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.

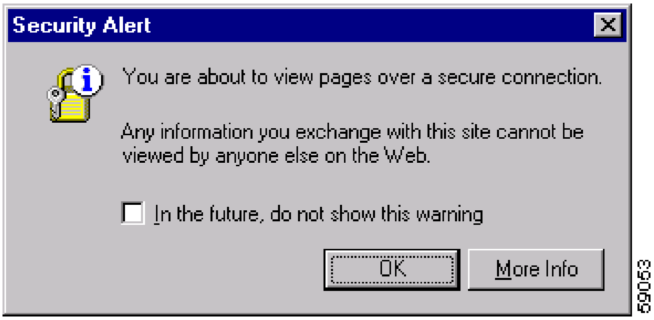
   For example:

   ```
   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



Security Alert

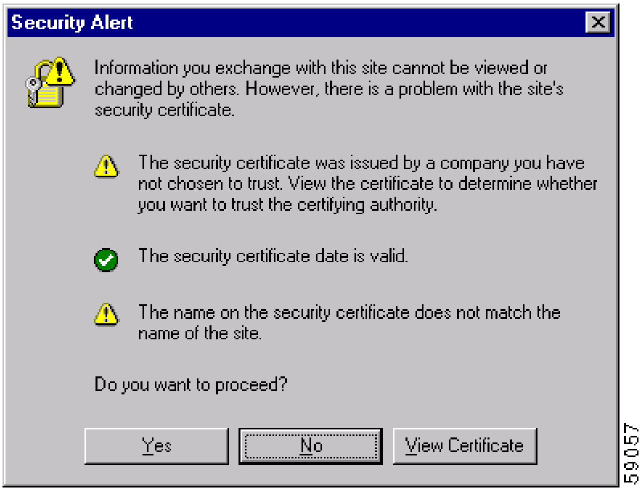
You are about to view pages over a secure connection.

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.

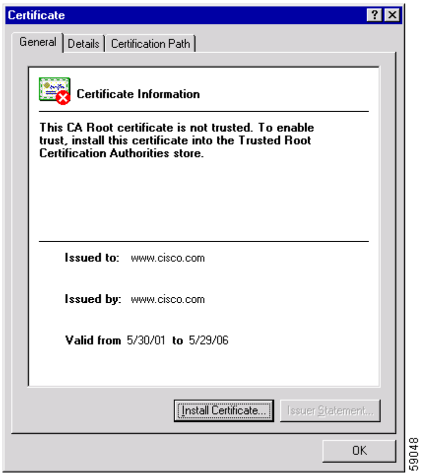
The security certificate date is valid.

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.

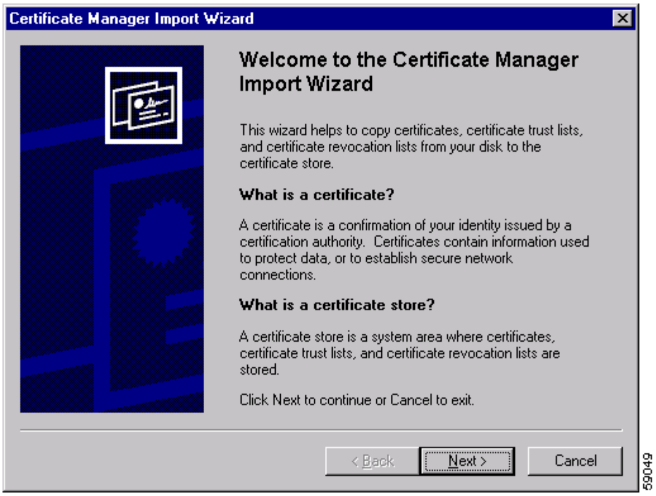
Issued to: www.cisco.com

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.

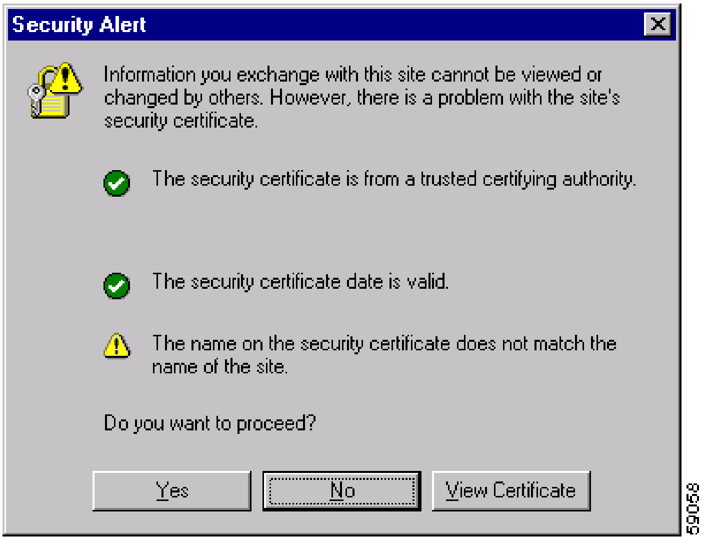
Click Next to continue or Cancel to exit.

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.

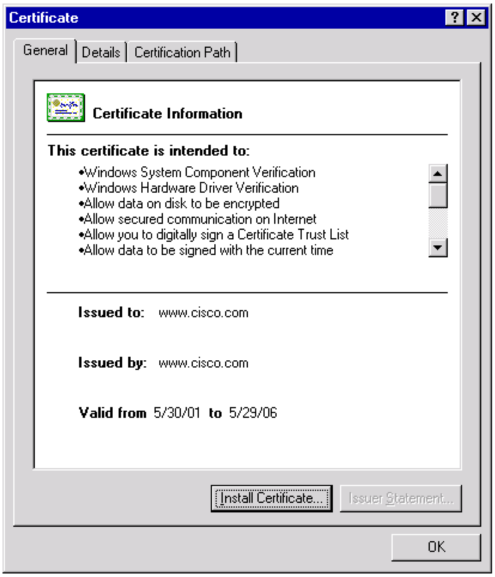
✓ The security certificate date is valid.

⚠ 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

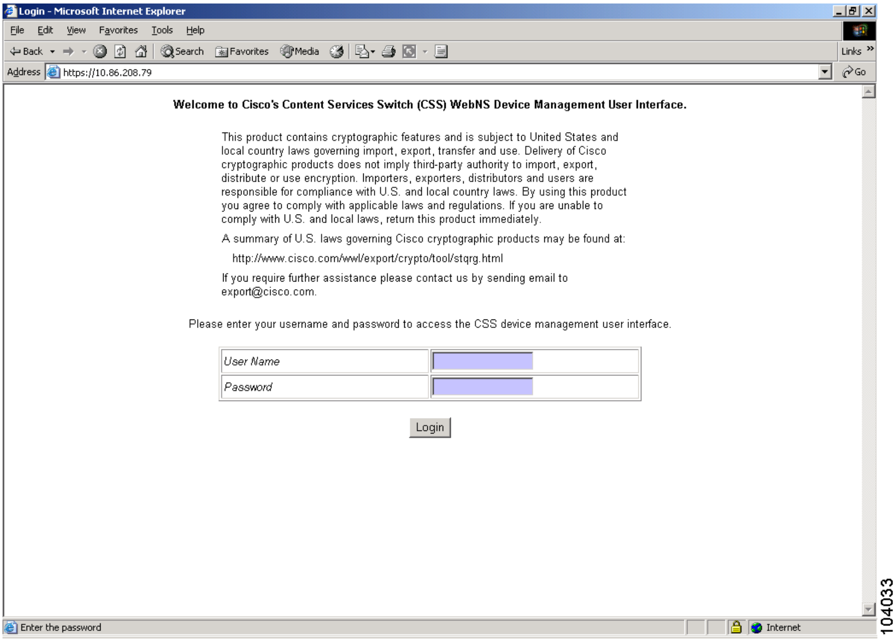
Issued by: www.cisco.com

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