



Data Sheet

CiscoWorks Hosting Solution Software 1.9

As companies turn to content networking technologies to deliver information and services to their customers, the need to manage and administer this unique and rigorous environment is rising. Designed to better enable companies to manage their content networking, CiscoWorks Hosting Solution Software (HSS) proactively manages the availability of data center infrastructure for Layer 4–7 network services.

Product Overview

CiscoWorks HSS is a complete and self-contained network management software package that helps operators to monitor, activate or suspend, and configure load-balancing services in data centers based on Cisco Systems® equipment. As part of the Cisco® Business-Ready Data Center, CiscoWorks HSS helps you to protect, optimize, and increase your business by providing up-to-date configuration, fault, and performance information about the network infrastructure, plus Layer 4–7 load-balancing services.

CiscoWorks HSS provides an access security model that facilitates delegation of authority and responsibility for operations, administration, and monitoring of Cisco load-balancing devices, including activation and suspension of selected load-balanced servers. CiscoWorks HSS automatically discovers the data center infrastructure and then can immediately begin collecting statistics and management information, providing a current snapshot of the managed environment. This up-to-date information helps operational staff to easily pinpoint the source of a problem. CiscoWorks HSS is a manageable software solution with a full Cisco Discovery Protocol implementation and supports Cisco MIB II.

CiscoWorks HSS 1.9 is an easily deployed software installation. The software provides an ISO load image, including all of the OS, device drivers, and HSS management software. Because of performance specifications and support requirements, CiscoWorks HSS 1.9 must run on a dedicated platform and cannot run other applications on the same platform.

By using CiscoWorks HSS 1.9 with the supported reference platforms, customers can take advantage of more widely available hardware sparing, maintenance, and support. The supported reference platforms provide a minor but discernable increase in both capacity and performance of the CiscoWorks Hosting Solution Engine (HSE) in heavily loaded environments. Table 1 lists features and benefits of Cisco HSS.

Table 1. Features and Benefits

Feature	Benefit
Flexible user security model with granular, tiered user access to content switches	Removes unnecessary overhead between network administrators and server managers to increase productivity of all operational staff; allows administrative tasks to be securely delegated without granting full device access
Configuration and activation of Layer 4–7 e-business services	Provides productivity gains for server managers by offering daily management features such as taking Web servers in and out of service, graceful shutdown, and changing weight; provides ability to perform simultaneous configurations to multiple devices at one time
Up-to-date, at-a-glance fault and performance monitoring of the data center infrastructure	Saves time and resources in daily operations through an optimized, operational GUI used to monitor Cisco infrastructure
Proactive Layer 4–7 e-business service monitoring	Saves time in troubleshooting e-business availability and the application traffic distribution among Web servers

Feature	Benefit
Web-based, lightweight, secure GUI with easy customer view personalization and reporting	Generates incremental revenue for managed service providers with one-stop customer service management
Fault event notifications for user-defined threshold crossing alerts through syslog, trap, or e-mail	Provides upper-layer network management systems and operations support systems integration for analysis

CiscoWorks HSS is ideal for enterprises and service providers that implement Cisco content switches such as the Cisco Content Services Switch (CSS) and the Cisco Content Switching Module (CSM) for the Cisco Catalyst® 6000 Series switches. These customers range from data center infrastructure providers, application service providers, and large enterprises, to e-business data centers and small and medium-sized enterprises.

Key Features and Benefits

CiscoWorks HSS also offers the following key features:

- A granular user access model (Role-Based Access Control) is used to partition network resources for Layer 4–7 services and switch ports as well as authorize user group access to individual application services with their actions logged for auditing.
- Delegated activation and suspension of virtual IP addresses (VIPs), real servers, and services eliminate any need for server administrators to have network topology or operations knowledge, with access controlled by Role-Based Access Control.
- Robust Layer 4–7 service configuration of content switches, including virtual servers, real servers, and content owners and rules is provided by a secure Web-based GUI. Eliminating the need to use the command-line interface (CLI) helps enable common configuration of devices for standardization of policies.
- Enhanced configurations are supported for server load-balancing tasks such as on the Cisco Content Services Switch for VIP redundancy and on Cisco Catalyst 6000 Series switches with CSMs for CSM redundancy. Support for creation of policy maps to help set up content probing, validate proper configuration, and specifically set policies for cookie, URL, and session maps.
- Secure Sockets Layer (SSL) proxy services are monitored and reported on the Cisco Catalyst 6000 Series with SSL Service Module and Cisco Content Services Switch.
- Near-real-time flexible fault and performance monitoring of a select set of Cisco routers, switches, Cisco PIX® security appliances, Cisco content software, Cisco content switches, and Layer 4–7 services can be done in Cisco technology-based data centers.
- The secure Web-based GUI facilitates easy customer view/report personalization and historical data reporting.
- It is easy to create filters, make predefined groups, and perform rapid searches to make selections of one or a set of devices and services, enabling quick and easy administration even in environments with thousands of managed objects.
- Upper-layer management system integration includes syslog, trap, and e-mail notifications, as well as Extensible Markup Language (XML) export of historical data.

Application Features

CiscoWorks HSS has a flexible user security model that allows it to be used as a dedicated resource or shared by many customers. Within CiscoWorks HSS, *domains* can be defined to include a specified subset of devices, interfaces, and Layer 4–7 services in the managed data center that is accessible only to users with rights to that domain. For example, one Cisco Content Services Switch and a pair of Web servers can be grouped under a domain for a particular application or customer. Only users with assigned rights to that domain can see the existence of and act on the devices and services in that group. Similarly, within CiscoWorks HSS user *roles* define granular access to various features offered by CiscoWorks HSS. For instance, a server manager user role has access to Layer 4–7 monitoring, service activation, and service configuration

functionality. By combining the assignment of users to specific roles and domains, a specific customer's server manager account can be limited to only this customer's domain with the granted server manager user role.

Users are authenticated either by local accounts created on CiscoWorks HSS or by common remote authentication methods such as TACACS+, RADIUS, Lightweight Directory Access Protocol (LDAP), or Active Directory (AD). Using one of the common remote authentication methods can greatly simplify administrative work and allows CiscoWorks HSS operations to be integrated to existing access security methods. CiscoWorks HSS uses 128-bit full encryption Secure Sockets Layer (SSL) connections between its platform and the client Web browser for secure communications with users. Authorized users can monitor, activate, and configure Layer 4–7 services remotely, even through firewalls. In addition to the Web-based GUI, CLIs like that of Cisco IOS® Software provide direct console, Telnet, or Secure Shell (SSH) Protocol access to CiscoWorks HSS.

To complete the security environment, CiscoWorks HSS also records the configuration changes that users make to devices into an audit log file. This helps ensure that a clear record of who changed what and when is maintained. This log is stored in a secure text file.

CiscoWorks HSS provides for delegation of activation and suspension of Layer 4–7 e-business services, such as taking Web servers in and out of service. Layer 4–7 e-business services with availability status are mapped to Web servers in a domain-limited listing so that users need not have knowledge of the content switch hierarchy. For a given (shared) physical Web server, CiscoWorks HSS also provides a mapping of all the virtual servers and content rules using the server. By using CiscoWorks HSS, before taking a server down, you can easily disable all its services from one place, instead of visiting all the affected virtual servers, content rules, and related configuration tasks. During activation and suspension tasks, a status monitor allows you to track in near-real time the effect of an action. Quick actions are provided for routine daily operational tasks.

CiscoWorks HSS provides up-to-date fault and performance monitoring of Cisco routers, switches, content software, and content switches in Cisco technology-based data centers. Detailed system- and interface-level information provides quick problem identification, governed by user security. For example, the Device Status page lists all the data center network devices available to a particular user, including detailed system-level information (such as device operational status, uptime, IP address, and CPU and memory usage) and interface-level information (such as interface operational status, utilization, drops, and errors). The Service Status page lists all the Layer 4–7 services available to a user along with detailed network service information (such as service status, virtual servers, content rules, content services, hits per second, and total connections).

Layer 2–7 faults that occur within the customer domain are highlighted in the Alarms page. Filtering and sorting by priority is available to view and act upon selected faults. This capability enables CiscoWorks HSS to effectively monitor network degradation and unavailability.

CiscoWorks HSS supports robust Layer 4–7 configuration of content switches. It supports redundant configuration of owners, content rules, services, virtual servers, real servers and their bindings on Cisco Content Services Switch and Cisco Catalyst content switching modules, as well as configuration of virtual servers, real servers, server farms, and their bindings for Cisco IOS Software server load-balancing devices. Although it does not provide for every possible configuration task on these devices, it provides the bulk of those needed by operators implementing or modifying services.

CiscoWorks HSS supports monitoring and reporting of SSL proxy services on Cisco Catalyst 6000 Series switches with the SSL Services Module, and Cisco content services switches. It provides a view of the SSL proxy server list (such data as virtual IP address, index number, port, RSA key, RSA certificate, DSA key, DSA certificate) and SSL statistics (such as connections attempted, connections completed, full handshakes, data failures, number of cipher alerts). This capability allows CiscoWorks HSS to provide reports on the SSL Services Module.

Personalized views and reports can be easily created and customized for each user, governed by user security. For example, a few specific Layer 4–7 services and a few specific interfaces can be singled out from a customer's domain to create a detailed view or report with attributes. Specific attributes of interest (tables and columns) from all the categories of monitored data (routers, switches, and content switches) can be

grouped into a personalized view or report. These provide users with quick and easy access to critical information relevant to daily operations and can be shared with different users to simplify customer network management.

CiscoWorks HSS offers many predefined historical data reports for service hits, connections, CPU utilization, and so forth. Just as with personalized views, customized historical data reports can be built by selecting desired attributes based on customer domain. Reports can be run against a set of devices by selecting a report and specifying a time period. Reports can be configured to be e-mailed periodically, simplifying the tasks of distributing reports.

Reports are available in both tabular and graphic formats. These are based on the formats used by the Cisco Network Analysis Module (NAM), simplifying the coordination for analysis of data from CiscoWorks HSS and Cisco NAM when both are used. CiscoWorks HSS can provide up to a few weeks of historical data depending on the level of reporting collection required. Administrators can specify both aggregation and truncation frequencies for the monitored data. Historical data and views can be exported in CSV and XML formats.

Product Specifications

Table 2 lists supported reference platform specifications. Variation from supported reference platform specifications will not be supported.

Table 2. Supported Platform Specifications

	Hewlett Packard DL350	IBM xSeries 336
Product Number	Proliant DL360 G4	xSeries 336 8837E2U
Memory	2G PC2700 DDR 333 SDRAM	2G ECC DDR SDRAM
Processor	Intel Xeon 3.0-GHz/800-MHz Processor (dual capability) with 1-MB Layer 2 cache	3.0 GHz/800 MHz, 2-MB Layer 2 Intel Processor
Storage Controller	Smart Array 6i Plus Controller	Integrated Single-Channel Ultra320 SCSI Controller
Storage (Hard Drive)	One or two 36.4-GB Ultra320 (use two for redundancy)	One 36.4-GB, 2.5-inch, 10,000-RPM Ultra320 SCSI Hot-Swappable SL HDD
Storage Type	Hardware RAID	SCSI

Ordering Information

To place an order, visit the [Cisco Ordering Home Page](#). Purchase CiscoWorks HSS 1.9 by placing an order beginning October 30, 2005, through normal sales channels. This is the first release of CiscoWorks HSS 1.9. CiscoWorks HSS contains strong encryption technologies controlled by the U.S. government, and you will be prompted to apply for permission to access the encrypted files.

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

For More Information

For more information about the Cisco Works Hosting Solution Software, visit <http://www.cisco.com/en/US/products/ps6518/index.html>, contact your local account representative, or write to ciscoworks@cisco.com.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks or 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. (0502R)

KW/LW9532 10/05

