



Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.4

January 23, 2005



Note

The most current Cisco documentation for released products is available on Cisco.com at <http://www.cisco.com>. The online documents may contain updates and modifications made after the hardcopy documents were printed.

Documentation Survey

Is Cisco documentation helpful? Click [here](#) to give us your feedback.

Contents

These release notes contain information about Cisco ACNS Software Program Manager for IP/TV, Release 5.4. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Limitations and Restrictions, page 4](#)
- [Caveats, page 4](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation, page 8](#)
- [Documentation Feedback, page 9](#)
- [Cisco Product Security Overview, page 9](#)
- [Obtaining Technical Assistance, page 10](#)
- [Obtaining Additional Publications and Information, page 12](#)



Corporate Headquarters:

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco ACNS Software Program Manager for IP/TV (commonly known as IP/TV Program Manager) is a Linux-based application that comes preinstalled on the Cisco Content Engine models CE-565, CE-566, CE-611, CE-7305, CE-7306, and CE-7326. You can access IP/TV Program Manager from a web browser to set up and manage IP/TV scheduled or on-demand programs, channels, recordings, and file transfers among IP/TV Servers.

You can access IP/TV Program Manager from Netscape Versions 4.5x through 4.7x, or Microsoft Internet Explorer Version 5.5 or later. The browser must have Java and JavaScript enabled.

IP/TV Program Manager helps you manage IP/TV Broadcast Server and clients such as IP/TV Viewer. It also allows you to set up interoperability with a Cisco Application and Content Networking System (ACNS) network when IP/TV is installed as part of an ACNS network.

This document contains the new features, limitations, caveats, and other important information regarding Cisco ACNS Software Program Manager for IP/TV, Release 5.4.

**Note**

Read this document in conjunction with the Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.4 and other documents listed in the Related Documentation section of this document.

New and Changed Information

This section describes the new and changed information in IP/TV Program Manager, Release 5.4.

Root Content Engine Failover and Fallback Support for a Cisco Streaming Engine Live Program

Cisco IP/TV Program Manager Release 5.4 supports failover and fallback mechanisms for the root Content Engine to ensure seamless streaming of a Cisco Streaming Engine live program in an IP/TV-integrated ACNS network. If a primary root Content Engine fails, the failover mechanism supports the election of a backup root Content Engine. Fallback occurs when the primary root Content Engine regains its primary position.

Root Content Engine failover requires that both the primary and backup Content Engines be located in the same root location and receive multicast streams from the Cisco IP/TV Broadcast Server. When the primary root Content Engine fails, the backup root Content Engine assumes control of the live program streaming, and the live program continues without interruption. The Content Engine elected as the location leader in the child location continues to receive the live stream from the backup root Content Engine. This process is transparent to user.

**Note**

The failover mechanism is not supported on unicast streams from the Cisco IP/TV Broadcast Server. If the primary root Content Engine fails while a program is playing, you must request for the program again.

Root Content Engines can fail for any of the following reasons:

- The Content Engine is switched off.
- The Content Engine is rebooted.
- The Cisco Streaming Engine is accidentally disabled in the Content Engine.
- A process running on the Content Engine fails.
- The Content Engine is disconnected from the rest of the network.

**Note**

For failover to work correctly, make sure that the Cisco IP/TV Broadcast Server, the root Content Engine, and at least one additional backup Content Engine in the root location are in the same multicast cloud.

Fallback occurs when the primary root Content Engine regains its primary position. Normally, when the primary root Content Engine resumes functioning after a failure, it receives the live stream from the active secondary root Content Engine and does not try to regain its primary position. The fallback mechanism occurs under the following circumstances:

- No other Content Engine in the location has been elected as a location leader.
- A program running on the Content Engine is restarted.
- The current program schedule ends and a new program schedule begins.

Configuring Root Content Engine Failover

To configure root Content Engine failover using the IP/TV Program Manager GUI, choose the Multicast mode of stream delivery to the root Content Engine while scheduling a new program using the New Scheduled Program window. Alternatively, you can choose Multicast mode of stream delivery when you edit an existing program from the Edit Scheduled Program window.

To disable failover to the root Content Engine, choose the unicast mode of stream delivery to the root Content Engine when you edit an existing program from the Edit Scheduled Program window.

For more information about setting up root Content Engine failover support for scheduled programs using the IP/TV Program Manager, see *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.4*

**Note**

If you create or edit a live streaming program by using the Content Distribution Manager and choose Multicast as the stream delivery mode, enter the Root Content Engine Port as 0 (zero). However, if you create the program by using the IP/TV Program Manager and choose Multicast as the stream delivery mode, the IP/TV Program Manager automatically assigns zero to the port setting.

Limitations and Restrictions

This section contains limitations and restrictions for Cisco IP/TV Program Manager, Release 5.4.

Interoperability with IP/TV Broadcast Server

Cisco IP/TV Program Manager, Release 5.4 requires Cisco IP/TV Broadcast Server, Release 5.2 or later for the proper functioning of its features. You may not be able to make use of features such as the scheduled rebroadcast of IP/TV programs over an ACNS network if you are using an IP/TV Broadcast Server release lower than Release 5.2.

Caveats

Caveats describe unexpected behavior in ACNS Software Program Manager for IP/TV, Release 5.4. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderately severe caveats. Only select severity 3 and severity 4 caveats are included in this note.

Open Caveats in IP/TV Program Manager, Release 5.4

This section lists the open caveats in Cisco IP/TV Program Manager Release 5.4.

IP/TV Plug-Ins

- CSCeb09278

Symptom: The IP/TV plug-in does not function when you use Silent Install mode to install the software.

Condition: This problem occurs when you do not copy the required files to the Plugins folder of the browser. When running in Silent Install mode, the installation package fails to find the path where the browser is installed.

Workaround: Copy the following files from the location: [Program Files Folder] \default\plugins folder of the installation package to the Plugins folder of the browser (For example: C:\Program Files\Internet Explorer):

- npfw32.dll
- CMEvtInterface.class
- CiscoMediaPlayer.class
- CMEvtObserver.class

- CSCin43119
Symptom: The IP/TV plug-in does not play SlideCast streams from an on-demand program containing SlideCast streams, and audio and video streams. The IP/TV plug-in plays only audio and video streams, whereas the QuickTime plug-in plays both SlideCast and video on top of each other in a single window.
Condition: This problem occurs when you use plug-ins to play on-demand programs that contain SlideCast streams, and audio and video streams.
Workaround: There is no known workaround.
- CSCin43846
Symptom: Slidecast stream loses audio when you play a scheduled program containing a live SlideCast stream as well as audio and video (live or file-based) streams using the IP/TV plug-in.
Condition: This problem occurs when the audio and video streams are rendered before the SlideCast stream.
Workaround: Restore the audio by activating the video window. Use the audio control buttons to activate the window.

IP/TV Program Manager

- CSCec62492
Symptom: IP/TV Program Manager OnDemand Program Listings window does not list a configured on-demand program, if the associated media file is not available.
Condition: This problem occurs only when you remove the media file associated with the on-demand program from the original location.
Workaround: Do not remove or change the media file location in IP/TV Broadcast Server after configuring on-demand programs that use the media file. If you must remove or change the media file location, then you must edit all programs that use that file to update the file name and location. If you have accidentally removed a media file, restore the file to the original location.
- CSCec52492
Symptom: Requests for on-demand programs from clients in an ACNS network are sent to IP/TV Program Manager. IP/TV Program Manager treats these requests as standalone IP/TV on-demand program requests and directs them to the IP/TV Broadcast Server that can service the request. This situation causes bandwidth constraints and affects the functioning of IP/TV Server.
Condition: This problem occurs when IPTV is integrated with ACNS network and requests for on-demand programs which are exported to the ACNS network, reach IP/TV Program Manager instead of being routed to the Content Engine that has the programs. This problem is related to a routing failure or a routing error.
Workaround: Configure routing correctly in ACNS networks so that on-demand requests are directed to the nearest Content Engine that is capable of servicing the program. Alternatively, you can change the proximity settings in IP/TV Program Manager so that it does not redirect the on-demand program requests to IP/TV Broadcast Server. However, if you choose the second approach, IPTV Broadcast Server may fail to service requests for standalone on-demand programs which have not been exported to ACNS network.

- CSCeg80650

Symptom: The table of contents and the index of IP/TV Program Manager online help are not functioning. When you open the online help window, the left pane, which contains the table of contents and index, appears blank.

Condition: This problem is caused by the Windows Security Update MS05-001. This security patch prevents the system from creating an instance of the HTML Help ActiveX control that is served in HTML content from outside the Local Machine zone.

Workaround: Since IP/TV Program Manager is part of your internal network, you may modify the Windows registry to allow the system to execute ActiveX controls that are served from within the Intranet zone. For more information on modifying the registry to workaround this issue, refer to Microsoft Knowledge Base article 892675, which is available at this URL:

<http://support.microsoft.com/kb/892675>.

- CSCin59664

Symptom: In some cases, IP/TV Program Manager lists files from IP/TV Broadcast Servers that are not managed by that particular IP/TV Program Manager.

Condition: This problem occurs when an IP/TV Program Manager no longer manages an IP/TV Broadcast Server that is listed in IP/TV Program Manager.

Workaround: When an IP/TV Broadcast Server is down, delete the server from the list of servers in that IP/TV Program Manager.

- CSCin61218

Symptom: IP/TV generates poor-quality audio and video.

Condition: This problem occurs when you use very low values in the Audio/Video Bandwidth field of the New Program window.

Workaround: Use the values given in Appendix A of the *Cisco IP/TV Broadcast Server User Guide, Release 5.1*. The document is available at this URL:

http://www.cisco.com/en/US/products/sw/conntsw/ps1869/products_user_guide_list.html

- CSCin63819

Symptom: The concurrent file transfer setting in the IP/TV Program Manager Preferences window does not take effect.

Condition: This problem occurs if you attempt to specify the concurrent file transfer option through the IP/TV Program Manager Preferences window.

Workaround: There is no known workaround.

Resolved Caveats in IP/TV Program Manager, Release 5.4

This section lists the resolved caveats in IP/TV Release 5.4.

- CSCei32852

A manifest file syntax error occurs when you try to create a Content Delivery Management (CDM) report for IPTV-ACNS integrated VOD programs that were created on Program Manager with filenames that contain a special character such as "&".

- CSCsc07812

A hacker can access unauthorized information (such as operating system details, software version numbers running on the server, server cookies, and authentication information) under the following conditions:

- When an HTTP Request is given to the Program Manager and the Apache Web server Server Token has not been set.
- When an HTTP trace request is given to the Program Manager and the HTTP TRACE has not been enabled in the web server.

- CSCeh13038

IP/TV Program Manager does not allow you to create a live program when the number of live programs on a Broadcast Server exceeds half the number of SSM addresses available. For example, if your SSM range has five multicast addresses, IP/TV Program Manager allows you to create two live programs on a Broadcast Server but generates the error message when you create a third live program. IP/TV Program Manager returns the following error message while creating a live program:

```
IP/TV found the following errors on your New Program page:  
IP/TV is unable to allocate multicast IP for this program. Please use Advanced Option  
to create the program and allocate the multicast IP manually.  
These data entry errors need to be fixed.  
Click the Back button to return to the New Program page.
```

Related Documentation

Use these release notes in conjunction with the following documents:

- *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.4*
- *Cisco IP/TV Release 5.2 Addendum*
- *Cisco IP/TV Broadcast Server User Guide, Release 5.1*
- *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.1*
- *Cisco IP/TV Viewer User Guide, Release 5.1*
- *Cisco IP/TV 3400 Series Servers User Guide*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Cisco Content Engine 511 and 566 Hardware Installation Guide*
- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.3*
- *Release Notes for Cisco ACNS Software, Release 5.3*

Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.4 documentation is located at the following website:

http://www.cisco.com/en/US/products/sw/conntsw/ps1869/products_user_guide_list.html

Cisco ACNS Software Program Manager for IP/TV, Release 5.3 documentation is located at the following website:

http://www.cisco.com/en/US/products/sw/conntsw/ps491/prod_release_notes_list.html

Cisco ACNS Software, Release 5.4 documentation is located at:

http://www.cisco.com/en/US/products/sw/conntsw/ps491/prod_release_notes_list.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command

output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://cisoiq.texterity.com/cisoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.
