Preface

This preface describes who should read the *Cisco ACNS Software Configuration Guide for Locally Managed Deployments,* how it is organized, and its document conventions. This preface contains the following sections:

Document Objectives

This guide is intended for administrators who want to configure, manage, and monitor standalone Content Engines that are running Cisco Application and Content Networking System (ACNS) 5.5 software.

The term *standalone Content Engines* is used throughout this guide to refer to Content Engines that the ACNS administrators have intentionally not registered with a Content Distribution Manager so that they can configure, manage, and monitor these Content Engines as standalone devices.

The term *locally managed deployments* is used throughout this guide to refer to deployments that consist of one or more standalone Content Engines that are running the ACNS 5.x software and are configured as caching and streaming engines.

Note To initially configure a Content Engine as a standalone device, you turn off the autoregistration feature so that the Content Engine will not automatically register with the Content Distribution Manager, and so that you can individually manage it through the Content Engine command-line interface (CLI) or the Content Engine graphical user interface (GUI) as a standalone device.

The Content Engine GUI allows you to configure, manage, and monitor standalone Content Engines remotely through your browser, a console connection or a terminal emulation program. Although either the Content Engine GUI or the CLI can be used to configure and manage standalone Content Engines, the instructions and examples in this guide primarily use the CLI method. (Certain features can be configured through the Content Engine CLI only.) The Content Engine GUI has context-sensitive online help that can be accessed by clicking the **HELP** button. See Appendix A, "Content Engine GUI Menu Options," for a complete list of Content Engine GUI options.

This guide explains how to configure, manage, and monitor standalone Content Engines running the ACNS 5.4 software for the following purposes:

- Transparent forward caching deployments
  - For conventional caching (DNS, HTTP, HTTPS, and native FTP caching)
  - For Windows Media Technologies (WMT) transparent caching
  - For RealMedia transparent caching
- Transparent reverse proxy caching deployments (HTTP caching for reverse proxy packets)
- Nontransparent forward proxy caching deployments:
  - For conventional caching (HTTP, HTTPS, and FTP-over-HTTP caching)
  - For WMT proxy caching
  - For RealMedia proxy caching
- WMT streaming deployments
- Real-Time Streaming Protocol (RTSP) streaming deployments

Note If you are using content routing, you must use the Content Distribution Manager. For information about configuring a centrally managed ACNS network device (Content Engines or Content Routers that are registered with a Content Distribution Manager), see the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5*.

Audience

This guide is intended for administrators who want to configure, manage, and monitor standalone Content Engines. The administrator should be familiar with Cisco router and switch configuration. An understanding of caching and streaming concepts is necessary. This guide is not a tutorial.

Document Organization

This guide includes the following chapters and appendixes that are divided into six parts:

- Overview that introduces some basic concepts and the typical ways to deploy standalone Content Engines
- Basic configuration for standalone Content Engines
- Configuration of content services for standalone Content Engines
- Advanced configuration of standalone Content Engines
- Monitoring and troubleshooting of standalone Content Engines
- Reference material that is pertinent to configuring and monitoring standalone Content Engines (for example, a list of Content Engine GUI options, a list of supported WCCP services, and a matrix of supported caching, filtering, and authentication mechanisms per protocol)

:

Chapter	Title	Description
Part 1	**Overview**	
Chapter 1	Introduction	Provides a brief overview of the ACNS network solution, and introduces the typical ways to deploy a standalone Content Engine.
Chapter 2	Understanding the Basics	Provides an overview of some basic concepts that are important to understand before you configure a standalone Content Engine for caching and streaming.
Chapter 3	Deployment Scenarios for Standalone Content Engines	Describes the typical ways that you can deploy standalone Content Engines as streaming and caching engines.
Part 2	**Basic Configuration for Standalone Content Engines**	
Chapter 4	Getting Started	Describes the procedures for configuring a basic configuration on standalone Content Engines. Includes instructions on how to use the interactive Setup utility to configure a basic configuration (device network settings, disk configurations, and some commonly used caching services) on standalone Content Engines. Also provides some important information about how to get started (for example, how to log in to a standalone Content Engine and preload content on it).
Chapter 5	Performing Other Basic Tasks for Standalone Content Engines	Describes how you can use the Content Engine CLI to perform other basic tasks such as setting the system clock and managing login accounts.

Chapter	Title	Description
Chapter 6	Configuring Transparent Redirection for Standalone Content Engines	Describes how to configure WCCP and Layer 4 switching as redirection methods that transparently intercept and redirect content requests (caching and streaming) to standalone Content Engines.
Chapter 7	Configuring Conventional Caching Services for Standalone Content Engines	Describes how to configure conventional caching services (DNS, HTTP, FTP, and HTTPS caching) on standalone Content Engines.
Chapter 8	Configuring RealMedia Services on Standalone Content Engines	Describes how to configure RealMedia streaming and caching services on standalone Content Engines. Also describes how to configure the Real-Time Streaming Protocol (RTSP) gateway, which runs on the Content Engine, and directs RTSP requests to the appropriate backend RTSP server (for example, the RealProxy server).
Chapter 9	Configuring WMT Streaming Media Services on Standalone Content Engines	Describes how to configure Windows Media Technologies (WMT) streaming and caching services on standalone Content Engines.
Part 3	**Configuration of Content Services for Standalone Content Engines**	
Chapter 10	Configuring Content Authentication and Authorization on Standalone Content Engines	Describes how to configure access control on a Content Engine for processing HTTP, HTTPS, and FTP requests for content.
Chapter 11	Configuring Content Preloading and URL Filtering on Standalone Content Engines	Describes how to configure a standalone Content Engine to configure content preloading and URL filtering on standalone Content Engines.
Chapter 12	Configuring ICAP on Standalone Content Engines	Describes how to configure a standalone Content Engine (HTTP proxy server) to use the Internet Content Adaptation Protocol (ICAP) to communicate with an external ICAP server that filters and adapts the requested content.
Chapter 13	Configuring the Rules Template on Standalone Content Engines	Describes how to configure a standalone Content Engine to use a set of configured rules to filter HTTP, HTTPS, FTP-over-HTTP, WMT, and RTSP requests. These configured rules rewrite certain headers, redirect the request, or otherwise manipulate the request.
Part 4	**Advanced Configuration of Standalone Content Engines**	
Chapter 14	Configuring Primary and Backup Proxy Servers for Standalone Content Engines	Describes how to configure primary and backup (failover) proxy servers for standalone Content Engines.

Chapter	Title	Description
Chapter 15	Configuring Advanced Transparent Caching Features on Standalone Content Engines	Describes how to configure advanced transparent caching features (for example, IP spoofing, traffic bypass, and flow protection) on standalone Content Engines.
Chapter 16	Configuring Additional Network Interfaces and Bandwidth on Standalone Content Engines	Describes how to set up additional network interfaces and configure bandwidth for these interfaces and content services on standalone Content Engines.
Chapter 17	Configuring Administrative Login Authentication and Authorization on Standalone Content Engines	Describes how to configure a standalone Content Engine to use specific login authentication mechanisms (local, RADIUS, or TACACS+) to process administrative login requests (requests from administrators who want to log on to a standalone Content Engine for configuration, monitoring, or troubleshooting purposes).
Chapter 18	Configuring AAA Accounting on Standalone Content Engines	Describes how to configure authentication, authorization, and accounting (AAA) accounting using TACACS+ for standalone Content Engines.
Chapter 19	Creating and Managing IP Access Control Lists for Standalone Content Engines	Describes how to configure and manage IP access control lists (ACLs) to control access to specific applications or interfaces on standalone Content Engines.
Chapter 20	Viewing and Modifying TCP Stack Parameters on Standalone Content Engines	Describes how to view or modify TCP stack parameters on standalone Content Engines.
Part 5	**Monitoring and Troubleshooting**	
Chapter 21	Monitoring Standalone Content Engines and Transactions	Describes how to monitor standalone Content Engines and transactions.
Chapter 22	Troubleshooting	Describes troubleshooting with standalone Content Engines.
Part 6	**Reference Material for Standalone Content Engines**	
Appendix A	Content Engine GUI Menu Options	Describes the tabs and subtabs (menu options) that are available from the Content Engine GUI. This GUI is an alternative method to the Content Engine CLI for configuring and monitoring standalone Content Engines.
Appendix B	Reference Material for Standalone Content Engine Deployments	Contains important reference material (for example, a list of supported WCCP services and a matrix of supported caching, filtering, and authentication mechanisms per protocol) that is pertinent to configuring and monitoring standalone Content Engines.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands, keywords, and button names are in **boldface**.
italic font	Variables for which you supply values are in *italics*. Directory names and filenames are also in italics.
`screen` font	Terminal sessions and information the system displays are printed in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Variables you enter are printed in *`italic screen`* font.
plain font	Enter one of a range of options as listed in the syntax description.
^D or **Ctrl-D**	Hold the **Ctrl** key while you press the **D** key.
string	Defined as a nonquoted set of characters. For example, when setting a community string for SNMP to "public," do not use quotation marks around the string, or the string will include the quotation marks.
Vertical bars (|)	Vertical bars separate alternative, mutually exclusive, elements.
{ }	Elements in braces are required elements.
[ ]	Elements in square brackets are optional.
{**x** | **y** | **z**}	Required keywords are grouped in braces and separated by vertical bars.
[**x** | **y** | **z**]	Optional keywords are grouped in brackets and separated by vertical bars.
[{ }]	Braces within square brackets indicate a required choice within an optional element.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For additional information on the Cisco ACNS software, see the following documentation:

- *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.5*
- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5*
- *Cisco ACNS Software Command Reference, Release 5.5*
- *Cisco ACNS Software API Guide, Release 5.5*
- *Release Notes for Cisco ACNS Software, Release 5.5*

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/cisco/web/support/index.html

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/web/siteassets/locator/index.html

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/cisco/web/support/index.html

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/cisco/web/support/index.html

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/en/US/support/tsd_contact_technical_support.html

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/web/about/ac123/ac114/about_cisco_packet_magazine.html

- *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/web/about/ac123/ac114/about_cisco_packet_magazine.html

  or view the digital edition at this URL:

  http://www.cisco.com/web/about/ac123/ac114/about_cisco_packet_magazine.html

- *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/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- 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:

  https://supportforums.cisco.com/index.jspa

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

  http://www.cisco.com/web/learning/index.html