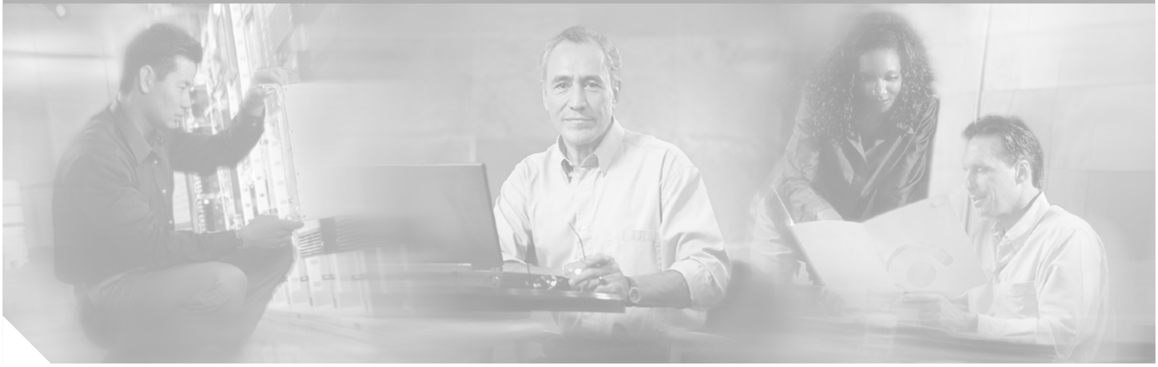
Cisco Systems



Cisco Content Services Switch Device Management User's Guide

March 2005

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

Text Part Number: OL-5653-02

Cisco Content Services Switch Device Management User’s Guide

CONTENTS

FIGURES

Preface

This guide provides information about accessing and using the Device Management user interface to configure and manage an 11500 series content services switch (hereinafter referred to as the CSS). Information in this guide applies to all CSS models except where noted.

The CSS software is available in a Standard or optional Enhanced feature set. The Enhanced feature set contains all of the Standard feature set and also includes Network Address Translation (NAT) Peering, Domain Name Service (DNS), Demand-Based Content Replication (Dynamic Hot Content Overflow), Content Staging and Replication, and Network Proximity DNS. Proximity Database and Secure Management, which includes Secure Shell Host and SSL strong encryption for the Device Management software, are optional features.

This preface contains the following major sections:

- Audience
- How to Use This Guide
- Related Documentation
- Symbols and Conventions
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the CSS:

- Web master
- System administrator
- System operator

How to Use This Guide

This section describes the chapters and contents in this guide.

Chapter	Description
Chapter 1, WebNS Device Management User Interface Overview	Provides an overview of the WebNS Device Management user interface.
Chapter 2, Configuring the CSS for Device Management	Describes the tasks that you need to perform before you use the Device Management user interface.
Chapter 3, Using the Device Management User Interface	Provides the basics on using the Device Management user interface.

Related Documentation

In addition to this document, the Content Services Switch documentation set includes the following:

Document Title	Description
Release Note for the Cisco 11500 Series Content Services Switch	This release note provides information on operating considerations, caveats, and command line interface (CLI) commands for the Cisco 11500 series CSS.
Cisco 11500 Series Content Services Switch Hardware Installation Guide	This guide provides information for installing, cabling, and powering the Cisco 11500 series CSS. In addition, this guide provides information about CSS specifications, cable pinouts, and hardware troubleshooting.
Cisco Content Services Switch Getting Started Guide	This guide describes how to perform initial administration and configuration tasks on the CSS, including: • Booting the CSS for the first time and a routine basis, and logging in to the CSS • Configuring the username and password, Ethernet management port, static IP routes, and the date and time • Configuring DNS server for hostname resolution • Configuring sticky cookies with a sticky overview and advanced load-balancing method using cookies • A task list to help you find information in the CSS documentation • Troubleshooting the boot process

Document Title	Description
Cisco Content Services Switch Administration Guide	This guide describes how to perform administrative tasks on the CSS, including upgrading your CSS software, and configuring the following: • Logging, including displaying log messages and interpreting sys.log messages • User profile and CSS parameters • SNMP • RMON • XML documents to configure the CSS • CSS scripting language • Offline Diagnostic Monitor (Offline DM) menu
Cisco Content Services Switch Routing and Bridging Configuration Guide	This guide describes how to perform routing and bridging configuration tasks on the CSS, including: • Management ports, interfaces, and circuits • Spanning-tree bridging • Address Resolution Protocol (ARP) • Routing Information Protocol (RIP) • Internet Protocol (IP) • Open Shortest Path First (OSPF) protocol • Cisco Discovery Protocol (CDP) • Dynamic Host Configuration Protocol (DHCP) relay agent

Document Title	Description
Cisco Content Services Switch Content Load-Balancing Configuration Guide	This guide describes how to perform CSS content load-balancing configuration tasks, including: • Flow and port mapping • Services • Service, global, and script keepalives • Source groups • Loads for services • Server/Application State Protocol (SASP) • Dynamic Feedback Protocol (DFP) • Owners • Content rules • Sticky parameters • HTTP header load balancing • Content caching • Content replication
Cisco Content Services Switch Global Server Load-Balancing Configuration Guide	This guide describes how to perform CSS global load-balancing configuration tasks, including: • Domain Name System (DNS) • DNS Sticky • Content Routing Agent • Client-Side Accelerator • Network proximity
Cisco Content Services Switch Redundancy Configuration Guide	This guide describes how to perform CSS redundancy configuration tasks, including: • VIP and virtual interface redundancy • Adaptive session redundancy • Box-to-box redundancy

Document Title	Description
Cisco Content Services Switch Security Configuration Guide	This guide describes how to perform CSS security configuration tasks, including: • Controlling access to the CSS • Secure Shell Daemon protocol • Radius • TACACS+ • Firewall load balancing
Cisco Content Services Switch SSL Configuration Guide	This guide describes how to perform CSS SSL configuration tasks, including: • SSL certificate and keys • SSL termination • Backend SSL • SSL initiation
Cisco Content Services Switch Command Reference	This reference provides an alphabetical list of all CLI commands including syntax, options, and related commands.

Symbols and Conventions

This guide uses the following symbols and conventions to identify different types of information.

⚠ **Caution** A caution means that a specific action you take could cause a loss of data or adversely impact use of the equipment.

Warning **A warning describes an action that could cause you physical harm or damage the equipment.**

Note A note provides important related information, reminders, and recommendations.

Bold text indicates a command in a paragraph.

`Courier text` indicates text that appears on a command line, including the CLI prompt.

`Courier bold text` indicates commands and text you enter in a command line.

Italics text indicates the first occurrence of a new term, book title, and emphasized text.

1. A numbered list indicates that the order of the list items is important.
    a. An alphabetical list indicates that the order of the secondary list items is important.

- A bulleted list indicates that the order of the list topics is unimportant.
    - An indented list indicates that the order of the list subtopics is unimportant.

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/univercd/home/home.htm

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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

- *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

- 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

WebNS Device Management User Interface Overview

The WebNS Device Management user interface is an HTML-based Web application that you use to configure and manage a Cisco 11500 series content services switch (CSS). The WebNS Device Management user interface is part of the WebNS system software included with each CSS. The Device Management user interface allows you to configure and monitor a CSS. You can manage a single CSS or, using multiple browser windows, you can manage multiple CSSs.

You access the WebNS Device Management user interface from a Web browser (Microsoft Internet Explorer is recommended). The Web browser typically connects to the Device Management user interface through the CSS Ethernet Management port.

This chapter includes the following topics:

- Browser and Platform Support
- WebNS Device Management User Interface
- Supported Features in the Device Management User Interface

Browser and Platform Support

The WebNS Device Management user interface has the following requirements:

- **Color Recommendations**—The minimum display resolution required is SVGA (800x600 resolution). For best results, use XGA (1024x768 resolution).
- **Browser Support**—The WebNS Device Management user interface requires Microsoft Internet Explorer version 5.0 or later, or Netscape Navigator 4.08, Communicator 4.51 or 4.71.

Note If the entire navigation tree does not display in Netscape Navigator or Communicator, press **Shift**, then click **Reload** to refresh your browser. The navigation tree will not display if you are using Netscape Communicator version 4.72, 4.73 or 4.74.

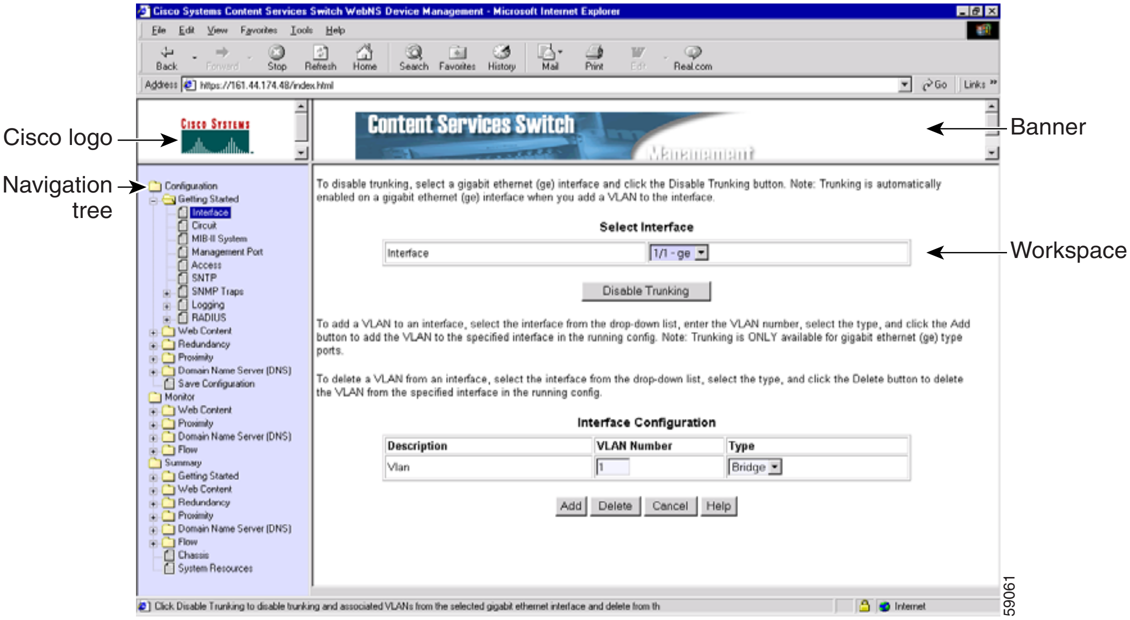
WebNS Device Management User Interface

The Device Management user interface is divided into four areas or frames:

- **Navigation Tree**—The Navigation tree (located in the lower left frame of the browser window) lists Configuration, Monitor, and Summary options arranged by category. Many of these options are the same as those found in the Command Line Interface (CLI). Each icon in the Navigation Tree corresponds to a Configuration form, a Monitor form, or a Summary form. Click the form name in the Navigation tree to display the associated form in the Workspace frame.
- **Workspace Frame**—The Workspace is a large frame that displays the Configuration form, Monitor form, or Summary form corresponding to the navigation tree option that you select. A form may contain a single task or may involve a configuration form that includes multiple steps designed to simplify the process of setting up basic services on your CSS.
- **Cisco Logo**—Clicking the Cisco Systems logo in the upper left corner opens a secondary browser window that links to Cisco.com, the Cisco Systems corporate Web site.
- **Banner**—Clicking the Content Services Switch banner opens a secondary browser window linking to the Cisco.com Web site.

Figure 1-1 provides a typical example of a WebNS Device Management user interface form.

Figure 1-1 WebNS Device Management User Interface Example



To disable trunking, select a gigabit ethernet (ge) interface and click the Disable Trunking button. Note: Trunking is automatically enabled on a gigabit ethernet (ge) interface when you add a VLAN to the interface.

Select Interface

Interface	1/1 - ge

To add a VLAN to an interface, select the interface from the drop-down list, enter the VLAN number, select the type, and click the Add button to add the VLAN to the specified interface in the running config. Note: Trunking is ONLY available for gigabit ethernet (ge) type ports.

To delete a VLAN from an interface, select the interface from the drop-down list, select the type, and click the Delete button to delete the VLAN from the specified interface in the running config.

Interface Configuration

Description	VLAN Number	Type
Vlan	1	Bridge

Click Disable Trunking to disable trunking and associated VLANs from the selected gigabit ethernet interface and delete from th

Supported Features in the Device Management User Interface

The Device Management user interface offers many of the same CSS capabilities that are available through the Command Line Interface (CLI). This section summarizes the supported CSS features, divided by:

- CSS Configuration Form Features
- CSS Monitor Form Features
- CSS Summary Form Features

CSS Configuration Form Features

The Device Management user interface offers many of the same CSS configuration capabilities that are available through the Command Line Interface (CLI). All Configuration forms are available under the Configuration Navigation Tree. The list below summaries the Configuration forms and associated parameters:

- **Interface**—Interface name, VLAN number, VLAN type (bridge or trunk).
- **Circuit**—VLAN number, IP address, IP prefix length.
- **MIB-II system information**—Name, contact, location, description, object ID, system up time.
- **Management port**—IP address and subnet mask.
- **Access**—Console, FTP, SNMP, Telnet, XML, console and virtual authentication.
- **SNTP**—State, server IP address, version, poll-interval, SNTP server state, seconds since last update.
- **SNMP traps**—Trap hosts, generic traps, enterprise traps (such as login failure, redundancy, service, DoS LAND attack, and so on).
- **Logging**—Logging host and logging disk filename, subsystems, and via email.
- **RADIUS**—RADIUS client, primary Remote Authentication Dial-In User Server (RADIUS) server, and secondary RADIUS server.

- **Portmapping**—Global portmapping, no-flow DNS portmapping.
- **Service**—Name, Adaptive Session Redundancy, IP address, type, protocol, port, domain, weight, maximum connections, string, cache bypass, bypass host tag, transparent host tag, keepalive type.
- **Owner**—Owner name, address, billing information, e-mail address, case, DNS exchange policy, DNS load-balancing method.
- **Content rule**—Owner name, Adaptive Session Redundancy, content name, virtual IP address, TCP/UDP port number, IP protocol, DNS balance, load balance, load threshold, bypass transparent caches, failover, primary sorry server, secondary sorry server, persistence, application type, sticky connection parameters, URL, EQL, URQL.
- **Services in content rule**—Owner name-content rule, service name, weight.
- **Source group**—Name, Adaptive Session Redundancy, IP address, port-mapping parameters.
- **Services in source group**—Source group, service name, service type.
- **Extension Qualifier Lists (EQLs)**—EQL name, description.
- **EQL Extension**—EQL extension, extension description.
- **Uniform Resource Locator Qualifier Lists (URQLs)**—Name, domain, description.
- **Uniform Resource Locators (URLs)**—URQL, number, URL, description.
- **Named keepalive**—Name, IP address, description, frequency, maximum failures, method, port, retry period, type, URI, FTP record name, script name, script arguments, script output.
- **Port Mapping**—Global port mapping, no-flow DNS port mapping.
- **Redundancy**—Box-to-box redundancy, VIP/interface redundancy, Adaptive Session Redundancy (ASR), Inter-Switch Communications (ISC).
- **Proximity**—APP, APP session, APP-UDP, Proximity Database (PDB), Proximity Domain Name Server (PDNS).
- **Domain Name System**—DNS server, DNS forwarder, DNS peer, domain acceleration, domain cache, DNS record, DNS Sticky, acceleration candidate, Content Routing Agent (CRA), CRA domain, CRA alias.
- **SSL Accelerator**—SSS proxy list, SSL proxy list cipher suite, SSL backend server proxy list, SSL backend server proxy list cipher suite, assign proxy list to service.

- **Save Configuration**—Copy running configuration to start configuration, copy running configuration to startup configuration and archive startup configuration.

CSS Monitor Form Features

There are a number of forms in the Device Management user interface that allow you to view statistical information about the CSS. All Monitor forms are available under the Monitor Navigation tree. Monitor forms include: Owner, Content Rule, Content Service, Proximity APP-UDP, Proximity RTT Probe, DNS Server, DNS Forwarder, DNS Proximity, DNS Content Routing Agent, Flow Statistics, and Denial of Service.

CSS Summary Form Features

There are a number of forms in the Device Management user interface that allow you to view configuration and summary statistical information about the CSS. All Summary forms are available under the Summary Navigation tree. Summary forms include: Boot Configuration, Interfaces, Trunked Interfaces, Logging Subsystems, Trap Hosts, RADIUS, Show Service, Show Owner, Show Content, Show Keepalive, Content Service Usage, Services, Content Services, Source Groups, Source Group Services, Owners, Content Rules (Summary, Main, Advanced Balance, and String), URQLs, URLs, EQLs, EQL Extensions, Named Keepalives, Service Keepalives, Box-to-Box Redundancy (Summary, Protocol, Circuits, Physical Links), Proximity APP Sessions, DNS Records, DNS Record Keepalives, DNS Domain Cache, DNS Acceleration Candidates, Content Routing Agent Domains, Denial of Service Attacks, Chassis, Session Processors, and System Resources.

Configuring the CSS for Device Management

Before you can use the WebNS Device Management user interface software, you need to perform the tasks described in the following sections:

- WebNS Device Management User Interface Quick Start
- Enabling the WebNS Device Management User Interface
- Entering the Secure Management License Key for SSL Strong Encryption (optional)
- Configuring Idle Timeout (optional)
- Configuring an Ethernet Port
- Configuring an SNMP Community
- Restricting Access to the Device Management User Interface (optional, but recommended)
- Configuring Your Browser
- Viewing and Installing the SSL Security Certificate

WebNS Device Management User Interface Quick Start

Table 2-1 provides a quick overview of the steps required to configure the Device Management user interface on a CSS. Each step includes the CLI command required to complete the task. For a complete description of each feature and all the options associated with the CLI command, refer to the sections following the table.

Table 2-1   Device Management Configuration Quick Start

Task and Command Example

1. Enter config mode.
`# config`
`(config)#`

2. Enable the Device Management user interface. See the "Enabling the WebNS Device Management User Interface" section. `(config)# no restrict web-mgmt`

3. Configure an Ethernet port (for example, the management port) by entering an IP address and subnet mask for the port. See the "Configuring an Ethernet Port" section.
`(config)# boot`
`(config-boot)#`
`(config-boot)# ip address 192.168.16.2`
`(config-boot)# subnet mask 255.255.255.0`

4. Configure an SNMP community. See the "Configuring an SNMP Community" section. `(config)# snmp community sqa read-write`
5. Restrict access to the Device Management user interface to authorized users only with user access privileges and ACLs. See the "Restricting Access to the Device Management User Interface" section.
6. View and install the SSL security certificate. See the "Viewing and Installing the SSL Security Certificate" section.

Enabling the WebNS Device Management User Interface

Use the **no restrict web-mgmt** CLI command to enable access to the WebNS Device Management user interface. The Device Management user interface is disabled by default.

To enable the Device Management user interface in a CSS, enter:

```
(config)# no restrict web-mgmt
```

Note Access to the Device Management user interface requires that virtual authentication be enabled and configured for the authentication method you want to use. By default, virtual authentication is enabled and uses the local CSS database to authenticate users. If you have disabled virtual authentication, you must reenable it to access Device Management. For details about configuring virtual authentication, refer to the *Cisco Content Services Switch Security Configuration Guide*.

To disable the Device Management user interface in a CSS, enter:

```
(config)# restrict web-mgmt
```

To determine the state of the Device Management user interface on a CSS, enter:

```
# show running-config
!************************ Global **************************
virtual authentication
no restrict web-mgmt
```

When the Device Management user interface is enabled, the **no restrict web-mgmt** command appears in the running-config.

Note By default, the Device Management user interface software runs with Secure Sockets Layer (SSL) weak encryption enabled. To enable SSL strong encryption, see the "Entering the Secure Management License Key for SSL Strong Encryption" section later in this chapter.

Entering the Secure Management License Key for SSL Strong Encryption

To enable SSL strong encryption for the Device Management software, you must purchase the Secure Management software option. If you purchased the Secure Management software option:

- During the initial CSS order placement, the software Claim Certificate is included in the accessory kit.
- After receiving the CSS, Cisco Systems sends the Claim Certificate to you by mail.

Note If you cannot locate the license key Claim Certificate, call the Cisco Technical Assistance Center (TAC) toll free, 24 hours a day, 7 days a week at 1-800-553-2447 or 1-408-526-7209. You can also e-mail the TAC at tac@cisco.com.

Follow the instructions on the license key Claim Certificate to obtain the Secure Management software license key.

To enter the Secure Management license key and enable SSL strong encryption on your CSS:

1. Log in to the CSS and enter the **license** command.

   ```
   # license
   ```

2. Enter the Secure Management license key.

   ```
   Enter the Software License Key (q to quit): nnnnnnnnnnnn
   ```

The Secure Management license key is now properly installed and SSL strong encryption is enabled.

Note The internal Web server loads the appropriate cipher suite for SSL strong encryption automatically when you disable the Device Management software using the **restrict web-mgmt** command and then reenable it using the **no restrict web-mgmt** command.

Configuring Idle Timeout

By default, the idle timeout for all active web management session is disabled (set to 0). To set the maximum amount of time that any active web management session can be idle on the CSS before the CSS logs it out, use the **idle timeout web-mgmt** command. Enter a timeout value between 0 and 65535 minutes.

For example, to set an idle timeout value of 15 minutes for all active web management sessions, enter:

```
(config)# idle timeout web-mgmt 15
```

To disable the web management timeout period, enter:

```
(config)# no idle timeout web-mgmt
```

Configuring an Ethernet Port

To access the WebNS Device Management user interface, ensure that you first configure the appropriate Ethernet interface port (for example, the Ethernet Management port) from the CSS CLI.

1. Log into the CSS.
2. Enter config mode by typing **config** at the CLI.

   ```
   # config
   (config)#
   ```

3. Enter boot mode by typing **boot**.

   ```
   (config)# boot
   (config-boot)#
   ```

4. Enter an IP address and subnet mask for the management port.

   ```
   (config-boot)# ip address 192.168.16.2
   (config-boot)# subnet mask 255.255.255.0
   ```

Configuring an SNMP Community

Use the **snmp community** command to set or modify Simple Network Management Protocol (SNMP) community names to access SNMP. You may specify as many community names as you wish.

The syntax for this global configuration mode command is:

snmp community *community_name* [**read-only**|**read-write**]

The variables and options are:

- *community_name* - The SNMP community name for this system. Enter an unquoted text string with no space and a maximum length of 12 characters.
- **read-only**—Allow read-only access for this community.
- **read-write**—Allow read-write access for this community.

For example:

```
(config)# snmp community sqa read-write
```

For details on SNMP, refer to the *Cisco Content Services Switch Administration Guide*.

Restricting Access to the Device Management User Interface

We recommend that you restrict access to the WebNS Device Management user interface to users who have the authority to modify CSS configuration settings. There are two ways that you can restrict access:

- Using Privileges to Restrict Access
- Configuring Access Control Lists

Using Privileges to Restrict Access

To access the WebNS Device Management Configuration tree HTML pages (SNMP GETs and SETs), you must be a privileged CSS user (SuperUser access). This includes all secondary Configuration pages that you access from the primary Configuration pages.

Non-privileged users (those with User access) have read-only access to the Monitor and Summary pages (SNMP Gets) and cannot access the Configuration pages. If a non-privileged user tries to access a Configuration page, the restriction page appears with the following message:

```
You do not have the appropriate privileges to access the configuration
page.
```

Note You must enable cookies in your web browser to log in to the Device Management software.

For information on creating users with User and SuperUser access, refer to the *Cisco Content Services Switch Administration Guide*, Chapter 1, Getting Started.

Configuring Access Control Lists

You can use ACLs to restrict WebNS Device Management user interface access to specific IP addresses or subnets. ACLs provide traffic-filtering capabilities by controlling whether packets are forwarded or blocked at the CSS interfaces. You can configure ACLs for routed network protocols, filtering the protocol packets as the packets pass through the CSS.

If you use the CSS Ethernet management port to access the Device Management software, ACLs will have no effect. To take advantage of ACLs, use a different Ethernet port to access the Device Management software.

An ACL consists of clauses that you define. The CSS uses these clauses to determine how to handle each packet it processes. When the CSS examines each packet, it either forwards or blocks the packet based on whether or not the packet matches a clause in the ACL.

Caution ACLs function as a firewall security feature. When you enable ACLs, all traffic that is not configured in an ACL permit clause *will be denied*. It is extremely important that you first configure an ACL to permit traffic *before you enable ACLs*. If you do not permit any traffic, you will lose network connectivity. Note that the console port is not affected.

We recommend that you configure either a permit all or a deny all clause depending on your ACL configuration. For example, you could first configure a permit all clause and then configure deny clauses for only the traffic you wish to deny. Or, use the default deny all clause and configure permit clauses only for the traffic you wish to permit.

To define ACL clauses and to set ACL options, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Configuring Your Browser

Before you can access the Device Management software, you must ensure that the following items are enabled in your Web browser:

- Cookies - The Device Management software uses cookies for authentication. Your browser must have cookies enabled to obtain access to the Device Management pages. Cookies are created when you log in using the login page and are valid only for the current browser session. If the CSS does not find a cookie, it does not allow you to access any pages. If the CSS finds a cookie, it determines whether you have SuperUser or User privileges. You must have SuperUser privileges to access all pages. User privileges enable you to access only non-configuration pages. Use the **username** command to configure SuperUser and User privileges. See the "Using Privileges to Restrict Access" section.
- JavaScript - The Device Management software requires JavaScript for the navigation tree and the online Help.

Viewing and Installing the SSL Security Certificate

To protect data transfers (which can include passwords) between the WebNS Device Management user interface and your Web browser, we provide Secure Sockets Layer (SSL) as the standard Internet protocol for secure communications. SSL provides certificate-based authentication and public key cryptography to establish encrypted communication with clients and the WebNS Device Management user interface. Securing traffic consists of identifying (authenticating) the person configuring or monitoring the CSS, and once authenticated, encrypting the data.

With SSL, the HTTP Web server (which resides in the CSS) provides a secure connection between your Web browser and the CSS. The Web browser displays a "closed lock" (or similar symbol) at the bottom of each Device Management form to inform you that SSL is enabled.

The WebNS Device Management user interface supports SSL version 3.0. The user interface understands and accepts an SSL version 2.0 ClientHello message to allow dual version clients to communicate with the CSS. In this case, the client indicates an SSL version of 3.0 in the version 2.0 ClientHello, which informs the WebNS Device Management user interface that the client can support SSL version 3.0. The WebNS Device Management user interface returns a version 3.0 ServerHello message.

Note There are very few clients on the market today that support only SSL version 2.0. The WebNS Device Management user interface cannot communicate with a client that supports only version 2.0.

When you first access the Device Management user interface, a Security Alert message box prompts you to install and view the Cisco-issued security certificate. Depending on your security requirements, you can choose to install and view the certificate, or bypass the Security Alert message box and continue operating the CSS. Bypassing the Security Alert message box does not affect the security of the communications when using the Device Management user interface. The Security Alert message box appears every time you access the Device Management user interface until you either accept the certificate or disable the message box.

To view and install the SSL security certificate:

1. In your Web browser, enter the CSS IP address in the Address or Location field (depending on your browser). The URL requires an “s” (https://) when accessing the WebNS Device Management user interface to obtain a secure connection.

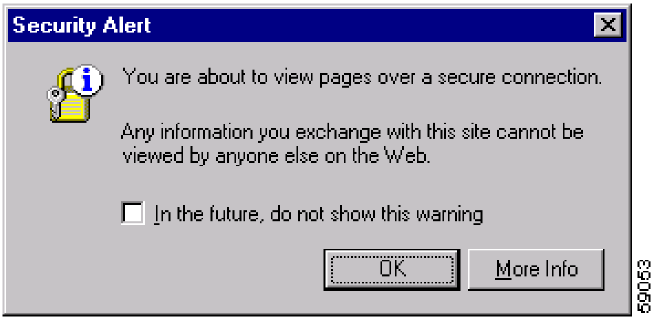
   For example:

   `https://192.168.16.2`

   Note If your Web browser has a bookmark to the WebNS Device Management user interface (WebNS version 4.10 or earlier) that includes a colon (:) and TCP 8081 management port number at the end of the IP address, the WebNS software denies the request. The browser indicates that the page cannot be displayed.

2. The first Security Alert message box appears stating that you are about to view pages over a secure connection. This is the standard Web browser message box that appears when requesting a secure page on the Internet.

Figure 2-1 First Security Alert Message Box



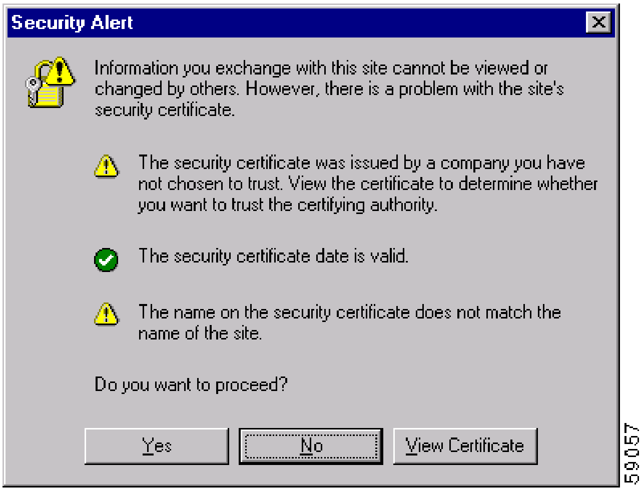
You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

□ In the future, do not show this warning

3. Click **OK**. The second Security Alert message box appears.

Figure 2-2 Second Security Alert Message Box



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

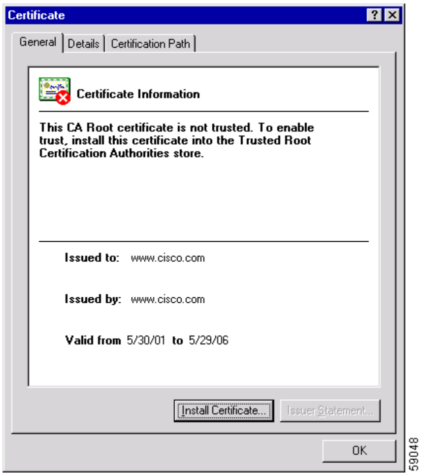
✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

4. Click **View Certificate**. The Certificate dialog box appears.

Figure 2-3   Certificate Dialog Box, General Property Tab



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate into the Trusted Root Certification Authorities store.

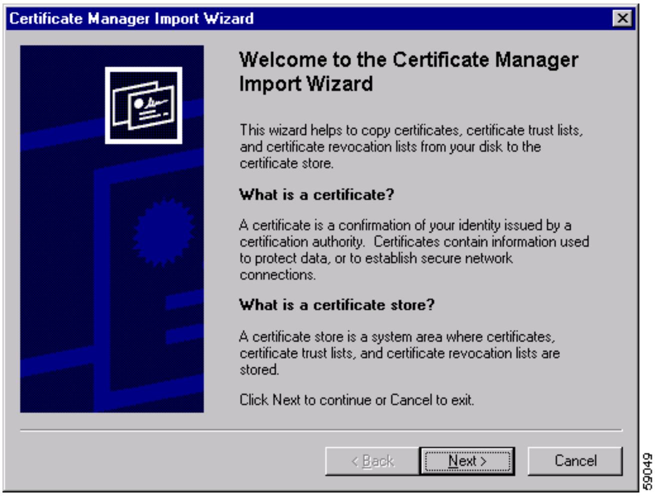
Issued to: www.cisco.com

Issued by: www.cisco.com

Valid from 5/30/01 **to** 5/29/06

5. Click **Install Certificate**. The Certificate Manager Import Wizard appears.

Figure 2-4   Certificate Manager Import Wizard



Welcome to the Certificate Manager Import Wizard

This wizard helps to copy certificates, certificate trust lists, and certificate revocation lists from your disk to the certificate store.

What is a certificate?

A certificate is a confirmation of your identity issued by a certification authority. Certificates contain information used to protect data, or to establish secure network connections.

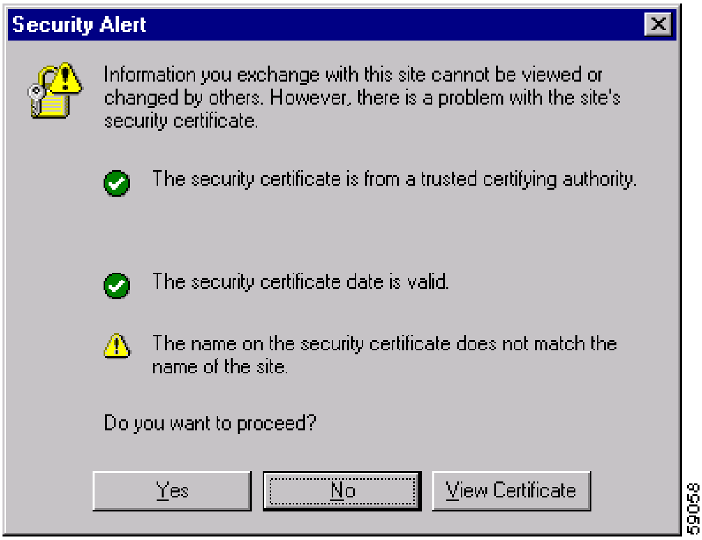
What is a certificate store?

A certificate store is a system area where certificates, certificate trust lists, and certificate revocation lists are stored.

Click Next to continue or Cancel to exit.

6. Click **Next**. Follow the prompts as the wizard steps you through the process of selecting a certificate store and importing the certificate. Use the wizard to copy the Cisco Systems-generated certificate into the certificate store on your computer (the system area where certificates are stored).
7. When you finish importing the certificate, you return to the Certificate dialog box shown in Figure 2-3.
8. Click **OK** to return to the Security Alert message box. Note that the first item in the list has changed to inform you that the security certificate is from a trusted certifying authority.

Figure 2-5 Security Alert Message Box With Certificate Information



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

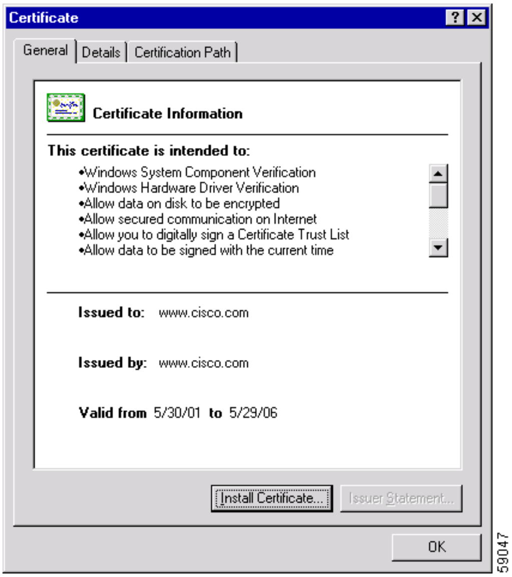
✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

9. Click **View Certificate**. The Certificate dialog box appears with the details of the certificate you imported.

Figure 2-6   Certificate Dialog Box With Certificate Information



Certificate Information

This certificate is intended to:

- Windows System Component Verification
- Windows Hardware Driver Verification
- Allow data on disk to be encrypted
- Allow secured communication on Internet
- Allow you to digitally sign a Certificate Trust List
- Allow data to be signed with the current time

Issued to: www.cisco.com

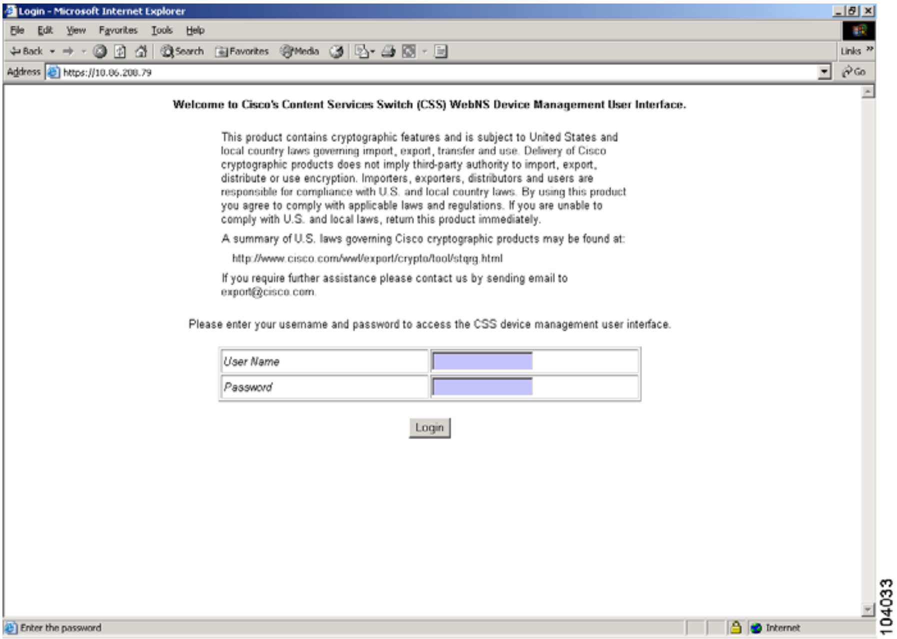
Issued by: www.cisco.com

Valid from 5/30/01 to 5/29/06

10. Click **OK**. The Device Management user interface Login form appears.

Figure 2-7 shows the Device Management Login form. For details on logging in to the Device Management software, see Chapter 3, Using the Device Management User Interface, in the "Accessing and Logging in to the WebNS Device Management User Interface" section.

Figure 2-7 WebNS Device Management User Interface Login Form



Welcome to Cisco's Content Services Switch (CSS) WebNS Device Management User Interface.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Please enter your username and password to access the CSS device management user interface.

User Name	
Password	

Login

Using the Device Management User Interface

Using the WebNS Device Management user interface, you can manage your CSS using a standard Web browser. This chapter describes the basics of using the Device Management user interface. It includes:

- Accessing and Logging in to the WebNS Device Management User Interface
- Navigating the WebNS Device Management Interface
- Adding or Modifying Configuration Information
- Using a Monitor Form
- Using a Summary Form
- Using Online Help
- Troubleshooting

Accessing and Logging in to the WebNS Device Management User Interface

Before establishing a WebNS Device Management user interface session, you must enable Device Management through the CLI and optionally create an ACL that defines the IP address that can connect to the management port. For more information, refer to Chapter 2, Configuring the CSS for Device Management, the "Enabling the WebNS Device Management User Interface" and "Configuring an SNMP Community" sections. For information on creating an ACL, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Note When you establish a connection to the CSS for Device Management using your Web browser, the CSS maintains that connection until the Web browser times out the connection. If you enter the **restrict web-mgmt** command at the CLI while a Device Management session is in progress, the CSS rejects any further navigation with the browser until you enter the **no restrict web-mgmt** command.

To access the WebNS Device Management user interface:

1. In your Web browser, enter the IP address of the CSS in the Address or Location field (depending on your browser). The URL requires an "s" (https://) when accessing the WebNS Device Management user interface to obtain a secure connection.

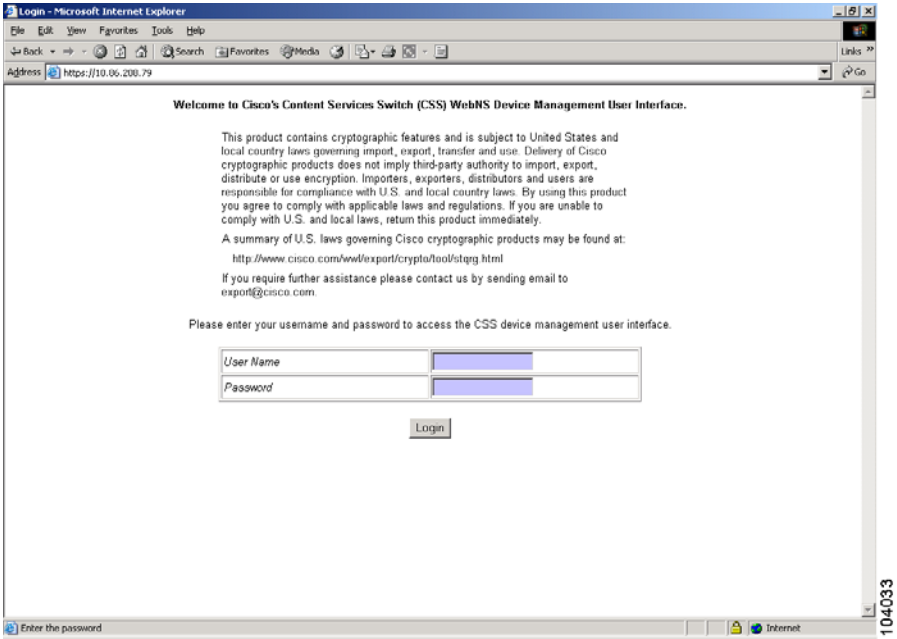
   For example:

   ```
   https://161.16.2.3
   ```

   The Security Alert message boxes appear informing you that you are about to view pages over a secure connection. These are the standard Web browser message boxes that appear when requesting any secure page on the Internet. For details on SSL security and installing the SSL security certificate, refer to Chapter 2, Configuring the CSS for Device Management, the "Viewing and Installing the SSL Security Certificate" section.

2. Click **Yes**. The WebNS Device Management Login form appears.

Figure 3-1 WebNS Device Management Login Form


Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Address https://10.86.208.79
Go
Enter the password
Internet
104033

Welcome to Cisco's Content Services Switch (CSS) WebNS Device Management User Interface.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Please enter your username and password to access the CSS device management user interface.

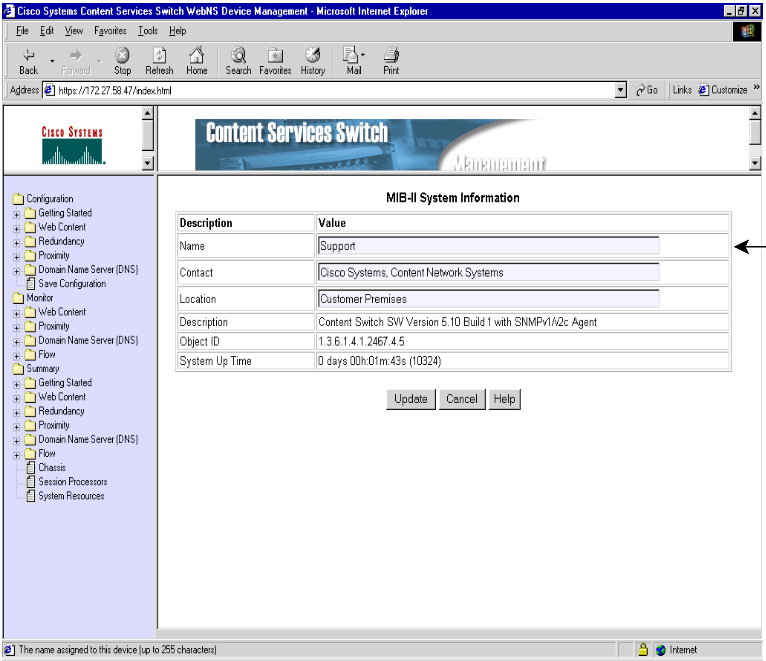
User Name	
Password	

Login

3. Enter a user name and password, then click **Login**. The MIB-II System Information form appears.

> **Note** The first time you log in to the WebNS Device Management user interface, use the default username of **admin** and the default password of **system**. To configure usernames and passwords, refer to the *Cisco Content Services Switch Getting Started Guide*, Chapter 1, Logging in and Getting Started.

Figure 3-2 WebNS Device Management MIB-II System Information Form



Cisco Systems Content Services Switch WebNS Device Management - Microsoft Internet Explorer

Address https://172.27.58.47/index.html

MIB-II System Information

Description	Value
Name	Support
Contact	Cisco Systems, Content Network Systems
Location	Customer Premises
Description	Content Switch SW Version 5.10 Build 1 with SNMPv1/v2c Agent
Object ID	1.3.6.1.4.1.2467.4.5
System Up Time	0 days 00h:01m:43s (10324)

The name assigned to this device (up to 255 characters)

Information related to the operating environment of the CSS.

Navigating the WebNS Device Management Interface

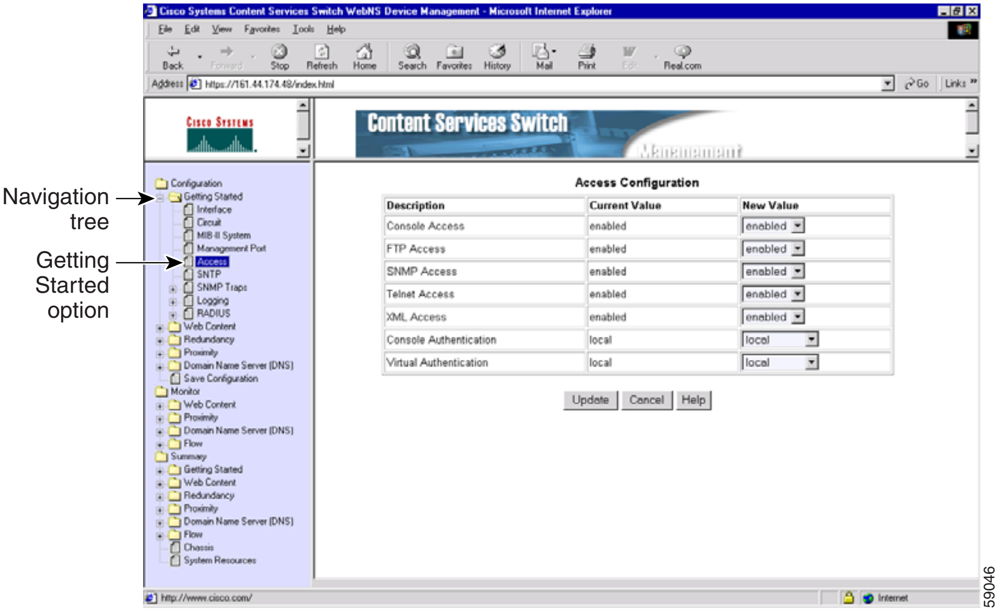
The Navigation tree (located in the lower left frame of the browser window) displays a list of folders that contain Configuration, Monitor, and Summary options that you select to configure and manage a CSS. Expand the appropriate folder, then select the option you want to configure. The Navigation tree lists Configuration, Monitor, and Summary options arranged by category.

Note Navigation tree icons may not always display properly, but the pages function correctly. Open a page by clicking the corresponding text.

For example, to configure access to your CSS:

1. Click the plus sign (+) next to the **Getting Started** folder in the Navigation tree. The folder expands to display a list of options that you can select to configure your CSS.
2. Click the **Access** icon. The Access Configuration form appears in the Workspace (right frame of the Device Management user interface) as shown in Figure 3-3.

Figure 3-3 Access Configuration Form



Access Configuration

Description	Current Value	New Value
Console Access	enabled	enabled
FTP Access	enabled	enabled
SNMP Access	enabled	enabled
Telnet Access	enabled	enabled
XML Access	enabled	enabled
Console Authentication	local	local
Virtual Authentication	local	local

3. Select the appropriate settings from the drop-down lists, then click **Update**. The software updates the CSS running configuration.

   To remove any changes you made in the form and return to the default values, click **Cancel**.

To obtain Online Help on a Device Management form and its fields, click the **Help** button at the bottom of the form (see the "Using Online Help" section for details on using Online Help).

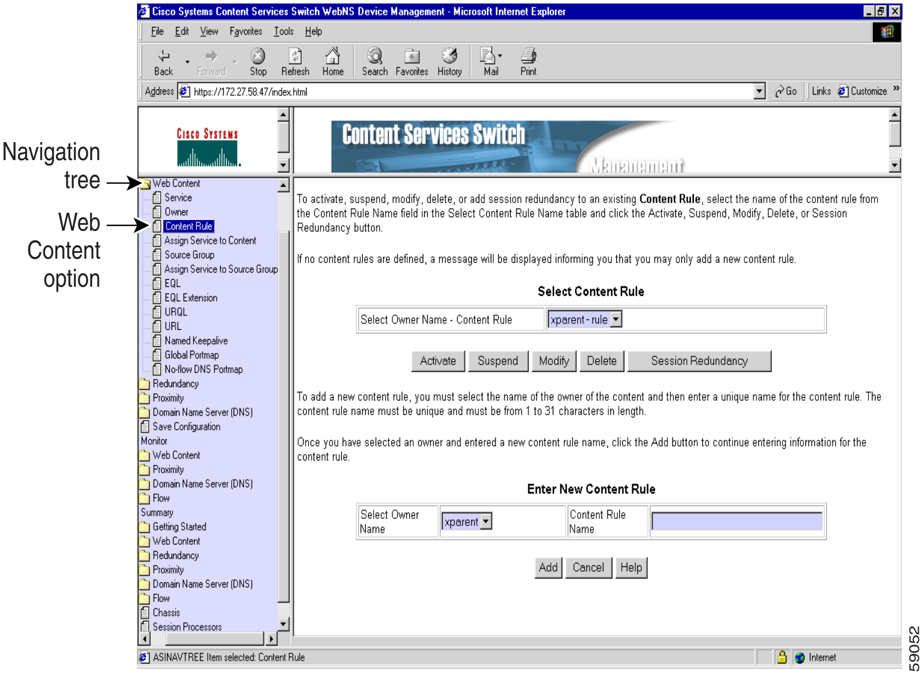
Adding or Modifying Configuration Information

A number of Configuration forms in the Web Content, Proximity, and Domain Name Server (DNS) Navigation tree allow you to add new configuration information to the CSS running configuration, and then to access, view, and modify that configuration information at a later time.

For example, to add a new content rule to the CSS running configuration, and then modify parameters in the content rule:

1. Click the plus sign (+) next to the **Web Content** folder in the Navigation tree. The folder expands to display a list of options that you can select to configure your CSS (Figure 3-4).

Figure 3-4 Content Rule Name Configuration Form



To activate, suspend, modify, delete, or add session redundancy to an existing **Content Rule**, select the name of the content rule from the Content Rule Name field in the Select Content Rule Name table and click the Activate, Suspend, Modify, Delete, or Session Redundancy button.

If no content rules are defined, a message will be displayed informing you that you may only add a new content rule.

Select Content Rule

Select Owner Name - Content Rule	xparent - rule

To add a new content rule, you must select the name of the owner of the content and then enter a unique name for the content rule. The content rule name must be unique and must be from 1 to 31 characters in length.

Once you have selected an owner and entered a new content rule name, click the Add button to continue entering information for the content rule.

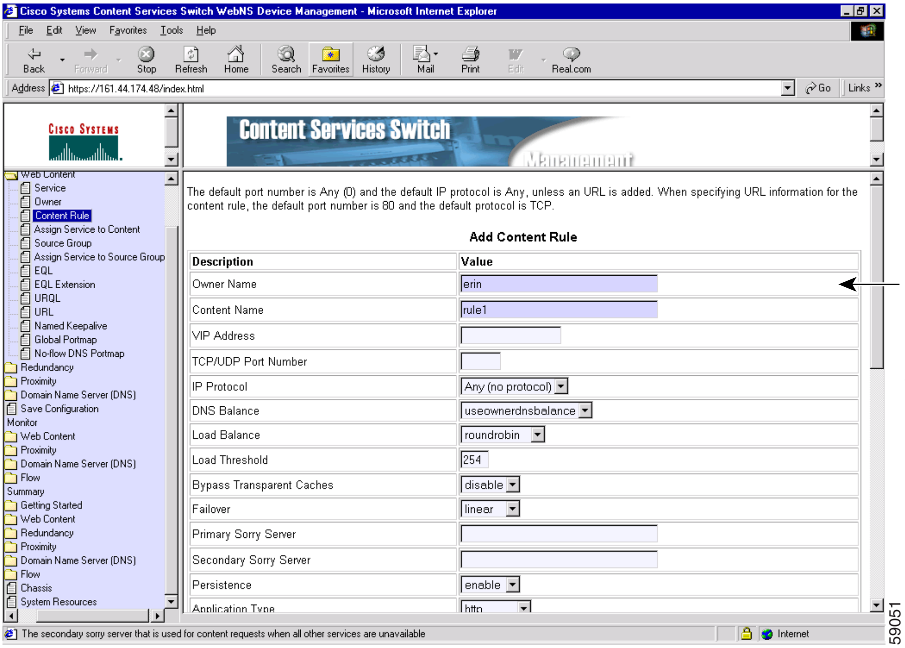
Enter New Content Rule

Select Owner Name	xparent	Content Rule Name	

2. Click the **Content Rule** icon. The Content Rule Name Configuration form appears in the Workspace (right frame of the Device Management user interface) as shown in Figure 3-4.

3. Select an owner name from the Select Owner Name drop-down list, then enter a content rule name. Click **Add** to access the Content Rule Configuration form (Figure 3-5) where you configure information related to the new content rule.

Figure 3-5 Content Rule Configuration Form



The default port number is Any (0) and the default IP protocol is Any, unless an URL is added. When specifying URL information for the content rule, the default port number is 80 and the default protocol is TCP.

Add Content Rule

Description	Value
Owner Name	erin
Content Name	rule1
VIP Address	
TCP/UDP Port Number	
IP Protocol	Any (no protocol)
DNS Balance	useownerdnsbalance
Load Balance	roundrobin
Load Threshold	254
Bypass Transparent Caches	disable
Failover	linear
Primary Sorry Server	
Secondary Sorry Server	
Persistence	enable
Application Type	http

The secondary sorry server that is used for content requests when all other services are unavailable

Enter information to configure a new content rule or to modify the information in an existing content rule.

4. Specify content rule, sticky, and content rule URL parameters to configure the content rule. When you are finished, click the **Add** button (located at the bottom of the Content Rule Configuration form) to save the content rule information in the CSS running configuration. The Content Rule Name Configuration form (see Figure 3-4) is redisplayed.

5. Click **Activate** to activate the content rule.

6. If you want to make a change to a content rule, select from the list of existing content rules in the Content Rule Name Configuration form, then click **Modify**. The Content Rule Configuration form (see Figure 3-5) for that content rule appears.

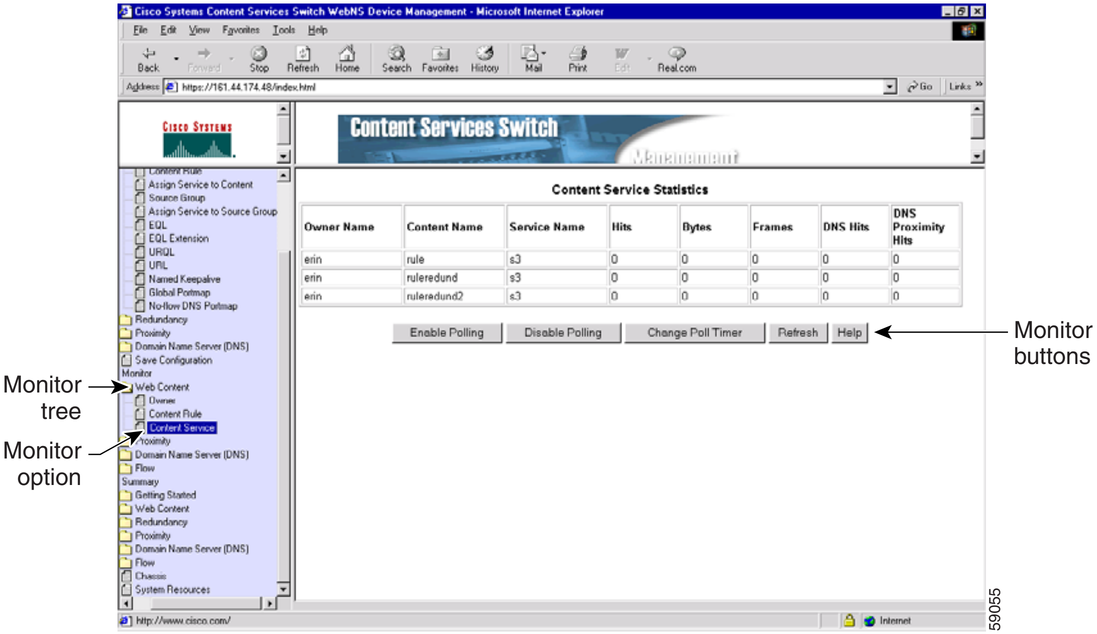
7. As necessary, modify content rule, sticky, and content rule URL parameters. When you are finished, click the **Modify** button (located at the bottom of the Content Rule Configuration form) to update the content rule information in the CSS running configuration. You return to the Content Rule Name Configuration form (see Figure 3-4).

Using a Monitor Form

There are a number of forms in the WebNS Device Management user interface that allow you to view statistical information about your CSS. Refer to Chapter 1, Using the Device Management User Interface, the "CSS Monitor Form Features" section.

To use a Monitor form, click the plus sign next to a folder in the Monitor tree. The folder expands to display a list of areas in your CSS that you can monitor.

Figure 3-6 Monitor Form Example



Content Service Statistics

Owner Name	Content Name	Service Name	Hits	Bytes	Frames	DNS Hits	DNS Proximity Hits
erin	rule	s3	0	0	0	0	0
erin	ruleredund	s3	0	0	0	0	0
erin	ruleredund2	s3	0	0	0	0	0

Monitor forms are polled pages, that is, the software automatically updates the information in the active Monitor form every 60 seconds. The polling interval (time between automatic refreshes) defaults to 60 seconds with a maximum of 24 hours.

Each Monitor form includes the following buttons:

- **Enable Polling**—Enables the automatic refresh of data in the Monitor form. The polling window is based on the specified poll timer.
- **Disable Polling**—Disables polling on any monitored form.
- **Change Poll Timer**—Allows you to change the polling interval for displaying statistical information. The button accesses a dialog box, from which you enter the desired poll interval. Available range is 60 seconds (default) to 86400 seconds (24 hours).
- **Refresh**—Updates the information displayed in the form.

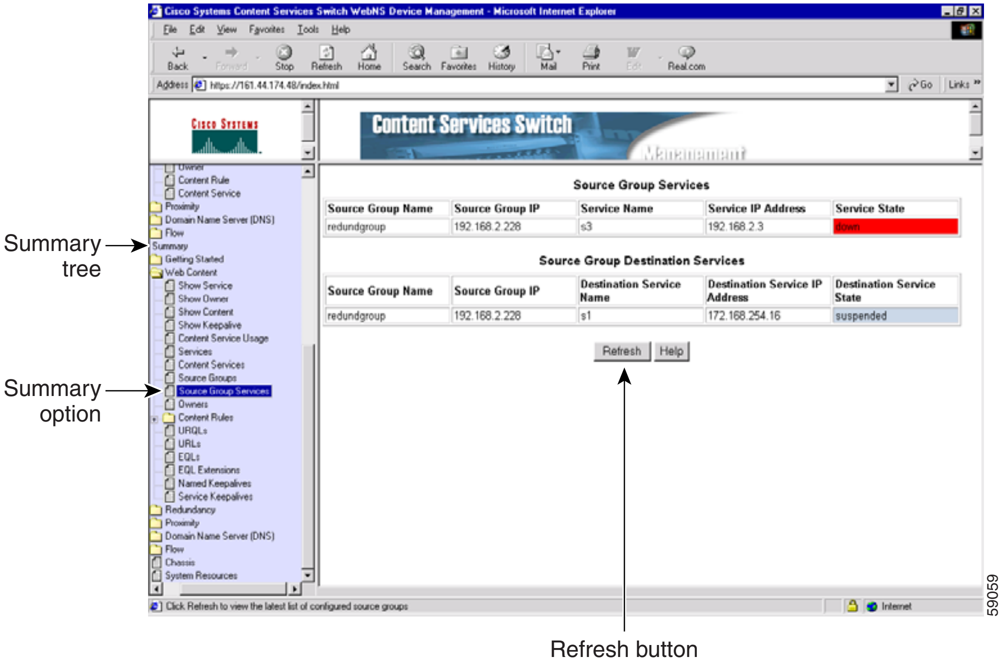
Using a Summary Form

There are a number of forms in the WebNS Device Management user interface that allow you to view configuration and statistical summary information about your CSS. Refer to Chapter 1, Using the Device Management User Interface, the "CSS Summary Form Features" section.

To use a Summary form:

1. Click the plus sign next to a folder in the Summary tree. The folder expands to display a list of functional areas in your CSS in which you can view summary information (Figure 3-7).

Figure 3-7 Summary Form Example



Cisco Systems Content Services Switch WebNS Device Management - Microsoft Internet Explorer

Address https://161.44.174.48/index.html

Source Group Services

Source Group Name	Source Group IP	Service Name	Service IP Address	Service State
redundgroup	192.168.2.228	s3	192.168.2.3	down

Source Group Destination Services

Source Group Name	Source Group IP	Destination Service Name	Destination Service IP Address	Destination Service State
redundgroup	192.168.2.228	s1	172.168.254.16	suspended

Click Refresh to view the latest list of configured source groups

2. Click **Refresh** to update the information displayed in the active Monitor form.

Using Online Help

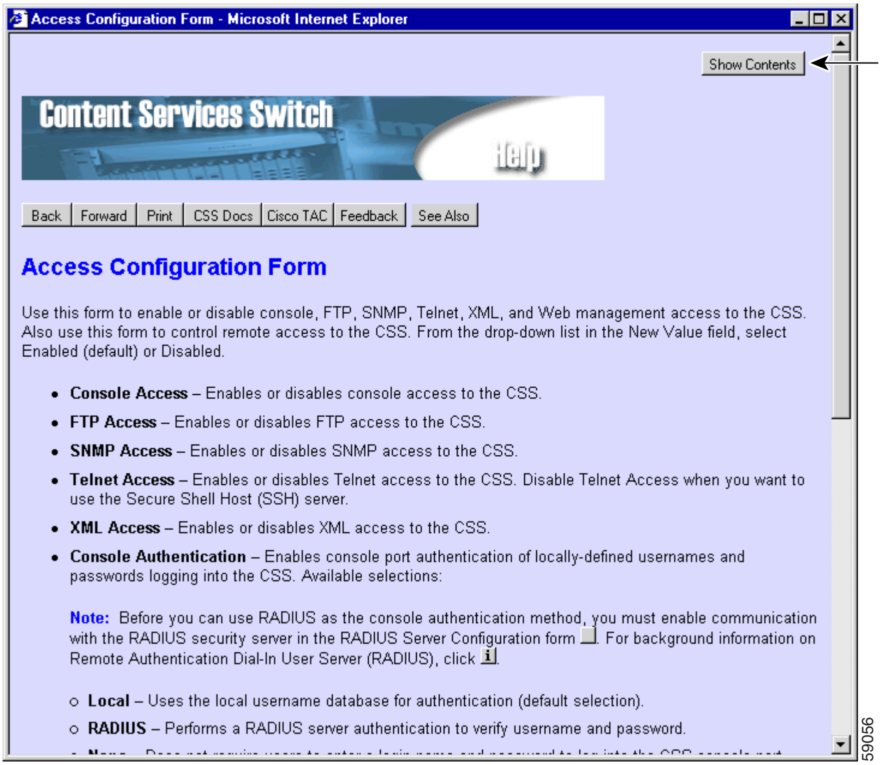
Each form in the WebNS Device Management user interface has a context-sensitive Online Help file associated with it. Each Online Help file contains information related to the form that you are using and also contains links to related topics. Online Help also includes a series of quick start procedures to assist you in navigating through the specific forms in the user interface and perform specific configuration procedures (for example, to configure a service or to configure a Client Side Accelerator).

Note For details on using the Online Help and its features, refer to the "Using WebNS Device Management User Interface Online Help" topic in the Help system.

To access Online Help:

1. In a form displayed in the workspace area, click the **Help** button at the bottom of the form (see Figure 3-7). The Online Help topic associated with the form displays in a separate browser window (Figure 3-8).

Figure 3-8 Online Help Topic Example



Access Configuration Form

Use this form to enable or disable console, FTP, SNMP, Telnet, XML, and Web management access to the CSS. Also use this form to control remote access to the CSS. From the drop-down list in the New Value field, select Enabled (default) or Disabled.

- **Console Access** – Enables or disables console access to the CSS.
- **FTP Access** – Enables or disables FTP access to the CSS.
- **SNMP Access** – Enables or disables SNMP access to the CSS.
- **Telnet Access** – Enables or disables Telnet access to the CSS. Disable Telnet Access when you want to use the Secure Shell Host (SSH) server.
- **XML Access** – Enables or disables XML access to the CSS.
- **Console Authentication** – Enables console port authentication of locally-defined usernames and passwords logging into the CSS. Available selections:

  Note: Before you can use RADIUS as the console authentication method, you must enable communication with the RADIUS security server in the RADIUS Server Configuration form. For background information on Remote Authentication Dial-In User Server (RADIUS), click.

  - **Local** – Uses the local username database for authentication (default selection).
  - **RADIUS** – Performs a RADIUS server authentication to verify username and password.

Show Contents/ Hide Contents button

2. Click the **Show Contents** button (in the upper right corner of the Online Help topic) to display the Contents, Index, and Search tabs, which allow you to access all the topics in the Help system. The name of this button changes to **Hide Contents** when the Contents, Index, and Search tabs appear.

   Note If you are using Internet Explorer to display the Contents, Index, and Search tabs, you must have Microsoft Virtual Machine installed on your computer. You can download Virtual Machine from www.microsoft.com.

3. To return to a previous Help topic, right-click the current topic, then select **Back** from the context menu.

Exiting from the Device Management User Interface

When you have finished configuring and monitoring your CSS with the Device Management user interface, exit from the software. This action clears the cache.

Troubleshooting

In addition to the information in this section, refer to the release notes that are included with your CSS for any additional caveats related to the WebNS Device Management user interface.

When establishing a Device Management session, if you experience a problem where your web browser fails to display the initial Device Management user interface screen, your Web browser may have failed to properly connect to the CSS. Verify that you have performed the following actions:

- Enabled Device Management. See the "Enabling the WebNS Device Management User Interface" section in Chapter 2, Configuring the CSS for Device Management.
- Specified a Simple Network Management Protocol (SNMP) community name to enable SNMP access to the WebNS Device Management user interface. See the "Configuring an SNMP Community" section in Chapter 2, Configuring the CSS for Device Management.
- Enabled cookies and JavaScript in your Web browser. See the "Configuring Your Browser" section in Chapter 2, Configuring the CSS for Device Management.
- Used the https:// designation when accessing the WebNS Device Management user interface URL (for example, https://161.16.2.3). If you do not use the proper URL designation, the Device Management user interface does not display and an error page appears.
- Ensured ACLs are not rejecting access to the management port IP address. To determine the status of configured ACLs, enter:

  ```
  # show acl config
  ```

  For information on ACLs, refer to the *Cisco Content Services Switch Security Configuration Guide.*

- Ran Device Management in a supported browser. For details, see Chapter 1, WebNS Device Management User Interface Overview, the "Browser and Platform Support" section.

Known Caveats with Netscape Communicator

The WebNS Device Management user interface may experience problems if you are using an unsupported version of Netscape Navigator or Communicator. Currently, the Device Management user interface supports the following versions of Netscape:

- Navigator 4.08
- Communicator 4.51 and 4.71

To download a supported Netscape browser, enter the following URL in your browser:

`http://www.netscape.com/`

Known Caveats with Microsoft Internet Explorer

With Microsoft Internet Explorer 6.0, whenh a Device Management opage is displayed and you highlight the page in the Address field and press Enter, an Internet Explorer expired page appears. To redisplay the Device Management page, click **Refresh** in the browser navigation bar, then click **Retry** in the message box that appears.

INDEX