  Condition: Unable to reproduce.
  Workaround: Restart RTSP server.

- CSCte33408
  Symptom: TCP sessions have unexpected termination or behavior during failure recovery.
  Condition: During stream or cache-fill failure recovery, a Streamer tries to start a large number of cache-fill requests in a small window. When using HTTP as the cache protocol, the Streamer only has a fixed set of buffers used to generate packets for HTTP requests to start the recovery. If requests are built too quickly, a buffer can be re-used before the previous packet built in the buffer was sent and can cause packet corruption. This confuses the Caching Node TCP stack, typically because the sequence numbers are out of order and cause an unexpected behavior.
  Workaround: No workaround exists.

- CSCtf29918
  Symptom: When mirroring between two Vaults, there are damaged content objects.
  Condition: The following conditions could cause this:
  - When there are mixed capabilities of two Vaults; that is, a CDE420 with 8 GigE ports, a CDE400 with 6 GigE ports, or a CDE400 with 4 GigE ports. This can cause an overflow of data from the higher capacity Vault to the lower capacity Vault.
  - If thin pipe mapping is configured, and a larger pipe is set on the sending Vault than on the receiving Vault, an overflow of the pipe can occur. This typically only happens when a very thin pipe is configured, specifically a pipe that is less than 50 Mbps.
  Workaround: Keep the capability of the Vaults the same and do not configure very thin pipes.
Resolved Caveats

The following caveats have been resolved since Cisco TV CDS Release 2.2.1. Not all resolved issues are mentioned here. The following list highlights associated with customer deployment scenarios.

CDSM

- CSCtf94376
  Symptom:
  Service group values greater than 32-bit signed integer (2147483647) are changed to 2147483647 prior to adding the entry to the database.
  Condition:
  CDS environments with gigabit Ethernet streaming that have end-users on both IP Subnets and QAMs typically set their CDSM for a cable environment (QAMs), and enter both QAMs and Subnet IPs on the QAM Gateway page in the CDSM GUI. They then convert each subnet IP address to an integer and enter this on the Headend Setup page as a service group. Unfortunately the processing for service groups uses a function that restricts the entry to a 32-bit signed integer and as such, converts any value greater than 2147483647 to 2147483647.

CServer

- CSCtd29132
  Symptom:
  A side effect of this defect is that it can lead to a server crash.
  Condition:
  There is a window where if an unnecessary ARP request is made from the Control server during a cost request to determine which server is best able to play the stream, a delayed ARP response could resume the cost request and reference a stream that has been destroyed prior to the response.

- CSCtf54171
  Symptom:
  A Caching Node prematurely ends a C2 transfer with a zero length HTTP chunk header. A premature termination should not include a zero length chunk header.
  Condition:
  This condition is triggered if a Caching Node fails to fill a missing part of a content either from disk or network in the middle of a transfer.

- CSCsw79171
  Symptom:
  When a Vault is offloaded, the protocol timing log does not specifically state that the server has been offloaded.
  Conditions:
The offload functionality on Vaults does not specifically notify the Caching Node that it should be placed offline as it is managed by the backoffice integration application. As a result the informational message is not displayed in the Cserver logs.

- **CSCtc20242**
  
  Symptom:
  When ingesting content with FSI ingest, there were some ingestions that failed.
  
  Conditions:
  When ingesting too many pieces of content at the same time and simultaneously capturing recordings, Linux will run out of memory and some of the ingestions will fail.

**Database**

- **CSCtf31677**
  
  Symptom:
  Database stops after time without user interaction.
  
  Condition:
  Servers are configured in the .arroyorc as active replication hosts that are not reachable which causes a slow memory leak.

- **CSCtd11276**
  
  Symptom:
  The STREAM_TRICK_REPORT.db continues to grow in file size.
  
  Conditions:
  Occurred in Release 2.0.0 fc2 on CDSM.

**MSA**

- **CSCte78915**
  
  Symptom:
  CDSM file system can become full and all logging will stop.
  
  Condition:
  For any customer site running MSA Logging.

**Video Quality**

- **CSCtf87497**
  
  Symptom:
  Tiling when jumping through an uncached asset. Macroblocking or tiling when transitioning from rewind, fast-forward or pause to 1x play.
  
  Condition:
VVI environment with Seachange Streamer. Asset must be slightly unusual in that most assets use the default 0xE0 value for the stream ID, and this asset must use something else.

**Network**

- CSCtb17542
  Symptom:
  Cache-Fill NICs on Vaults show as malfunctioning adapters in the protocoltiming logfile.
  Conditions:
  A combination of reduced cache-fill NICs (three or less), high fill-load (in the 1000s), and active local evaluators (local smoothing, defrag).

**RTSP**

- CSCtc41337
  Symptom:
  In specific customer integration testing, a specific backoffice sends a SETUP request for a session. RTSP server is unable to send the SETUP response back to the backoffice.
  Conditions:
  Specific Customer integration testing. SETUP requests coming on the backoffice port 554.

**Vaults**

- CSCtc83454
  Symptom:
  Rewind trick modes may appear to have regular “jitter” where a frame every so often appears out of place. On some STBs this could manifest as scrambled video frames interleaved with working ones. Other manifestations are possible. The interval should be somewhat predictable. The rate of the “jitter” should be somewhat predictable. In one case with a key change every 8 seconds in the content and a 4X trick file, a frame jitter was seen about every 2 seconds. The jitter occurs during the playback of the trick (for example, while rewinding), not at the start or end of the trick mode itself.
  Conditions:
  The content must be encrypted with PowerKey. It must be using keys that change on a regular basis.

**SNMP**

- CSCtf00863
  Symptom:
  SNMP Query to a Vault running 2.6.18-53.el5.cdstv.2.1.1.es1.b6 on:
  `cdstvCacheStatsFillRecieveStreamCount - 1.3.6.1.4.1.15946.1.2.1.1.1.2`
  `cdstvCacheStatsFillStreamActualBWinKBits - 1.3.6.1.4.1.15946.1.2.1.1.1.3`
cdstvCacheStatsFillStreamCommittedBWinKBits - "1.3.6.1.4.1.15946.1.2.1.1.1.4.1.1.1.1.1.4" returns:
SNMPv2-SMI::enterprises.15946.1.2.1.1.1.1.2.1 = Gauge32: 0
SNMPv2-SMI::enterprises.15946.1.2.1.1.1.1.3.1 = Gauge32: 3350
SNMPv2-SMI::enterprises.15946.1.2.1.1.1.1.4.1 = Gauge32: 0
SNMPv2-SMI::enterprises.15946.1.2.1.1.1.1.5.1 = Gauge32: 0
SNMPv2-SMI::enterprises.15946.1.2.1.1.1.1.6.1 = Gauge32: 0

All values should be zero as this is a Vault not a Streamer

Condition:
This number includes the total data received for any type of packet; for example, mirror traffic, committed rate-fill traffic, monitoring and control traffic, ARP, and so on. Hence, it is normal to have non-zero value on a Vault.

On a Vault, the values represent mirroring and other traffic. On Streamers, this represents streaming traffic.

**Upgrading to Release 2.2.1**

For new installation, upgrade, and downgrade procedures, see the *Cisco TV CDS 2.2 Installation, Upgrade, and Maintenance Guide*.

---

**Note**
Release 2.2 supports upgrades from Release 2.0.x and Release 2.1.x. If your CDS is running an older version, you need to upgrade to Release 2.0.x or 2.1.x, before upgrading to Release 2.2.

---

**Note**
The following TV CDS software releases can coexist during an upgrade process, which allows for long upgrade windows, if necessary:

- For VVI in an ISA environment with SCS, the Release 2.1.3 software can coexist with the Release 2.2.1 software.
- For VVI in an RTSP environment with HTTP Streamers, the Release 2.1.3 ES3 software can coexist with the Release 2.2.1 software.
- For CDS (non-VVI) in both an ISA and RTSP environment, the Release 2.0.x and 2.1.x software can coexist with the Release 2.2.1 software.

The above TV CDS software releases can only coexist during an upgrade process, and only if the upgrade sequences described in the *Cisco TV CDS 2.2 Installation, Upgrade, and Maintenance Guide* are followed.

Different TV CDS software releases are not supported in the long term on an ongoing basis.
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.

Step 2

Change the permissions on the CDE. As user root, enter the following command:

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

Step 3

Install the device driver update. As user root user enter the following commands:

```bash
# 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:

```bash
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.

```bash
# 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:


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

```bash
# find /sys/devices -name "model" | xargs grep SSDSA2BW16
```

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

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

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.

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

**Step 2**

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

```bash
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.

```bash
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:

```bash
/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.

---

**Related Documentation**

Refer to the following documents for additional information about the Cisco TV CDS 2.2:

- *Cisco TV CDS 2.2 ISA Software Configuration Guide*

- *Cisco TV CDS 2.2 RTSP Software Configuration Guide*

- *Cisco TV CDS 2.1–2.2 API Guide*

- *Cisco TV CDS 2.2 Installation, Upgrade, and Maintenance Guide*

- *Cisco Content Delivery System 2.x Documentation Roadmap*

- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*

- *Cisco Content Delivery Engine 110 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.