Cisco CNS Configuration Engine 1.4 Administrator Guide

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-1791-03

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco CNS Configuration Engine 1.4 Administrator Guide

CONTENTS

Preface

This document describes how to install and configure the software for the Cisco CNS Configuration Engine 1.4 on the Cisco CNS 2100 Series Intelligence Engine. It also contains information about how to administer the various network management features available with this product.

Note This product contains cryptographic features and is subject to US and local laws governing import, export, transfer, and use.

Audience

This guide is intended primarily for:

- System administrators familiar with installing high-end networking equipment
- System administrators responsible for installing and configuring internetworking equipment who are familiar with Cisco IOS software

Conventions

This guide uses basic conventions to represent text and table information.

- Commands that you enter are in **boldface** font.
- Variables for which you supply values are in *italic* font.
- Terminal sessions and information the system displays are printed in `screen` font.
- Information you enter is in **`boldface screen`** font. Variables you enter are printed in *`italic screen`* font.
- Button names are in **boldface** font.

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

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Related Documentation

Other documentation related to this product include:

- *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*
- *Release Notes for Cisco CNS Configuration Engine 1.4*
- *Regulatory Compliance and Safety Information For Cisco Intelligence Engine 2100 Series*
- *Cisco CNS 2100 Series Intelligence Engine Installation Guide*
- *Release Notes For Cisco CNS 2100 Series Intelligence Engine*
- *Cisco CNS 2100 Series Intelligence Engine Machine Code License*
- *Cisco CNS SDK 1.5.4 API Reference and Programmer Guide*

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

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 Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- 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 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

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

- 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 online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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

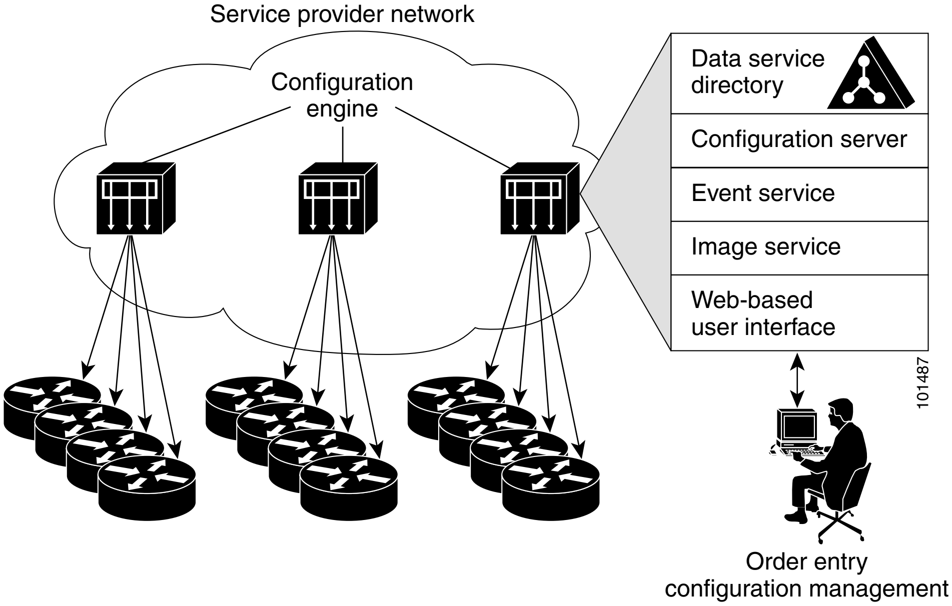
Product Overview

This chapter provides a high-level overview of the Cisco CNS Configuration Engine 1.4. It is organized as follows:

- Cisco IOS Dependences
- Modes of Operation
- CNS Configuration Service
- CNS Event Service
- CNS Image Service
- PIX Firewall Support
- Intelligent Modular Gateway
- IMGW Device Module Toolkit
- Modular Router Support
- Data Administration Tool
- Encryption
- How the Cisco CNS Configuration Engine 1.4 Works
- Dynamic ConfigID and EventID Change Synchronization
- Network Management Tools

The Cisco CNS Configuration Engine 1.4 is a network management application that acts as a configuration service for automating the deployment and management of network devices and services (see Figure 1-1). The Cisco CNS Configuration Engine 1.4 runs on the Cisco CNS 2100 Series Intelligence Engine (CNS 2100 Series system) hardware platform.

Figure 1-1 Cisco CNS Configuration Engine 1.4 Architectural Overview



Each Cisco CNS Configuration Engine 1.4 manages a group of Cisco devices and services they deliver, storing their configurations and delivering them as needed. The Cisco CNS Configuration Engine 1.4 automates initial configurations and configuration updates by generating device-specific configuration changes, sends them to the device, executes the configuration change, and logs the results.

Note If you are running devices that use an earlier version of Cisco IOS, or a different operating system, such as Catalyst, you should invoke the Intelligent Modular Gateway for communicating with the device. For more information about Intelligent Modular Gateway, see "Intelligent Modular Gateway" section on page 1-10.

The Cisco CNS Configuration Engine 1.4 utilizes the following popular industry standards and technologies:

- eXtensible Markup Language (XML)
- Java naming directory interface (JNDI)
- Hypertext Transport Protocol (HTTP)
- Java servlets
- Lightweight Directory Access Protocol (LDAP)

The Cisco CNS Configuration Engine 1.4 supports two modes of operation (Internal Directory and External Directory) and it includes the following Cisco CNS components:

- Configuration service (web server, file manager, and namespace mapping server)
- Image Service (Cisco IOS images)
- Event service (event gateway)
- Data service directory (data models and schema)
- Intelligent Modular Gateway (IMGW)

The Cisco CNS Configuration Engine 1.4 can be used as the runtime component for deployment of customer-developed applications. These applications can be developed using the Cisco CNS SDK 1.5.4.

Cisco IOS Dependences

Table 1-1 lists Cisco IOS versions with corresponding versions of CNS Configuration Engine including feature limitations associated with each version.

Table 1-1 CNS Configuration Engine and Cisco IOS Dependencies

Cisco IOS	CNS Configuration Engine	Limitations
12.3	1.3.2 or later	
12.2(11)T	1.2 or later	
12.2(2)T	1.2 or later with no authentication.	Applications will be unable to use exec commands or point-to-point messaging.

Modes of Operation

There are two modes of system operation for the Cisco CNS Configuration Engine 1.4:

- Internal Directory Mode
- External Directory Mode

Internal Directory Mode

In Internal Directory mode, the Cisco CNS Configuration Engine 1.4 supports an embedded CNS Directory Service. In this mode, no external directory or other data store is required. To store device configuration information, the Cisco CNS Configuration Engine 1.4 uses the CNS data models implemented as an extended X.500 directory schema in the CNS Directory Service.

External Directory Mode

In External Directory mode, the Cisco CNS Configuration Engine 1.4 supports the use of a user-defined external directory. In this mode, the Cisco CNS Configuration Engine 1.4 supports the following directory services:

- Novell Directory Services
- Critical Path
- iPlanet

CNS Configuration Service

The CNS Configuration Service is the core component of the Cisco CNS Configuration Engine 1.4. It consists of a configuration server that works in conjunction with configuration agents located at each router. The CNS Configuration Service delivers device and service configurations to Cisco IOS devices for initial configuration and mass reconfiguration by logical groups. Routers receive their initial configuration from the CNS Configuration Service when they start up on the network the first time.

The CNS Configuration Service uses the CNS Event Service to send and receive events required to apply configuration changes and send success and failure notifications.

The configuration server consists of a web server that uses configuration templates and the device-specific configuration information stored in the embedded (Internal Directory mode) or remote (External Directory mode) directory.

Configuration templates are text files containing static configuration information in the form of command-line interface (CLI) commands. In the templates, variables are specified using lightweight directory access protocol (LDAP) URLs that reference the device-specific configuration information stored in a directory.

The configuration template includes additional features that allow simple conditional control structures and modular sub-templates in the configuration template (see the “Templates and Template Management” section on page 2-57).

The configuration server uses Hypertext Transport Protocol (HTTP) to communicate with the CNS Configuration Agent running on the managed Cisco IOS device. The configuration server transfers data in eXtensible Markup Language (XML) format. The configuration agent in the router uses its own XML parser to interpret the configuration data and remove the XML tags from the received configuration.

The configuration agent can also perform a syntax check on received configuration files. The configuration agent can also publish events through the event gateway to indicate the success or failure of the syntax check.

The configuration agent can either apply configurations immediately or delay the application until receipt of a synchronization event from the configuration server.

CNS Event Service

The Cisco CNS Configuration Engine 1.4 uses the CNS Event Service for receipt and generation of events. The CNS Event Agent resides on Cisco IOS devices and facilitates communication between routers and the event gateway on the Cisco CNS Configuration Engine 1.4.

The CNS Event Service is a highly-scalable publish and subscribe communication method. The CNS Event Service uses subject-based addressing to help messages reach their destination. Subject-based addressing conventions define a simple, uniform namespace for messages and their destinations.

New Event Subject Names

The base element of the CNS event subject namespace has been changed from *cisco.cns.** to *cisco.mgmt.cns.** in support of Cisco IOS 12.3.

The CNS event subject namespace has been modified in accordance with the new Cisco subject naming conventions. In order to keep up with the new subject naming convention, CNS agents in Cisco IOS have been modified and released with the 12.3 Cisco IOS train. The change affects the subject names that the CNS agents subscribe to and publish on.

This section lists the new event subject names that are associated with Cisco IOS 12.3.

CNS Event Agent

cisco.mgmt.cns.event.boot

cisco.mgmt.cns.event.id-changed

CNS Image Agent

cisco.mgmt.cns.image.* – Events related to the image distribution agent

cisco.mgmt.cns.image.checkServer

cisco.mgmt.cns.image.inventoryRequest

cisco.mgmt.cns.image.upgradeRequest

cisco.mgmt.cns.image.status

CNS Exec Agent

cisco.mgmt.cns.exec.* – Events related to exec command-like functions.

cisco.mgmt.cns.exec.cmd

cisco.mgmt.cns.exec.rsp

cisco.mgmt.cns.exec.reload

CNS Config Agent

cisco.mgmt.cns.config.complete

cisco.mgmt.cns.config.failure

cisco.mgmt.cns.config.warning

cisco.mgmt.cns.config.sync-status

cisco.mgmt.cns.config.reboot – deprecated. Use cisco.mgmt.cns.exec.reload instead.
cisco.mgmt.cns.config.load

cisco.mgmt.cns.config.id-changed

cisco.mgmt.cns.config-changed

cisco.mgmt.cns.config-changed.lost

CNS Inventory Agent

cisco.mgmt.cns.inventory.get

cisco.mgmt.cns.inventory.device-details

cisco.mgmt.cns.inventory.oir

CNS Syslog Agent

cisco.mgmt.cns.log.emerg

cisco.mgmt.cns.log.alert

cisco.mgmt.cns.log.crit

cisco.mgmt.cns.log.err

cisco.mgmt.cns.log.warning

cisco.mgmt.cns.log.notice

cisco.mgmt.cns.log.info

cisco.mgmt.cns.log.debug

CNS MIB Access Agent

cisco.mgmt.cns.mibaccess.request

cisco.mgmt.cns.mibaccess.response

cisco.mgmt.cns.mibaccess.notification

cisco.mgmt.cns.snmp.rqst

cisco.mgmt.cns.snmp.resp

cisco.mgmt.cns.snmp.trap

CNS Event Gateway

cisco.mgmt.cns.device.connect

cisco.mgmt.cns.device.disconnect

For IMGW Device Module Development Toolkit

This section lists the new event subject names that are associated the IMGW Device Module Development Toolkit.

cisco.mgmt.cns.imgw.devicemodule.request.register

cisco.mgmt.cns.imgw.devicemodule.request.deregister

cisco.mgmt.cns.imgw.devicemodule.response.register

cisco.mgmt.cns.imgw.devicemodule.response.deregister

Legacy Subject Names

The following is a list of all the subject names in use in Cisco IOS releases prior to 12.3, and CNS Configuration Engine release 1.3.2. Starting with release 12.3 of Cisco IOS and release 1.3.2 of the CNS Configuration Engine, the prefix for all of the subjects listed below will be modified from *cisco.cns* to *cisco.mgmt.cns*.

Here is the list of subjects names in use prior to IOS 12.3:

cisco.cns.config.complete

cisco.cns.config.failure

cisco.cns.config.warning

cisco.cns.config.sync-status

cisco.cns.config.reboot

cisco.cns.config.load

cisco.cns.config.id-changed

cisco.cns.exec.cmd

cisco.cns.exec.rsp

cisco.cns.inventory.get

cisco.cns.inventory.device-details

cisco.cns.inventory.oir

cisco.cns.config-changed

cisco.cns.config-changed.lost

cisco.cns.event.boot

cisco.cns.event.id-changed

SYSLOG

cisco.cns.log.emerg

cisco.cns.log.alert

cisco.cns.log.crit

cisco.cns.log.err

cisco.cns.log.warning

cisco.cns.log.notice

cisco.cns.log.info

cisco.cns.log.debug

SAA

cisco.cns.slm

cisco.cns.customtrap

MIB Access

cisco.cns.mibaccess.request

cisco.cns.mibaccess.response

cisco.cns.mibaccess.notification

cisco.cns.snmp.rqst

cisco.cns.snmp.resp

cisco.cns.snmp.trap

CNS Event Gateway

cisco.cns.device.connect

cisco.cns.device.disconnect

NameSpace Mapper

The CNS Namespace Mapping Service (NSM) allows you to address multiple network devices by a single posting of a publish or subscribe event, and it allows your network administrator to map Cisco-standardized event names to names of his or her choosing.

For example, in a network of 100 routers, there may be 10 which the administrator wants to configure as a VPN (Virtual Private Network). In order to load a configuration into each of these devices, your client application could either publish 10 *cisco.mgmt.cns.config.load* events, or the administrator could associate the 10 devices with a common group name and your client application can post the event once. The administrator could rename the *cisco.*mgmt.*cns.mgmt.config.load* subject to *application.load* and group all the devices in the West Coast under a group called “westcoast.” Then the application would just have to publish on *application.load.westcoast* and the devices in the “westcoast” group would get the event.

NSM Modes

The NameSpace Mappers can operate in one of two NSM modes:

- Default
- Provider

The NSM mode is set when you run the **Setup** program (refer to the *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*).

Default Mode

No directory setup is required for Default mode. In this mode, subject mappings are specified in a configuration file. The subject map can be tailored to suit the namespace that the application is using.

To set Default mode, use **default** for the value of the NSM Directive parameter in the **Setup** program (refer to the *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*).

Provider Mode

Directory setup is required for Provider mode. NSM looks up the directory for subject mappings for a device. This mode allows you to address a group of devices in one event.

To set Provider mode, use **http** for the value of the NSM Directive parameter in the **Setup** program.

More information about NSM can be found in the *CNS SDK 1.5.4 API Reference and Programmer Guide*.

Directory setup can be done using the Directory Administration Tool (see “Directory Administration Tool” section on page 4-1.

Event Gateway

The CNS Event Gateway acts as a relay between the CNS Integration Bus and CNS agent-enabled devices, which enables event-based communication.

The CNS Event Gateway uses NSM to map subjects. The mode of operation is determined by the value set for the NSM Directive parameter during **Setup** (refer to the *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*).

Note This mode must match the mode that your application is using for NSM.

If you choose the Provider mode (**http**), the Event Gateway must be given a parameter that indicates which application namespace must be used for subject mapping. The Cisco CNS Configuration Engine 1.4 prompts for this parameters value during **Setup** with the message:

```
Enter NSM directive (default, http):
```

The default value for this parameter is **default**. However, during **Setup**, you can override this value with one of your own.

Each Event Gateway process can support up to a maximum of 500 devices. To support more than 500 devices, you can run multiple gateway processes. During **Setup**, you can set the number of concurrent gateway processes to start with either one or both of the following prompts, depending on how you want to setup your SSL (see “Encryption” section on page 1-13) communications:

```
Enter number of Event Gateways that will be started with crypto operation:
Enter number of Event Gateways that will be started with plaintext operation:
```

Dynamic Template and Object

The original servlet, *com.cisco.cns.config.Config*, gets the configuration template from the attribute value of the Device Object in the configuration server data store (LDAP server), parses the template, and does string substitution on parameters inside the template. It is tightly coupled with the template that is assigned to the device and the attributes of device object.

The new servlet, **DynaConfig**, loosens the restriction so that the template can be assigned dynamically and the parameter values can be obtained from other objects in data store.

This servlet gets **PathInfo** information by means of **HttpServletRequest.getPathInfo()**, parse it, and gets the related template name and object reference. The structure of **PathInfo** is:

/<*argument name*>=<*argument value*>.

Data Structures

The feature of dynamic template and object utilizes **PathInfo**, which is passed from the client side to the servlets. The structure of **PathInfo**, which the servlet can understand is in following format:

```
[/<argument name>=<value>]*
```

The argument and format for dynamic template and object is:

```
[/cfgtpl=value[/object=value]]
```

For more information about Dynamic Template and Object, refer to the *Cisco CNS SDK 1.5.4 API Reference and Programmer Guide.*

CNS Image Service

The CNS Image Service is an automated, scalable, and secure mechanism designed to distribute Cisco IOS images and related software updates to Cisco IOS devices that have Cisco Intelligence Agents (CIAs).

For more information about how to use the CNS Image Service, see “CNS Image Service” section on page 2-75.

For those devices that do not have a CIA, non-Cisco IOS devices, and non-Cisco devices, you can use the IMGW Toolkit to create scripts that support SSH sessions between these devices and the CNS Configuration Engine 1.4.

For more information about the IMGW Device Module Toolkit, see Chapter 6, “IMGW Device Module Development Toolkit.”

PIX Firewall Support

Cisco CNS Configuration Engine 1.4 provides configuration management and image service to Cisco PIX firewall devices (PIX device).

For more information about PIX firewall support, see Chapter 5, "Cisco PIX Firewall Device Support."

Intelligent Modular Gateway

Intelligent Modular Gateway (IMGW) allows you to run the Cisco CNS Configuration Engine 1.4 for automatically distributing configuration files to Cisco IOS network devices running Cisco IOS versions earlier than 12.2(2)T; as well as to Catalyst switches, CCS 11k devices, Cache Engines, and PIX firewalls.

Note If you are running devices that use Cisco IOS version 12.2(2)T or later, you should use the CNS Event Gateway.

The Intelligent Modular Gateway accomplishes this task by adding the ability to use alternate access methods to connect to devices that do not have CNS agents in their software. Currently, the access method is SSH.

The interface to the Intelligent Modular Gateway is the same as that of the CNS Event Gateway. It responds to the same events. The NameSpace Mapper operates in the same way. Therefore, once some initial setup work is done, applications need not know the difference between communicating with agent-enabled devices by way of the Event Gateway and non-agent devices by way of the Intelligent Modular Gateway.

Restrictions

Using the Intelligent Modular Gateway with an SSH transport creates some restrictions in terms of how the Cisco CNS Configuration Engine 1.4 architecture is used.

- When using SSH as a transport, no syntax checking can be done on the configurations before they are applied.

  Syntax checking in the Cisco CNS Configuration Engine 1.4 architecture is accomplished by an intelligent agent in the device that has access to internal parser functions. An SSH interface does not provide any means to access this functionality. Therefore, any syntax checking attributes are ignored. Errors are only detected when the configuration is actually applied and applications must deal with the fact that configuration lines prior to the error were executed.

- Because all logic is external to the device, there is no way to watch for configuration changes that are done outside the scope of the network management software.

  For example, if a network administrator uses a standard SSH client to directly access a network element and changes the configuration, that element would not be synchronized with the network management infrastructure, and depending on the change, might become unmanageable. This is especially true if the login mechanisms (usernames and passwords) are changed. Login mechanism changes should be handled during a maintenance window, during which event-based configuration is not occurring, so that race conditions do not occur. Any such changes must be reflected on the provisioning system's device information screen so that the Device Information Database is properly updated before any new partial configurations are sent.

- The scope of error checking upon configuration load is limited to syntax checking.

  Semantic errors cannot be detected. The output is returned in a buffer that applications should log. In a case where something is not operating properly, a network administrator can manually look at the log of what the device was reporting and determine if a semantic error occurred.

- The initial configuration mechanism as defined in the Cisco CNS Configuration Engine 1.4 architecture is not supported.

  This mechanism allows a router to be preconfigured with the **cns config initial** command, causing it to contact the configuration server to retrieve its initial configuration. However, because the legacy devices do not have the agent code in them, they can never contact the configuration server (they do not understand the configuration command). Therefore, this mechanism does not make sense when using SSH as a transport. If an initial configuration needs to be delivered by the Cisco CNS Configuration Engine 1.4, it has to be done through the partial configuration mechanism.

- Aside from the device information database, the gateway is stateless.

  There is no read back of configurations to make sure they were applied, nor is there automatic rollback of configurations if a failure occurs.

- If a device is not directly connected to the management network, it must be attached through a Cisco communication servers.

  The API allows you to set up an arbitrary network topology to reach the device. However, this release only supports two possible topologies: direct connection to one of the device network interfaces, or console access by way of a Cisco access server, such as a 2511.

- Device failures are only detected within a user-specified polling interval.

  This is because while the standard Event Gateway requires that routers maintain a connection to the Event Gateway (so any breakage of that connection would signal a problem), the SSH interface is implemented through a transient connection. Therefore, the gateway must poll all devices at some user-specified interval to make sure they are responding, so failure detection is not immediate.

- When both agent-enabled and legacy devices are present on the same network, it is recommended that both gateways be run at the same time.

  The standard (CNS) Event Gateway talks to the agent-enabled devices and the Intelligent Modular Gateway talks to the legacy devices.

Note Do not put an entry in the Device Information Database for a router that is already agent-enabled because both gateways will try to control the router and unpredictable results may occur.

IMGW Device Module Toolkit

IMGW Device Module Toolkit allows you to develop your own device modules, plug them into Cisco CNS Configuration Engine 1.4, then use them to configure devices.

For more information about the IMGW Device Module Toolkit, see Chapter 6, “IMGW Device Module Development Toolkit” and Appendix B, “How to Use the IMGW Device Module Development Toolkit.”

Modular Router Support

Cisco CNS Configuration Engine 1.4 supports modular routers. A modular router chassis includes slots in which you can install line and network interface cards. For example, the Cisco 3660 (see Figure 1-2) has six network module slots. You can install any module into any available slot in the chassis. Some modules like 2 Ethernet 2 WAN card slot module can in turn have sub slots to install network interface cards or line cards (see Figure 1-3 on page 1-12). Device management supports subdevices representing these line and network cards.

Figure 1-2 Cisco 3660 Modular Router

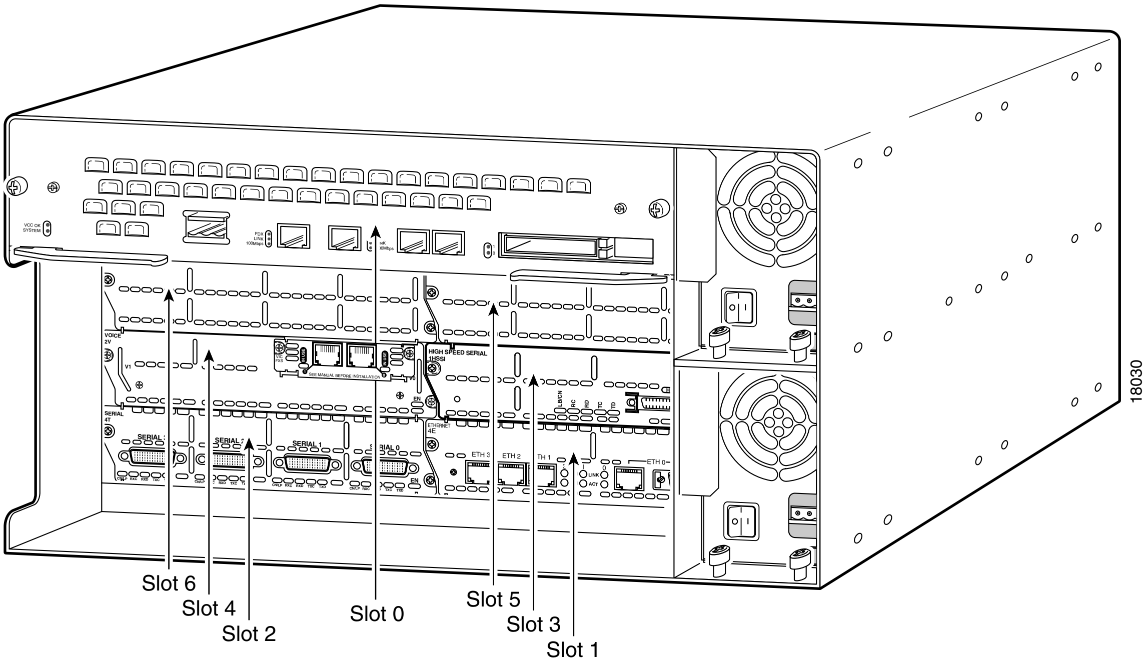
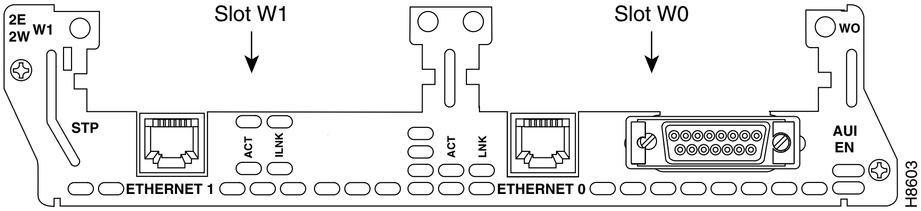


Figure 1-3 Interface or Line Card Slots



Additional attributes representing line card type and subdevices have been added to the existing device object structure in the directory server in order to have the same structure to represent the main device or the subdevice.

For a modular router, a subdevice configuration object and configuration template is defined for every network module whose interfaces need to be configured and for which the interface number can be variable; based on the slot. Then, a device configuration object and a template is defined for the main device. Fixed interface numbers can be configured in the main device template.

Modular router events are published to the event bus and are accessible to applications connected to the bus. The Cisco IOS device publishes the system hardware configuration in the *cisco.mgmt.cns.config.device-details* event after hardware discovery. The Cisco CNS Configuration Engine 1.4 is configured to listen for this event, retrieve it and extract the hardware configuration of the device.

In Internal Directory mode, modular router support sessions work with NSM in both modes (see "NSM Modes" section on page 1-8).

Data Administration Tool

The Data Administration Tool (DAT) presents you with a web-based user interface that allows you to populate and manage the data in the directories. You can View/Add/Delete/Update devices (CNS agent-enabled devices, see "Intelligent Modular Gateway" section on page 1-10), groups of devices, and applications in the directory. Also, you can View/Add/Delete/Update events specific to each application.

DAT also provides you with the additional capability of bulk data upload.

Note You cannot change (extend) the schema using DAT. You have to populate the schema manually in the directory server.

For information about how to use DAT, see "Directory Administration Tool" section on page 4-1.

Encryption

Secure Socket Layer (SSL) method has been adopted as the encryption mechanism for HTTP sessions between the configuration agent and the configuration server, and the TCP session between the CNS Event Gateway and the event agent.

To use encryption, the Cisco IOS devices must be running a crypto image and version 12.2(11)T of the Cisco IOS.

Device Authentication

The configuration server and CNS Event Gateway are supplied with a X.509 certificate generated by a certificate authority (CA) server. It is the responsibility of the network administrator to have a CA server and to control certificate generation and revocation.

The Cisco IOS device must—to be configured—be recognize by the CA. There is no client-side certificate in the Cisco IOS device.

For the configuration server, once the Cisco IOS device has validated the certificate, it sends **cns_id:cns_password** over the encrypted pipe. The device uses a CNS password to be authenticated by the Cisco CNS Configuration Engine 1.4.

Note Authentication is also done when the links are in clear text.

A server configured for secure connections is also able to enact non-secure (clear-text) sessions. The password check is done regardless of whether encryption is used or not.

Once the server is secured, it is no longer be able to process requests that do not have a password. It cannot tell the difference between a clear-text request from a device in a secure environment from a device in an non-secure environment.

For the CNS Event Gateway, once the Cisco IOS device has validated the certificate, it sends a DeviceID control message over the encrypted pipe that has the CNS password of the device. The **event_id:cns_password** is validated using the authentication API. If it is not matched, the SSL session is terminated and an entry made to the security log. This ensures only authorized customer premises equipment (CPE) devices connect to the CNS Event Gateway and are able to use the CNS Integration Bus.

Bootstrap Password

Cisco CNS Configuration Engine 1.4 provides a bootstrap password for use where multiple devices are deployed in a batch. In this case, all devices in a particular batch are given the same (bootstrap) password to use when they each start up on the network for the first time.

The bootstrap password can be changed for different batches of devices by using the **BootStrap** function under Security Manager in the user interface (see “Security Manager” section on page 2-69).

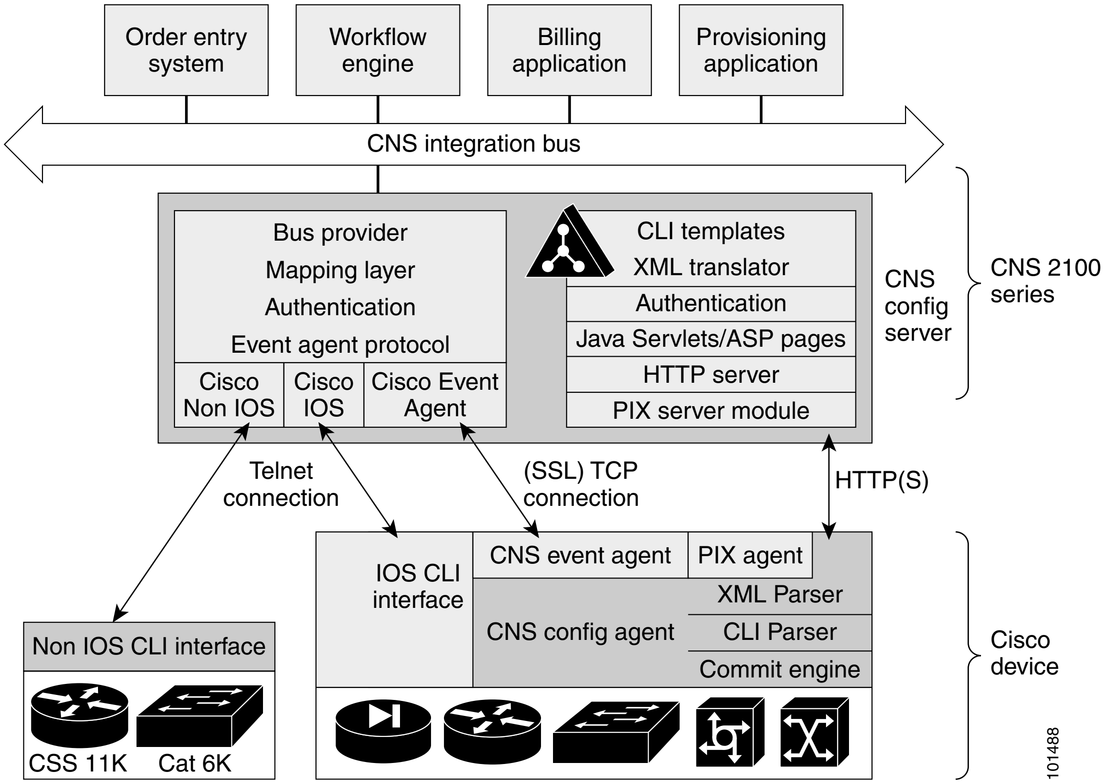
Resynchronize cns_password

If the cns_password of a device becomes corrupted so that there is a mismatch between the device and the corresponding password information help in the CNS Configuration Engine 1.4 directory, you can resynchronize the device with the CNS Configuration Engine 1.4 by using the **Resync Device** function in the user interface (see “How to Resynchronize a Device” section on page 2-19)

How the Cisco CNS Configuration Engine 1.4 Works

The Cisco CNS Configuration Engine 1.4 dynamically generates Cisco IOS configuration files (documents), packages these file in XML format, and distributes them by means of Web/HTTP (see Figure 1-4 on page 1-15). This takes place in response to a *pull* (get) operation.

Figure 1-4 Configuration Engine Functional Diagram

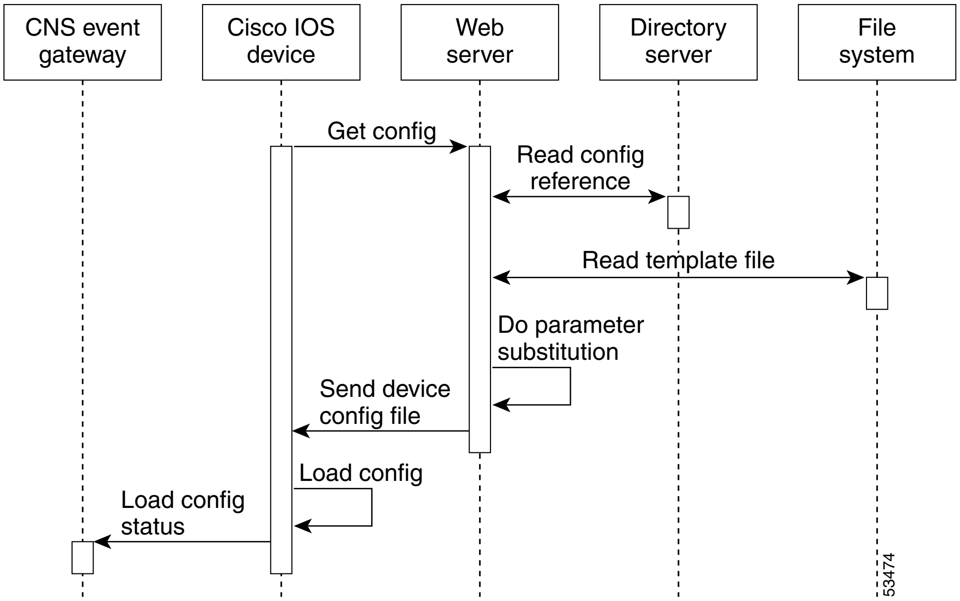


A Cisco IOS device initiates a get operation when it first appears on the network (**cns config init…**) or when notified (by subscribed event) of a configuration update (**cns config partial…**).

Note For more information about these and other related CLI commands, refer to the Cisco IOS configuration guide and command reference publications.

When a Cisco IOS device issues a request for a device configuration file, the request includes a unique identifier (configID = hostname) used to help locate the relevant configuration file parameters for this device on the directory server. Figure 1-5 shows the process flow for a configuration load operation.

Figure 1-5 Configuration Load Process Flow



When the web server receives a request for a configuration file, it invokes the Java Servlet and executes the embedded code. This directs the web server to access the directory server and file system to read the configuration reference for this device and template. The configuration server prepares an instantiated configuration file by substituting all the parameter values specified in the template with valid values for this device. The configuration server forwards the configuration file to the web server for transmission to the Cisco IOS device.

The configuration agent at the router accepts the configuration file from the web server, performs XML parsing, syntax checking (optional), and loads the configuration file. The router reports the status of the configuration load as an event that can be subscribed to by a network monitoring or workflow application.

Load Initial Configuration

1. The Cisco CNS Configuration Engine 1.4 reads the template files.
2. The Cisco CNS Configuration Engine 1.4 does the parameter substitution.
3. The Cisco CNS Configuration Engine 1.4 sends the device configuration to the Cisco IOS device.
4. The Cisco IOS device tries to load the initial configuration.
5. The Cisco IOS device publishes the load configuration status event to the event gateway.

Modular Router

1. The modular router posts an HTTP request containing the hardware configuration to the Cisco CNS Configuration Engine 1.4 for the initial configuration.
2. The Cisco CNS Configuration Engine 1.4 reads the hardware configuration of the device from the HTTP request and updates the directory server with the latest configuration.
3. The Cisco CNS Configuration Engine 1.4 reads the template files.
4. The Cisco CNS Configuration Engine 1.4 does the parameter substitution.

5. The Cisco CNS Configuration Engine 1.4 sends the device configuration to the Cisco IOS device.
6. The modular router tries to load the initial configuration.
7. The modular router publishes the load configuration status event to the event gateway.

Load Partial Configuration

1. The user modifies a template in the Cisco CNS Configuration Engine 1.4 user interface.
2. The template contents are passed to the Cisco CNS Configuration Engine 1.4.
3. The Cisco CNS Configuration Engine 1.4 stores the template in the file system.
4. The user clicks the update device button in the user interface.
5. The Cisco CNS Configuration Engine 1.4 publishes a *cisco.mgmt.cns.config.load* event.
6. The Cisco IOS device retrieves the *cisco.mgmt.cns.config.load* event and in response to this event requests its configuration by contacting the server.
7. The Cisco CNS Configuration Engine 1.4 reads the template files.
8. The Cisco CNS Configuration Engine 1.4 does the parameter substitution.
9. The Cisco CNS Configuration Engine 1.4 sends the device configuration to the Cisco IOS device.
10. The Cisco IOS device tries to load the partial configuration.
11. The Cisco IOS device publishes the load configuration status event to the event gateway.

Modular Router

1. The user modifies a template in the Cisco CNS Configuration Engine 1.4 user interface.
2. The template contents are passed to the Cisco CNS Configuration Engine 1.4.
3. The Cisco CNS Configuration Engine 1.4 stores the template in the file system.
4. The user clicks the update device button in the user interface.
5. The Cisco CNS Configuration Engine 1.4 publishes a *cisco.mgmt.cns.config.load* event.
6. The modular router retrieves the *cisco.mgmt.cns.config.load* event and in response to this event requests its configuration by contacting the server.
7. The Cisco IOS device posts a HTTP request containing the hardware configuration to the Cisco CNS Configuration Engine 1.4 for the partial configuration.
8. The Cisco CNS Configuration Engine 1.4 reads the template files.
9. The Cisco CNS Configuration Engine 1.4 does the parameter substitution.
10. The Cisco CNS Configuration Engine 1.4 sends the device configuration to the modular router.
11. The modular router tries to load the partial configuration.
12. The modular router publishes the load configuration status event to the event gateway.

How EventID, and ConfigID are Used

The Cisco CNS Configuration Engine 1.4 intersects two name space domains:

- Configuration Domain
- Event Domain

The CNS Configuration Engine 1.4 uses the Configuration Domain when a device communicates with the configuration server. It uses the Event Domain when a device communicates with the Cisco CNS Configuration Engine 1.4 using the publish and subscribe mechanism of the CNS Integration Bus.

The device must be uniquely identified in these namespaces. The ConfigID uniquely identifies the device in the Configuration Domain. The EventID uniquely identifies the device in the Event Domain.

Because the Cisco CNS Configuration Engine 1.4 uses both the CNS Integration Bus (event bus) and the configuration server to provide configurations to devices, both EventID and ConfigID must be defined for each configured Cisco IOS device.

The values for EventID and ConfigID for each device can be identical, or you can make them different when you add or edit device information using the user interface (see “Managing Devices” section on page 2-7).

Dynamic ConfigID and EventID Change Synchronization

The Cisco IOS, version 12.2.(11)T, was enhanced with new CLI ID commands that can modify the EventID and ConfigID, then reconnect the device to the Cisco CNS Configuration Engine 1.4 with the new IDs.

Network Management Tools

The CNS 2100 Series platform includes the Tivoli Management Agent (TMA). The Tivoli Product(s) is copyrighted and licensed (not sold) and therefore not transferred.

The owner of the Tivoli Product DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE USE OF THE TIVOLI PRODUCT(S) INCLUDING (WITHOUT LIMITATION) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

To initialize the Tivoli Management Agent, refer to the *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*.

CHAPTER 2

Administration Tasks for Internal Directory Mode

This chapter describes the Cisco CNS Configuration Engine 1.4 administration tasks for Internal Directory mode including information about:

- Levels of Access
- How to Login and Out of the System
- Managing Devices
- How to Manage User Accounts
- Device Configuration Order Entry
- Management Tools
- CNS Image Service
- Backup and Restore
- Redefining Hostname, Domain Name, and Country Code
- Recovering Your CNS Password

Levels of Access

In Internal Directory mode, there are two categories of users who have access to device information:

- Administrator
- Operator

An Administrator has the higher access level of the two categories; full access to device and user information. An Operator has access to only order entry and operator password-related tasks.

For example, an Administrator can access all the functional areas of the user interface. Whereas, an Operator only has access to Order Entry and Tools functions.

How to Login and Out of the System

You can connect to the system by means of:

- SSH
- System console

How to Login

To login to the system, follow these steps:

Step 1 Launch your web browser.

This user interface is best viewed using Microsoft Internet Explorer, version 5.5 or later.

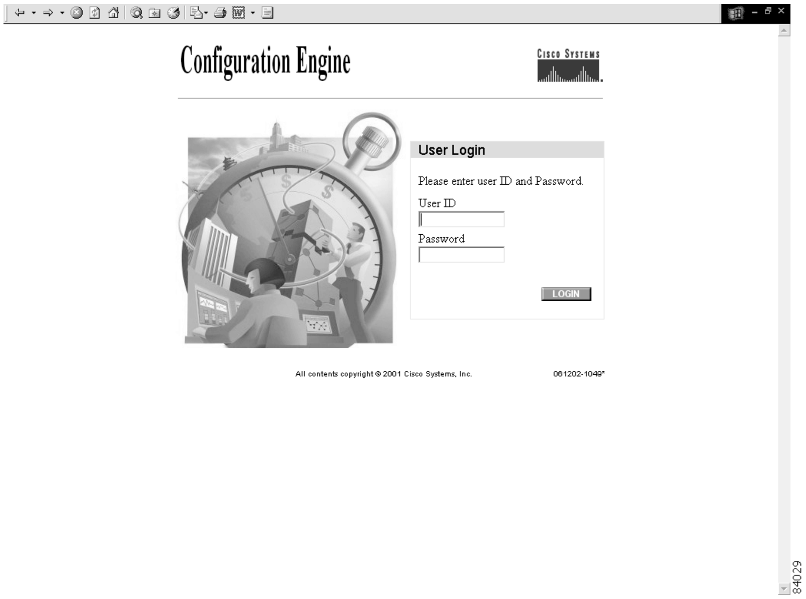
Step 2 Go to the Cisco CNS Configuration Engine 1.4 URL.

For example: **http://<***ip_address***>**

Note If encryption is set during Setup (see "Encryption Settings" section on page 2-6), use **https://<***ip_address***>**.

The login window appears (see Figure 2-1).

Figure 2-1 Logging In to the Configuration Server



Please enter user ID and Password.

All contents copyright © 2001 Cisco Systems, Inc. 061202-1049*

Step 3 Enter your **User ID**.

This is the value for the **ConfigService AdminID** parameter that you entered during **Setup**.

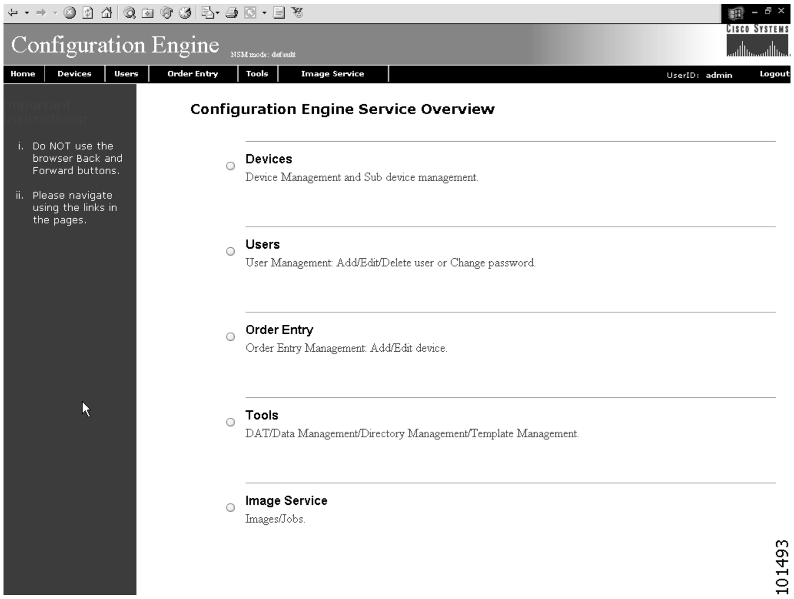
Step 4 Enter your password.

Step 5 Click **LOGIN**.

For an Administrator, the full-function Cisco CNS Configuration Engine 1.4 Home page appears (see Figure 2-2).

For an Operator, a limited-function Cisco CNS Configuration Engine 1.4 Home page appears where the active tabs are **Home**, **Order Entry**, and **Tools** (see Figure 2-3).

Figure 2-2 Administrator Home Page



Important Instructions:

i. Do NOT use the browser Back and Forward buttons.

ii. Please navigate using the links in the pages.

Configuration Engine Service Overview

○ **Devices**
Device Management and Sub device management.

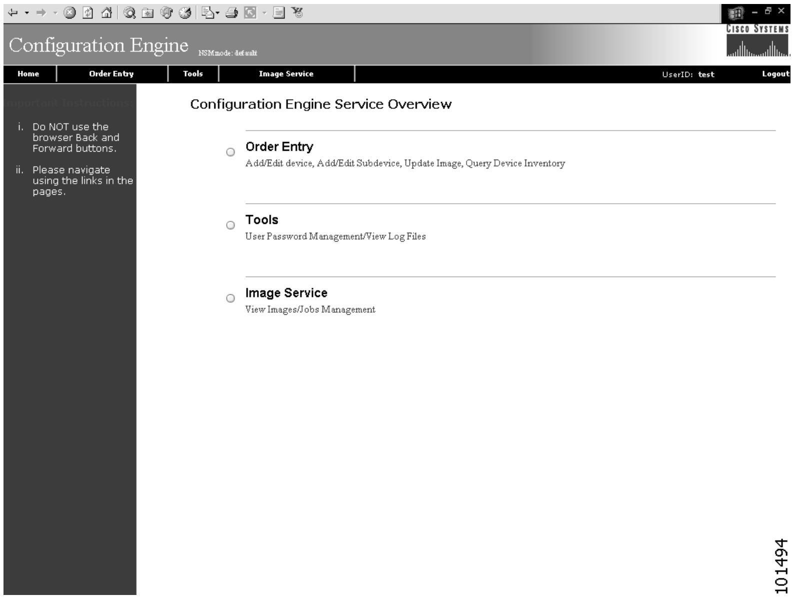
○ **Users**
User Management: Add/Edit/Delete user or Change password.

○ **Order Entry**
Order Entry Management: Add/Edit device.

○ **Tools**
DAT/Data Management/Directory Management/Template Management.

○ **Image Service**
Images/Jobs.

Figure 2-3 Operator Home Page



Important Instructions:

i. Do NOT use the browser Back and Forward buttons.

ii. Please navigate using the links in the pages.

Configuration Engine Service Overview

○ **Order Entry**
Add/Edit device, Add/Edit Subdevice, Update Image, Query Device Inventory

○ **Tools**
User Password Management/View Log Files

○ **Image Service**
View Images/Jobs Management

How to Log Out

To log out of the system, click the **Logout** button.

Operator-Level Operations

After logging into the Cisco CNS Configuration Engine 1.4, an Operator has access to the following functions:

- Order Entry
  - New Order
  - Edit Order
  - Subdevice Order
  - Update Image
  - Query Device Inventory
- Tools
  - Change Password
  - View Event Log
  - View Image Server Log
- Image Service
  - View Image
  - Query Job
  - Cancel/Stop Job
  - Restart Job

Device Configuration Order Entry

The order entry functions of creating a new device configuration order, editing an existing order, and managing subdevice orders are available to both Administrator and Operator.

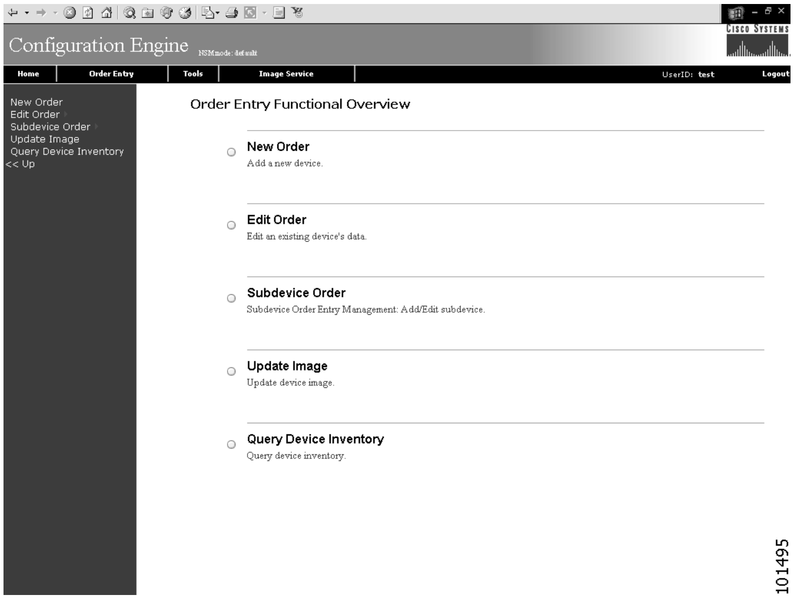
To conduct device configuration order entry operations as an Operator, follow these steps:

Step 1 From the Home page, click **Order Entry**.

The Order Entry page appears (see Figure 2-4).

Step 2 To add and edit device configuration orders, see "Device Configuration Order Entry" section on page 2-36.

Figure 2-4 Order Entry for Operator-Level User



Order Entry Functional Overview

○ **New Order**
Add a new device.

○ **Edit Order**
Edit an existing device's data.

○ **Subdevice Order**
Subdevice Order Entry Management: Add/Edit subdevice.

○ **Update Image**
Update device image.

○ **Query Device Inventory**
Query device inventory.

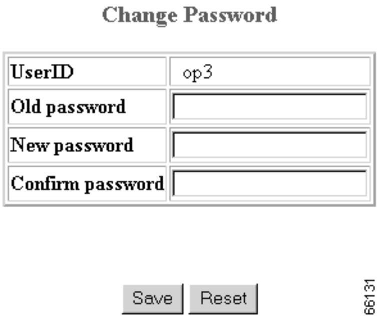
How to Change or Reset a Password at the Operator Level

Under tools, an Operator has access to the password editor (for changing or resetting only their own password), and the event log.

To change or reset a password at the operator level, click **Tools**.

The password editor appears (see Figure 2-5).

Figure 2-5 Operator Password Editor



Change Password

UserID	op3
Old password	
New password	
Confirm password	

Step 1 Enter your old password.

Table 2-1 lists valid values for these fields.

Table 2-1 Valid Values for Change Password by Operator

Attribute	Description	Valid Values
Old Password	Password	Printable characters with a length of 6 – 12
New Password	Password	Printable characters with a length of 6 – 12
Confirm Password	Password	Printable characters with a length of 6 – 12

Step 2 Enter your new password.

Step 3 To confirm your new password, enter it again.

Step 4 To save your changes, click **Save**.

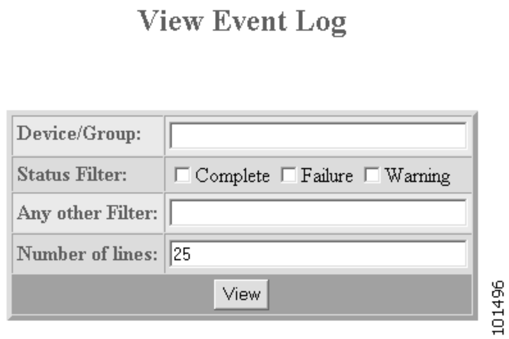
Step 5 To return to the Tools main menu, click the **Tools** tab.

How to View the Event Log

As an operator, to view the Event Log, click **Tools** -> **View Event Log**.

The Event Log control panel appears (see Figure 2-6)

Figure 2-6 Operator-Level Event Log Control Panel



View Event Log

Device/Group:

Status Filter: □ Complete □ Failure □ Warning

Any other Filter:

Number of lines: 25

Table 2-2 Valid Values for View Event Log by Operator

Attribute	Description	Valid Values
Device/Group	Name of device or group.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Status Filter	View complete Event Log, or just Failure Events or Warning Events.	Check Box

Table 2-2 Valid Values for View Event Log by Operator (continued)

Attribute	Description	Valid Values
Any other Filter		a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Number of lines	Default = 25	

CNS Image Service

Under **Image Service**, an Operator can view available images (see "How to View an Image" section on page 2-77) and perform tasks on image update operations the same as an administrator (see "Working with Image Update Jobs" section on page 2-84).

Administrator-Level Operations

In Internal Directory mode, an Administrator can access all of the functions provided by the Cisco CNS Configuration Engine 1.4 user interface including managing user accounts and devices.

Managing Devices

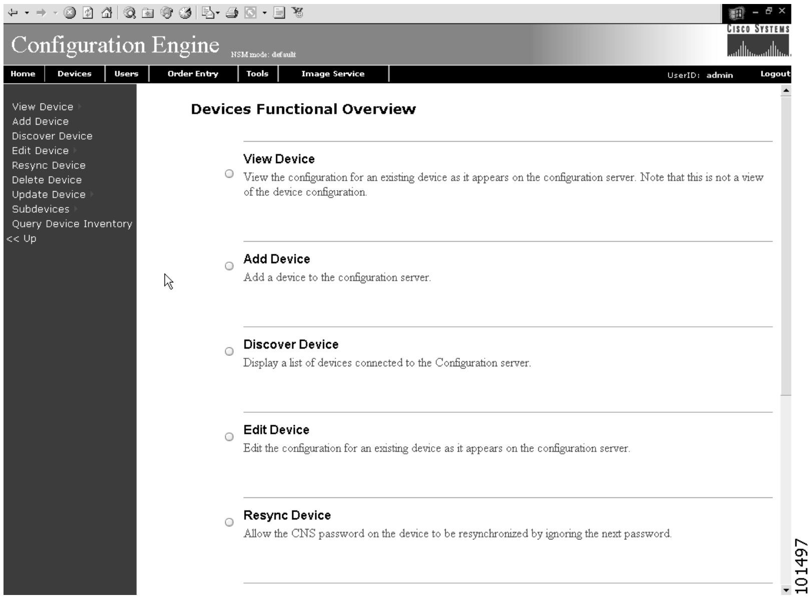
To begin managing devices, follow these steps:

Step 1 Login to the system (see "How to Login and Out of the System" section on page 2-1).

Step 2 From the Home page, click on the **Devices** tab.

A functional overview of the device administration options appears (see Figure 2-7).

Figure 2-7 Device Administration Overview



Devices Functional Overview

○ **View Device**
View the configuration for an existing device as it appears on the configuration server. Note that this is not a view of the device configuration.

○ **Add Device**
Add a device to the configuration server.

○ **Discover Device**
Display a list of devices connected to the Configuration server.

○ **Edit Device**
Edit the configuration for an existing device as it appears on the configuration server.

○ **Resync Device**
Allow the CNS password on the device to be resynchronized by ignoring the next password.

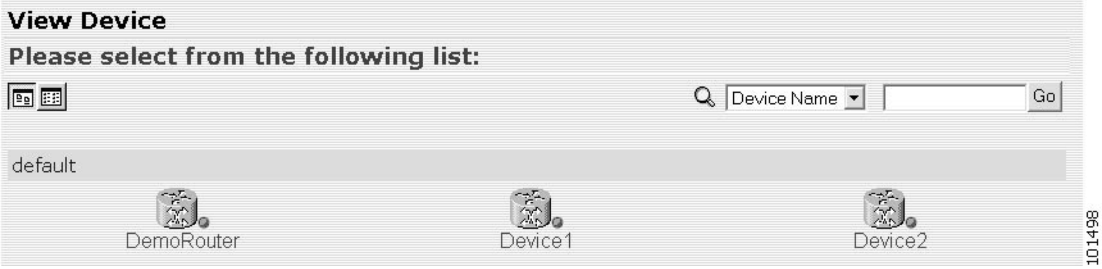
How to View Device Configuration

To view a device configuration, follow these steps:

Step 1 From the Devices Functional Overview page, click **View Device**.

The Device List page appears (see Figure 2-8).

Figure 2-8 View Device List



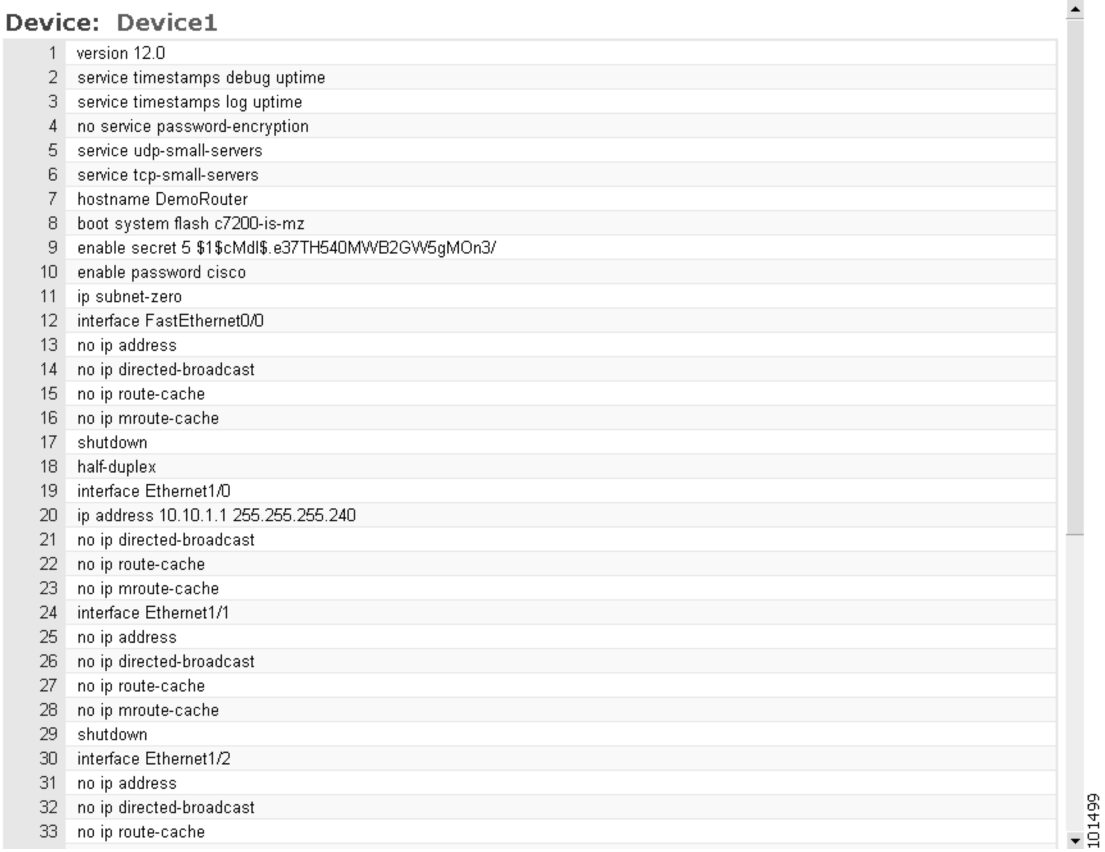
View Device

Please select from the following list:

Step 2 Click on the icon for the device configuration you wish to view.

The Configuration for that device appears (see Figure 2-9).

Figure 2-9 Device Configuration



Device: Device1

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
hostname DemoRouter
boot system flash c7200-is-mz
enable secret 5 $1$cMdl$.e37TH540MWB2GW5gMOn3/
enable password cisco
ip subnet-zero
interface FastEthernet0/0
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
half-duplex
interface Ethernet1/0
ip address 10.10.1.1 255.255.255.240
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
```

Note The device configuration displayed is the configuration as it appears at the configuration server. It may not be the configuration running on the device.

Step 3 To view subdevices (if applicable), in the left pane, click **View Subdevices.**

Step 4 To view Images associated with this device (if applicable), in the left pane, click **View Images**.

Step 5 To return to the Devices main menu, click on the **Devices** tab.

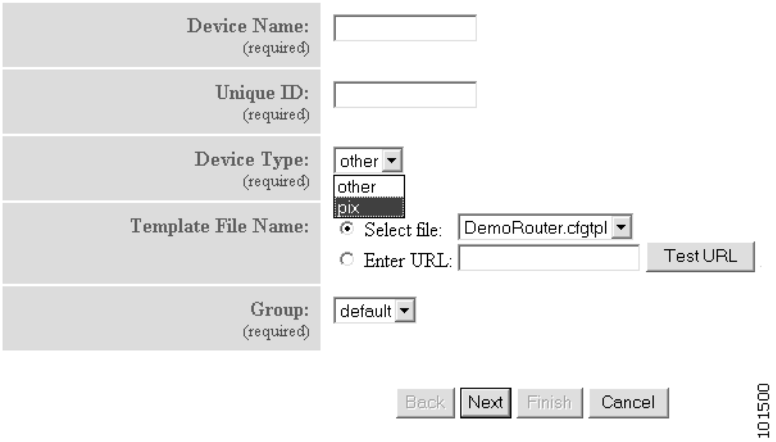
How to Add a Device

To add the logical appearance of a device to the configuration server, follow these steps:

Step 1 From the Devices Functional Overview page, click **Add Device**.

The Device Information page appears (see Figure 2-10).

Figure 2-10 Device Information Page



Device Name: (required)

Unique ID: (required)

Device Type: (required) other

Template File Name: ● Select file: DemoRouter.cfgtpl ○ Enter URL:

Group: (required) default

Step 2 Enter a valid value (no spaces) in the **Device Name** field.

Table 2-3 list valid values for these attributes.

Table 2-3 Valid Values for Add Device

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Unique ID	Unique ID of the device.	Default or a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Device Type	Type of device	From drop-down list
Template File Name	Name of the configuration template to associate with the device.	From drop-down list
Group	Names of groups with which this device can be associated.	From drop-down list

Step 3 In the **Unique ID** field, accept the default value that appears or enter another valid value (no spaces).

Step 4 Select a device type from the drop-down list.

Step 5 Choose a template file.

To use a template on your Cisco CNS Configuration Engine 1.4:

a. Choose **Select file**.

b. Use the drop-down list to choose a template.

OR

To use an external template:

a. Choose **Enter URL**.

b. Enter the full URL for the server, directory, and filename where the template is stored. Currently, only **http** is supported.

c. To test access to the external template, click **Test URL**.

If the server is unavailable or the external template cannot be accessed, an error appears. You can still save this logical device, but the template is not available until you have access to the external template.

Step 6 Choose a group.

Tip Use the Group Manager under DAT (see "How to Add a Group" section on page 4-15) to set up groups before you add a device.

Step 7 To cancel creating a device and return to the Devices main menu, click **Cancel**.

Step 8 To return to the Devices main menu and cancel creating a device, click on the **Devices** tab.

Step 9 To continue creating IDs for this device, click **Next**.

If the Device Type is not Pix, the Create Device page for adding device IDs appears (see Figure 2-12).

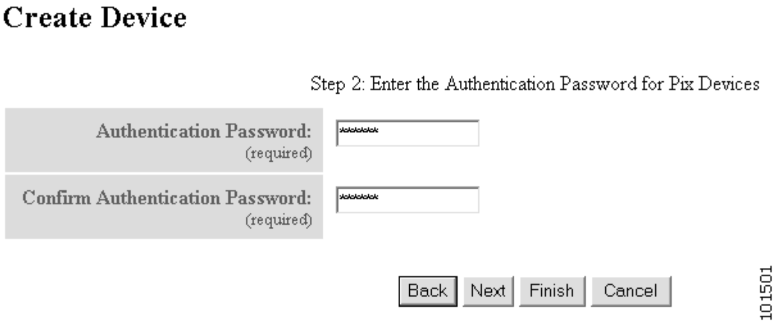
If the Device Type is Pix, the Pix Password page appears (see Figure 2-11).

Step 10 If applicable, enter an authentication password for Pix device, otherwise skip to Step 11.

Table 2-4 Valid Values for Change Password by Operator

Attribute	Description	Valid Values
Authentication Password	Password	Printable characters with a length of 6 – 12
Confirm AuthenticationPassword	Password	Printable characters with a length of 6 – 12

Figure 2-11 Pix Password Page



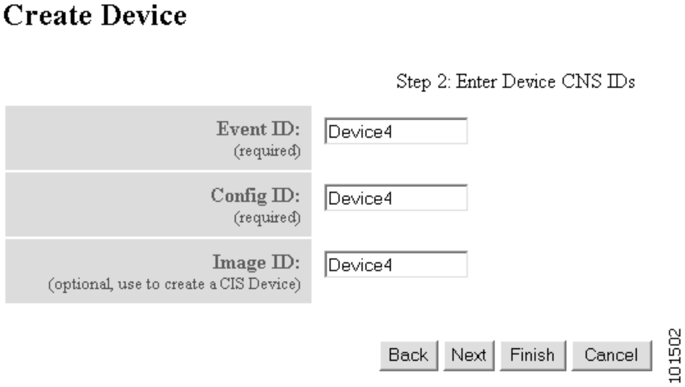
Create Device

Step 2: Enter the Authentication Password for Pix Devices

Authentication Password: (required) ******

Confirm Authentication Password: (required) ******

Figure 2-12 Device IDs Page



Create Device

Step 2: Enter Device CNS IDs

Event ID: (required)	Device4
Config ID: (required)	Device4
Image ID: (optional, use to create a CIS Device)	Device4

Step 11 For the **Event ID**, accept the default value that appears or enter another value.

Table 2-5 list valid values for these attributes.

Table 2-5 Valid Values for Add Device

Attribute	Description	Valid Values
Event ID	Event ID to associated with this device.	Default, or a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Config ID	Configuration ID to associated with this device.	Default, or a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Image ID	Image ID to associated with this device.	Default, or a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 12 For the **Config ID**, accept the default value that appears or enter another value.

Step 13 For the Image ID, if you are using configuration service only, leave this field blank.

To use image service this parameter must be specified.

Step 14 To cancel creating a device and return to the Devices main menu, click **Cancel**.

Step 15 If applicable (modular router), choose subdevices.

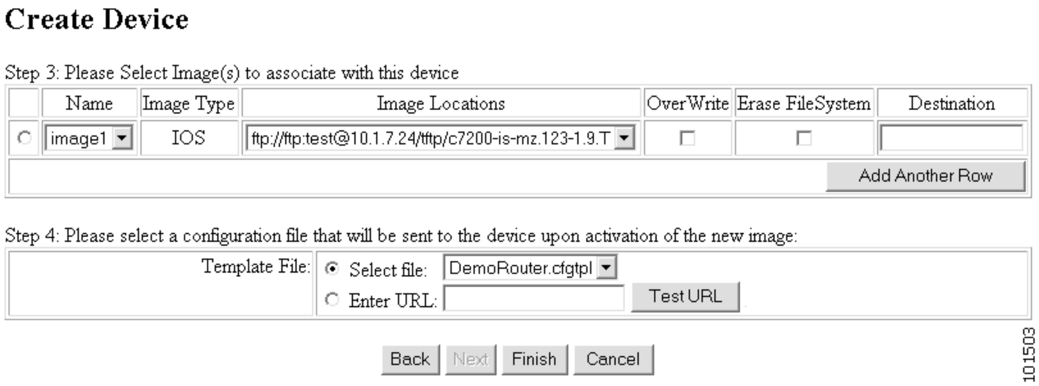
Step 16 To go back to the previous page, click **Back**.

Step 17 To finish creating this device at this point, click **Finish**.

Step 18 To continue creating Image associations for this device, click **Next**.

The Create Device page for adding Image associations appears (see Figure 2-13).

Figure 2-13 Create Device Image Association



Create Device

Step 3: Please Select Image(s) to associate with this device

	Name	Image Type	Image Locations	OverWrite	Erase FileSystem	Destination
○	image1 ▾	IOS	ftp://ftp:test@10.1.7.24/tftp/c7200-is-mz.123-1.9.T ▾	□	□	

Step 4: Please select a configuration file that will be sent to the device upon activation of the new image:

Template File: ● Select file: DemoRouter.cfgtpl ▾
○ Enter URL:

Step 19 In Step 3 on the page, select the image from the **Name** drop-down list.

The **Image Type** field and **Image Location** drop-down box are populated with corresponding information for the image.

Step 20 From the **Image Location** drop-down list, select the desired location.

Step 21 To add another row for image location, click **Add Another Row**.

You can locate multiple copies of an image on separate servers. This allows you to do load-sharing when updating a large number of devices. Each device in a large group can be associated with a copy of the image located at one of many server locations.

Step 22 In the Destination field, enter a valid URL where the image will be copied.

For example:

disk0:/c7200-mz

Step 23 To indicate which image is to be activated on the device after distribution, select the radio button in front of each row.

Step 24 In Step 4, on the page, select the Configuration Control template file you want to send to this device for activation of a new image:

Tip Use the Configuration Control template that contains the CLI commands required for image activation for this device (see "Configuration Control Template" section on page 2-22). If you do not have such a template, see "How to Add a Template" section on page 2-65.

a. To select a template file from the drop-down list, click the **Select file** radio button.

b. Use the drop-down list to choose a template file.

OR

To use an external template:

a. Choose **Enter URL**.

b. Enter the full URL for the server, directory, and filename where the template is stored. Currently, only **http** is supported.

c. To test access to the external template, click **Test URL**.

If the server is unavailable or the external template cannot be accessed, an error appears. You can still save this logical device, but the template is not available until you have access to the external template.

Step 25 To cancel creating a device and return to the Devices main menu, click **Cancel**.

Step 26 To go back to the previous page, click **Back**.

Step 27 To finish creating this device, click **Finish**.

How to Edit a Device

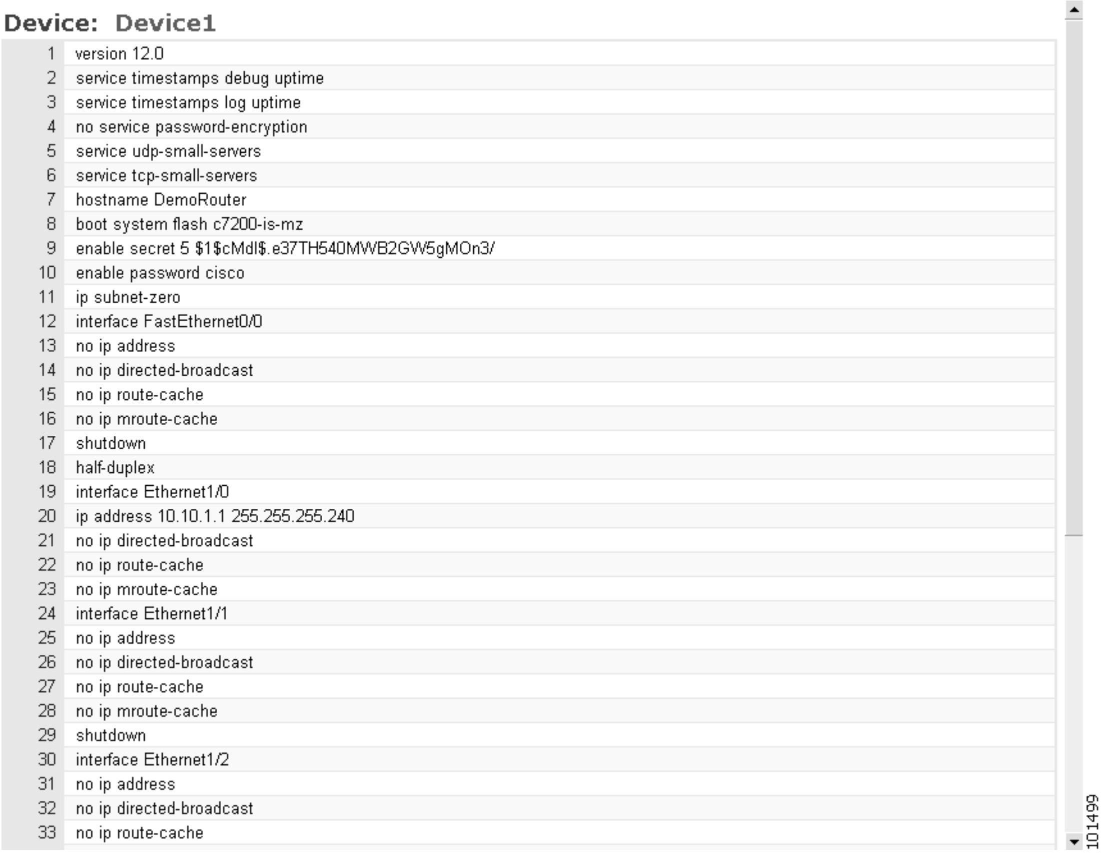
To edit information associated with a particular device, follow these steps:

Step 1 From the Devices Functional Overview page, click **Edit Device**.

Step 2 From the Edit Device page, click on the icon for the device you wish to edit.

The device configuration appears with a menu of edit functions in the left pane (see Figure 2-14).

Figure 2-14 Device Configuration



Device: Device1

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
hostname DemoRouter
boot system flash c7200-is-mz
enable secret 5 $1$cMdl$.e37TH540MWB2GW5gMOn3/
enable password cisco
ip subnet-zero
interface FastEthernet0/0
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
half-duplex
interface Ethernet1/0
ip address 10.10.1.1 255.255.255.240
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
```

Step 3 From the left pane, choose the edit function you want to use.

Step 4 To go back to the Device List page, in the left pane, click **<< Up**.

Step 5 To return to the Devices main menu, click on the **Devices** tab.

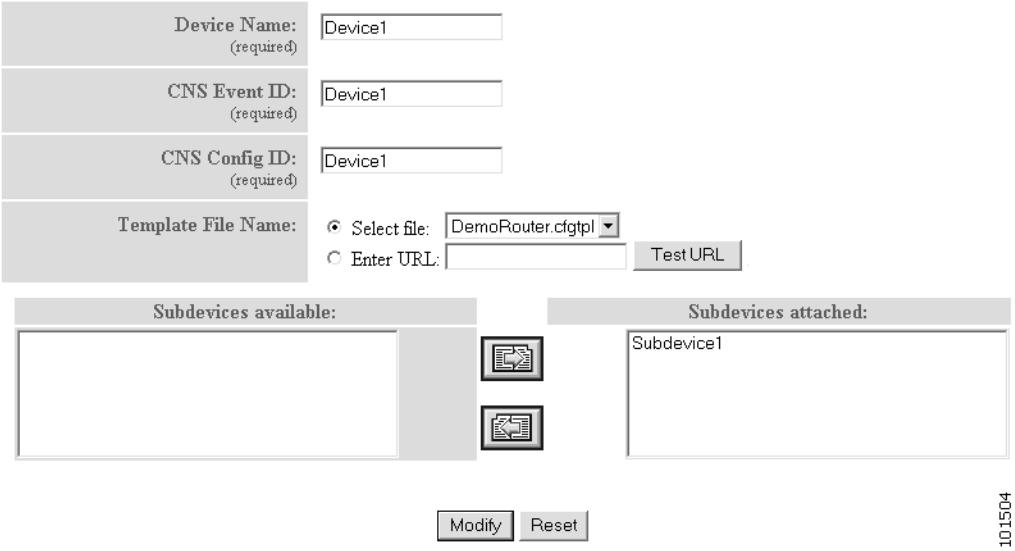
How to Edit Device Information

To edit device information, follow these steps:

Step 1 From the Edit Device page, click **Edit Information**.

The device information editor page appears. For devices other than PIX, see Figure 2-15. For PIX device, see Figure 2-16.

Figure 2-15 Device Information Editor



Device Name: (required) Device1

CNS Event ID: (required) Device1

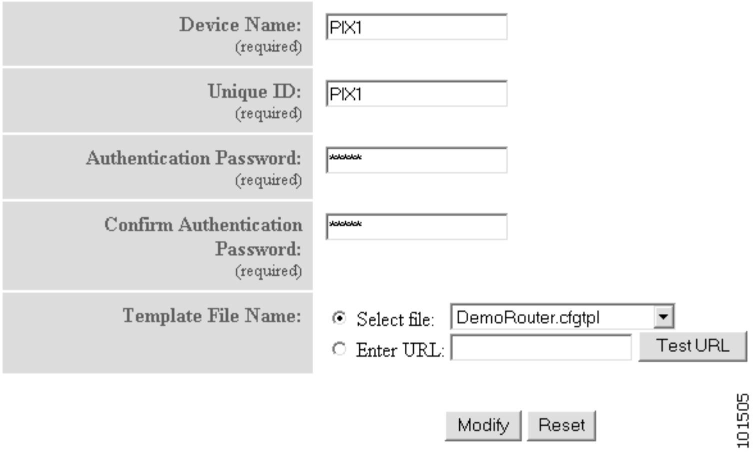
CNS Config ID: (required) Device1

Template File Name: ● Select file: DemoRouter.cfgtpl ○ Enter URL:

Subdevices available:

Subdevices attached: Subdevice1

Figure 2-16 Device Information Editor for PIX Device



Device Name: (required)	PIX1
Unique ID: (required)	PIX1
Authentication Password: (required)	*****
Confirm Authentication Password: (required)	*****
Template File Name:	● Select file: DemoRouter.cfgtpl ○ Enter URL:

Step 2 To modify the device name, enter a valid value (no spaces) in the **Device Name** field.

Table 2-6 Valid Values for Edit Device

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Unique ID	Unique ID of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Authentication Password	Password	Printable characters with a length of 6 – 12
Device Type	Type of device	From drop-down list
Template File Name	Name of the configuration template to associate with the device.	From drop-down list

Step 3 To modify the Unique ID, enter a valid value (no spaces) in the **Unique ID** field.

Step 4 Modify the template file as required.

Step 5 To revert to the existing values, click **Reset**.

Step 6 To update device information, click **Modify**.

Step 7 To return to the Devices main menu, click on the **Devices** tab.

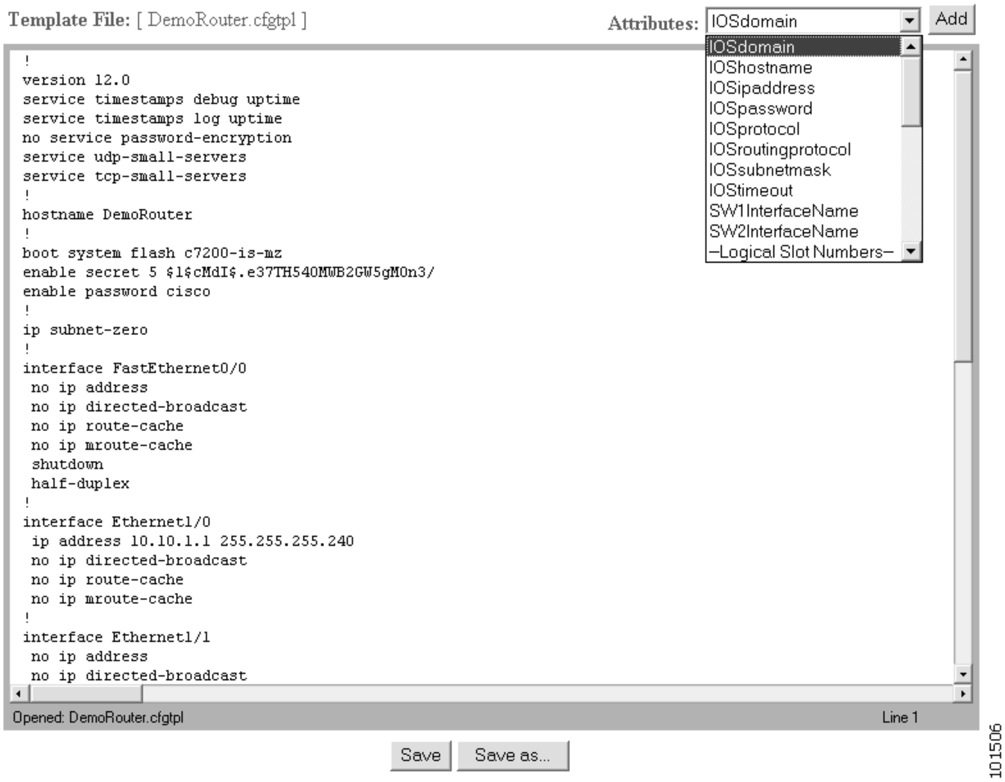
How to Edit Device Templates

To edit a device template, follow these steps:

Step 1 From the Edit Device page, click **Edit Template**.

The template editor appears (see Figure 2-17).

Figure 2-17 Template Editor



Template File: [DemoRouter.cfgtpl]

Attributes: IOSdomain

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname DemoRouter
!
boot system flash c7200-is-mz
enable secret 5 $1$cMdI$.e37TH540MWB2GW5gM0n3/
enable password cisco
!
ip subnet-zero
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
 half-duplex
!
interface Ethernet1/0
 ip address 10.10.1.1 255.255.255.240
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/1
 no ip address
 no ip directed-broadcast
```

Opened: DemoRouter.cfgtpl

Line 1

Step 2 In the **Attributes** field, click the drop-down arrow.

Step 3 Choose the attribute you wish to add to the template, then click **Add**.

Step 4 Repeat Steps 2 and 3 for all attributes you wish to add to the template file.

Step 5 Delete all unusable strings from the template file.

Step 6 Edit strings as necessary.

The default multi-line begin and end tags are **^[** and **^]** respectively. The delimiter for these tags are: ~ ! @ ^ & * - = |. Do not use # or %.

For example, a multi-line test banner might be:

```
banner exec ^[*
    This is a Test Banner
    1. Hi
    2. Hello
    3. Test is 1234567890*
^]
```

Step 7 To save your edits, click **Save**.

Step 8 To save this version as a new template, click **Save as**.

Step 9 To return to the Devices main menu, click on the **Devices** tab.

How to Edit Device Parameters

To edit device parameters, follow these steps:

Step 1 From the Edit Device page, click **Edit Parameter**.

The parameters editor appears.

Step 2 Edit all active lines as required.

Step 3 To save your edits, click **Save Parameters**.

Step 4 To return to the Devices main menu, click on the **Devices** tab.

How to Edit Contact Information

To edit contact information related to the physical location of a device, follow these steps:

Step 1 From the Edit Device page, click **Edit ContactInfo**.

The contact information appears.

Step 2 Edit all active fields as required.

Step 3 To clear your entries, click **Reset**.

Step 4 To save your edits, click **Update**.

Step 5 To return the to the Devices main menu, click on the **Devices** tab.

How to Edit Subdevices

For complete information about working with subdevices, including editing, see “Working with Subdevices” section on page 2-23.

How to Edit Image Association Information

To edit image information associated with a device, follow these steps:

Step 1 From the Edit Device page, click **Edit Images**.

The Edit Device Image page appears.

Step 2 Edit image and configuration information as required.

Step 3 To revert to the previous state, click **Cancel**.

Step 4 To complete this task, click **Finish**.

How to Resynchronize a Device

If the cns_password of a device becomes corrupted so that there is a mismatch between the device and the corresponding password information help in the directory, you can resynchronize the device with the CNS Configuration Engine 1.4 by using the Resync Device function.

To resynchronize a device, follow these steps:

Step 1 From the Devices Functional Overview page (see Figure 2-7), click **Resync Device**.

Step 2 From the Resync Device page, click on the icon for the device you wish to re-synchronize.

Note PIX devices will not be visible on this page.

Step 3 In the confirmation window that appears, click **Ok**.

Step 4 To return to the Devices main menu, click on the **Devices** tab.

How to Delete a Device

To delete the logical appearance of a device from the configuration server, follow these steps:

Step 1 From the Devices Functional Overview page (see Figure 2-7), click **Delete Device**.

Step 2 From the Delete Device page, click **View**.

Step 3 Click the check box for the device(s) you wish to delete.

Step 4 Click **Next**.

A list of devices selected for deletion appears.

Step 5 To abandon this task at this point, in the left pane, click **<< Up**.

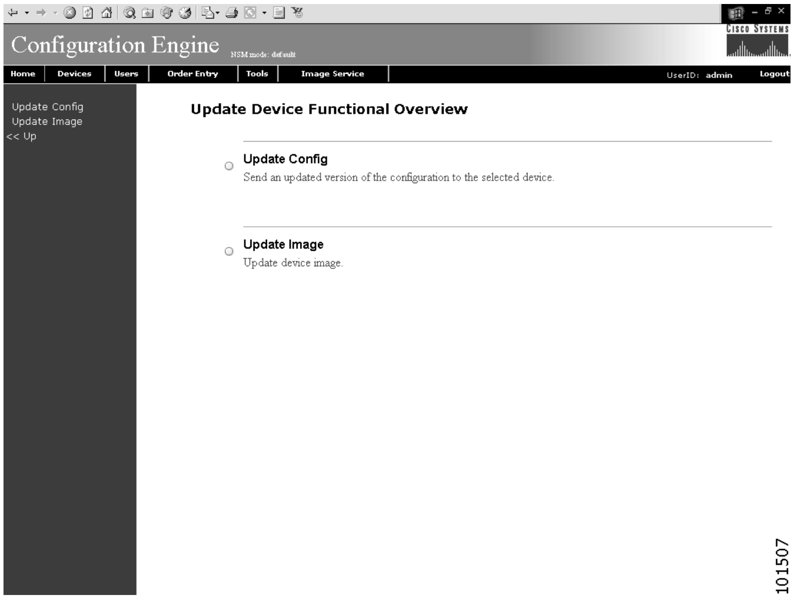
Step 6 To continue, click **Delete**.

Step 7 To return to the Devices main menu, click on the **Devices** tab.

How to Update Device Configuration and Image

To send an updated version of the configuration or a new image to a device, from the Devices Functional Overview page, click **Update**. The Update Device Functional Overview page appears (see Figure 2-18).

Figure 2-18 Update Device



Update Device Functional Overview

○ Update Config
Send an updated version of the configuration to the selected device.

○ Update Image
Update device image.

How to Update Device Configuration

To update a device configuration, complete the following steps:

Step 1 From the Update Device Functional Overview page, click **Update Config**.

Step 2 To update all the devices in a particular group(s), click the check box next to the icon for the desired group(s).

Step 3 To update the configuration for certain devices, from the Update Device Config page, click **View**.

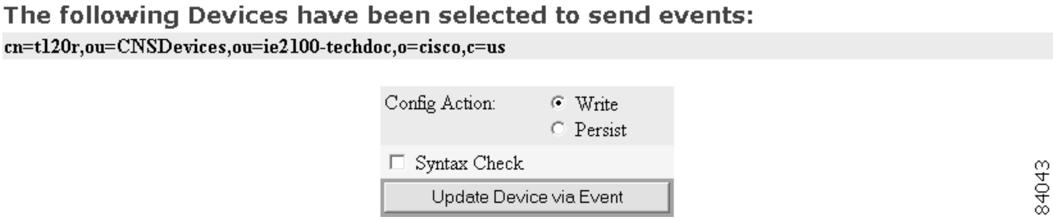
Step 4 Click the check box next to the icon for the device(s) you wish to update.

Note PIX devices will not be visible on this page.

Step 5 Click **Next**.

The update task dialog box appears (see Figure 2-19)

Figure 2-19 Update Task



The following Devices have been selected to send events:

cn=t120r,ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

Config Action: ● Write ○ Persist

□ Syntax Check

Step 6 Choose the **Config Action** task you require.

- Write – applies the configuration without causing it to persist in NVRAM.

- Persist – applies the change and causes it to persists in NVRAM.

Step 7 If required, check the **Syntax Check** check-box.

Step 8 Click **Update Device via Event**.

Step 9 To return to the Devices main menu, click on the **Devices** tab.

How to Update Device Image

To update a device image, complete the following steps:

Step 1 From the Update Device Functional Overview page, click **Update Image**.

Step 2 To update all devices in a particular group, click the check box for the desired group.

Step 3 To update the image for a certain device, from the Update Device Image page, click **View**.

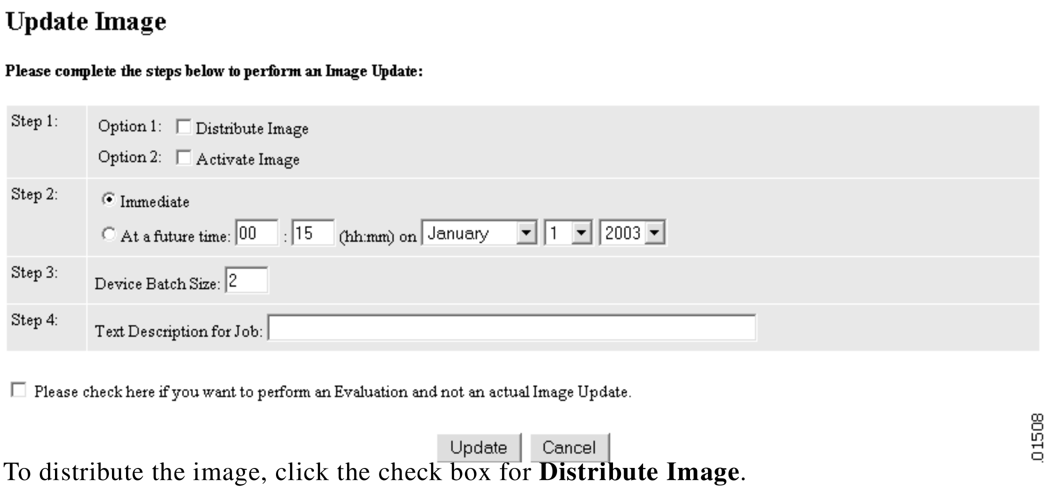
Step 4 Click the check box next to the icon for the device(s).

Note PIX devices will not be visible on this page.

Step 5 Click **Submit**.

The Update Image page appears (see Figure 2-20)

Figure 2-20 Update Image



Update Image

Please complete the steps below to perform an Image Update:

Step 1:	Option 1: □ Distribute Image Option 2: □ Activate Image
Step 2:	● Immediate ○ At a future time: 00 : 15 (hh:mm) on January 1 2003
Step 3:	Device Batch Size: 2
Step 4:	Text Description for Job:

□ Please check here if you want to perform an Evaluation and not an actual Image Update.

Step 6 To distribute the image, click the check box for **Distribute Image**.

Step 7 To activate the image, click the check box for **Activate Image**.

Tip All three agents (event, partial config, and image) must be running on the device for the activation process to succeed.

Note For the image to become active on the device, you must have a Configuration Control template associated with this device that contains the CLI commands for image activation (see "Configuration Control Template" section on page 2-22).

Step 8 To update the image immediately, click the radio button for **Immediate**.

Step 9 To update the image at a specified time in the future, click the radio button for **At a future time**:

a. Enter a time value.

b. Enter a date value.

Step 10 Set the **Device Batch Size**.

This is the number of concurrent image updates. This feature allows you to limit the number of concurrent requests to a server. When one batch of image update requests has been satisfied, then next batch starts.

Note If you are running a device image update session to a mix of IMGW and agent devices, the effective device batch size limit for IMGW devices—concurrent Telnet session limit—is equal to the value (default = 20) set for this attribute in the **Setup** program (refer to the *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*).

Step 11 If applicable, enter a text description of the job.

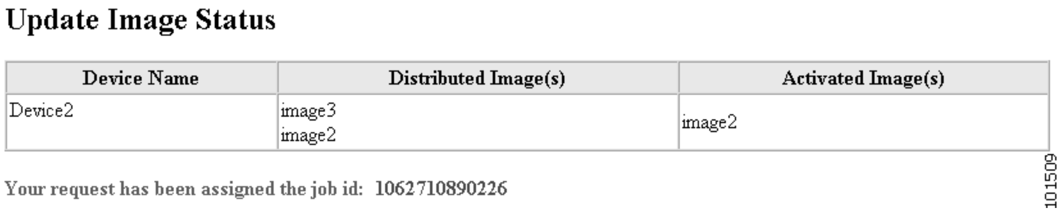
Step 12 To perform an evaluation rather than an actual update, click the check box at the bottom of this pane.

Step 13 To abandon this task, on the Update Image page, click **Cancel**.

Step 14 To continue, complete the steps called for, then click **Update.**

The Update Image Status page appears (see Figure 2-21). You can use this Job ID to perform job-related tasks (see "Image Update Jobs" section on page 2-83).

Figure 2-21 Job ID for Update Image



Update Image Status

Device Name	Distributed Image(s)	Activated Image(s)
Device2	image3 image2	image2

Your request has been assigned the job id: 1062710890226

Step 15 To return to the Devices main menu, click on the **Devices** tab.

Configuration Control Template

To restart a device with a new image, you need to issue the CLI commands that you would normally enter from the device console to activate a new image.

For example, if you want to restart a Cisco 3600 Series router with an image named *3600.image*, from the device console, you would issue the following CLI commands:

no boot system
boot system flash:3600.image

Because you are using the CNS 2100 Series system running the CNS Configuration Engine 1.4 application to update and activate a new image on a device, you need to provide the device with a Configuration Control template that contains the required CLI commands for image activation.

If you do not have such a template, see "How to Add a Template" section on page 2-65. Also, you must associate this Configuration Control template with the particular device (see Step 24 under "How to Add a Device").

The content of the Configuration Control template for image activation should contain the CLI commands that you would normally enter from the device console to activate a new image on the device.

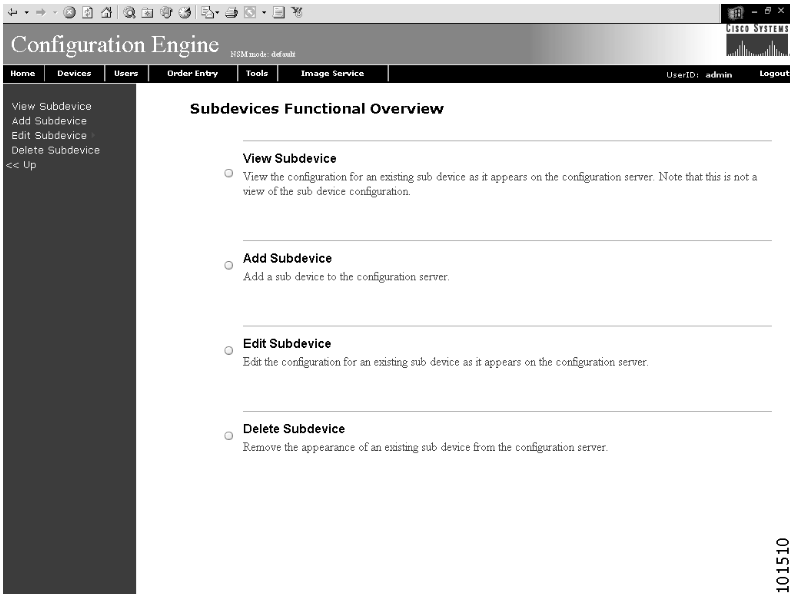
Working with Subdevices

A subdevice is a configuration object for network modules in a modular router. When working with subdevices, it is very important to pick the correct type of interface card or module.

To work with subdevices, from the Devices Functional Overview page, click **Subdevices**.

The Subdevices Functional Overview page appears (see Figure 2-22).

Figure 2-22 Subdevices



Subdevices Functional Overview

○ **View Subdevice**
View the configuration for an existing sub device as it appears on the configuration server. Note that this is not a view of the sub device configuration.

○ **Add Subdevice**
Add a sub device to the configuration server.

○ **Edit Subdevice**
Edit the configuration for an existing sub device as it appears on the configuration server.

○ **Delete Subdevice**
Remove the appearance of an existing sub device from the configuration server.

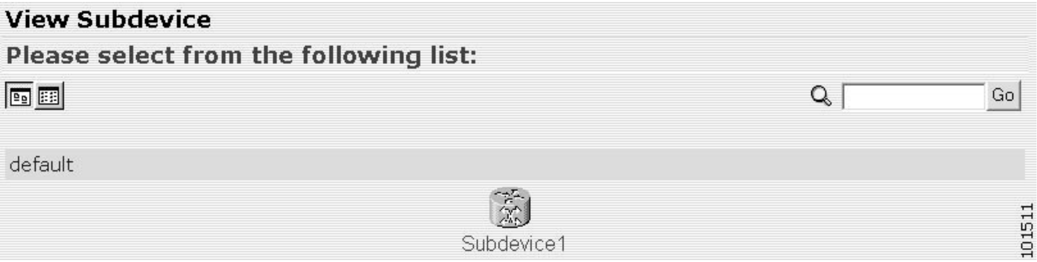
How to View Subdevices

To view subdevices, follow these steps:

Step 1 From the Subdevices Functional Overview page, select **View Subdevice**.

The list of subdevices appears (see Figure 2-23).

Figure 2-23 View Subdevice



View Subdevice

Please select from the following list:

default

Subdevice1

Step 2 Click on the icon for the device configuration you wish to view.

The Configuration for that device appears.

> **Note** The subdevice configuration displayed is the configuration as it appears at the configuration server. It may not be the configuration running on the subdevice.

Step 3 To return to the Devices main menu, click on the **Devices** tab.

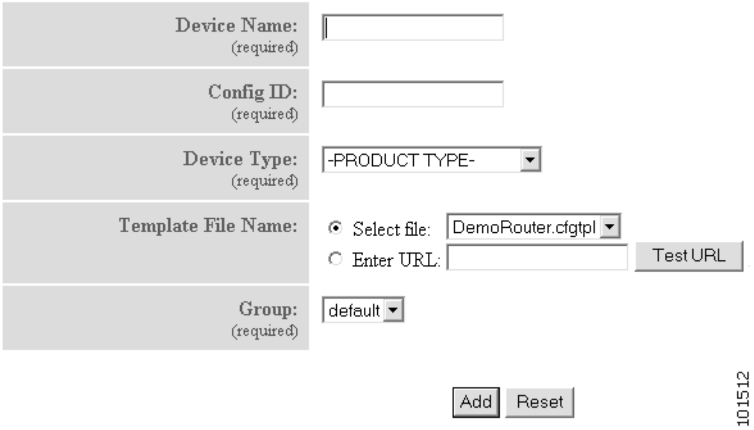
How to Add Subdevices

To add the logical appearance of a subdevice to the configuration server, follow these steps:

Step 1 From the Subdevices Functional Overview page, click **Add Subdevice**.

The Subdevice Information page appears (see Figure 2-24).

Figure 2-24 Subdevice Information Page



Device Name: (required)	
Config ID: (required)	
Device Type: (required)	-PRODUCT TYPE-
Template File Name:	● Select file: DemoRouter.cfgtpl ○ Enter URL:
Group: (required)	default

Step 2 Enter a valid value (no spaces) in the **Device Name** field.

Table 2-7 Valid Values for Add Subdevice

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
ConfigID	Configuration ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Device Type		From drop-down list
Template File Name	Name of the configuration template to associate with the device.	From drop-down list
Group	Names of groups with which this device can be associated.	From drop-down list

Step 3 Accept the default value that appears or enter another valid value (no spaces) in the **Config ID** field.

Step 4 From the **Device Type** drop-down list, choose the type of device to which this subdevice is associated.

Device type is the name of the network module as defined in the Cisco product catalog (price list).

Step 5 Choose a template file.

To use a template on your Cisco CNS Configuration Engine 1.4:

a. Choose **Select file**.

b. Use the drop-down list to choose a template.

OR

To use an external template:

a. Choose **Enter URL**.

b. Enter the full URL for the server, directory, and filename where the template is stored. Currently, only **http** is supported.

c. To test access to the external template, click **Test URL**.

If the server is unavailable or the external template cannot be accessed, an error appears. You can still save this logical subdevice, but the template is not available until you have access to the external template.

Step 6 Choose a group.

Step 7 To clear your entries, click **Reset**.

Step 8 To add this device, click **Add**.

Step 9 To return to the Devices main menu, click on the **Devices** tab.

How to Edit Subdevices

To edit information associated with a particular subdevice, follow these steps:

Step 1 From the Subdevices Functional Overview page, click **Edit Subdevice**.

Step 2 From the Edit Subdevice page, click on the icon for the subdevice you wish to edit.

The subdevice configuration appears with a menu of edit functions in the left pane.

Step 3 From the left pane, choose the edit function you want to use.

Step 4 To go back to the Device List page, in the left pane, click **<< Up**.

Step 5 To return to the Devices main menu, click on the **Devices** tab.

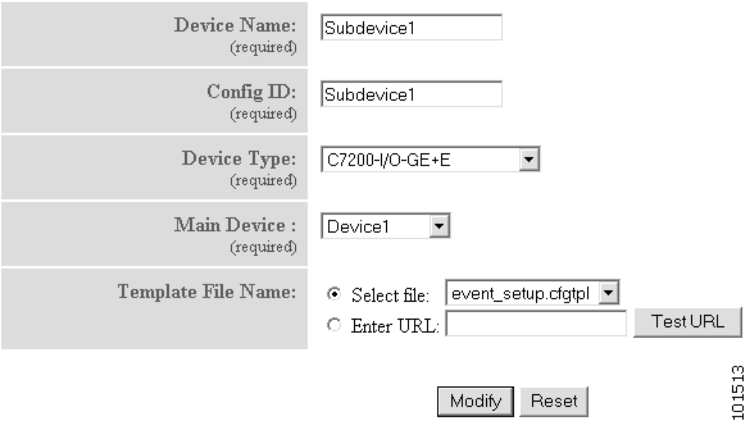
How to Edit Subdevice Information

To edit subdevice information, follow these steps:

Step 1 From the Edit Subdevice page, click **Edit Information**.

The subdevice information editor dialog box appears (see Figure 2-25).

Figure 2-25 Device Information Editor



Device Name: (required)	Subdevice1
Config ID: (required)	Subdevice1
Device Type: (required)	C7200-I/O-GE+E
Main Device : (required)	Device1
Template File Name:	● Select file: event_setup.cfgtpl ○ Enter URL:

Step 2 To modify the device name, enter a valid value (no spaces) in the **Device Name** field.

Table 2-8 Valid Values for Modify Subdevice

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
ConfigID	Configuration ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Device Type		From drop-down list
Template File Name	Name of the configuration template to associate with the device.	From drop-down list

Step 3 To modify the ConfigID, enter a valid value (no spaces) in the **Config ID** field.

Step 4 To modify the device type, choose the appropriate device.

Step 5 To modify the template filename, choose a new template filename.

Step 6 Modify the template file as required.

Step 7 Use the Arrow buttons to modify the status of subdevices attached to this device.

Step 8 To clear your entries, click **Reset**.

Step 9 To update device information, click **Modify**.

Step 10 To return to the Devices main menu, click on the **Devices** tab.

How to Edit Subdevice Template

To edit a device template, follow these steps:

Step 1 From the Edit Subdevice page, click **Edit Template**.

The template editor appears.

Step 2 In the **Attributes** field, click the drop-down arrow.

Step 3 Choose the attribute you wish to add to the template, then click **Add**.

Step 4 Repeat Steps 2 and 3 for all attributes you wish to add to the template file.

Step 5 Delete all unusable strings from the template file.

Step 6 Edit strings as necessary.

The default multi-line begin and end tags are **^[** and **^]** respectively. The delimiter for these tags are: ~ ! @ ^ & * - = |. Do not use # or %.

A multi-line test banner might be:

```
banner exec ^[*
    This is a Test Banner
    1. Hi
    2. Hello
    3. Test is 1234567890*
^]
```

Step 7 To save your edits, click **Save**.

Step 8 To save this version as a new template, click **Save as**.

Step 9 To return to the Devices main menu, click on the **Devices** tab.

How to Edit Subdevice Parameters

To edit subdevice parameters, follow these steps:

Step 1 From the Edit Subdevice page, click **Edit Parameter**.

The parameters editor appears.

Step 2 Modify parameters values as required.

Step 3 To save your edits, click **Save Parameters**.

Step 4 To return to the Devices main menu, click on the **Devices** tab.

How to Edit Contact Information

To edit contact information related to the physical location of a device, follow these steps:

Step 1 From the Edit Device page, click **Edit ContactInfo**.

The contact information appears.

Step 2 Edit all active fields as required.

Step 3 To clear your entries, click **Reset**.

Step 4 To save your edits, click **Update**.

Step 5 To return the to the Devices main menu, click on the **Devices** tab.

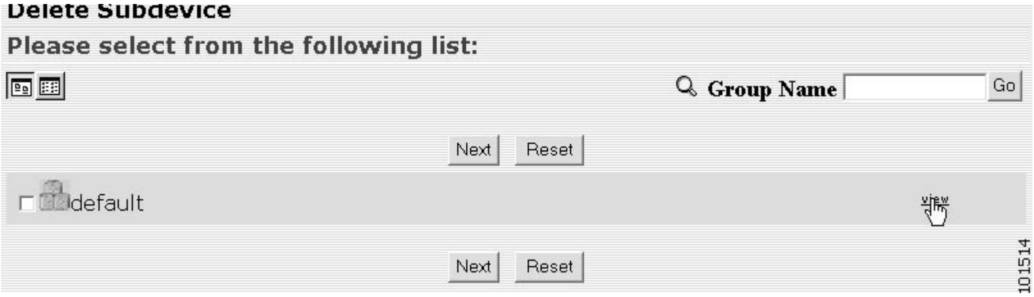
How to Delete Subdevices

To delete the logical appearance of a subdevice from the configuration server, follow these steps:

Step 1 From the Subdevices Functional Overview page (see Figure 2-22), click **Delete Device**.

The Delete Subdevice page appears (see Figure 2-26).

Figure 2-26 Delete Subdevice



Step 2 To delete all subdevices in a group, check the group.

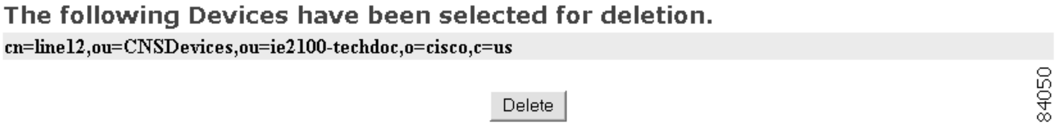
Step 3 To delete certain subdevices in a group, click **View**.

Step 4 From the list, check the subdevices you wish to delete.

Step 5 To proceed, click **Next**.

A status page appears indicating that the subdevice has been selected for deletion (see Figure 2-27).

Figure 2-27 Delete Subdevice



The following Devices have been selected for deletion.

cn=line12,ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

Step 6 To delete this subdevice, click **Delete**.

Step 7 To return to the Devices main menu, click on the **Devices** tab.

How to Query Device Inventory

You can use the Query Device Inventory feature to get a reports from devices about:

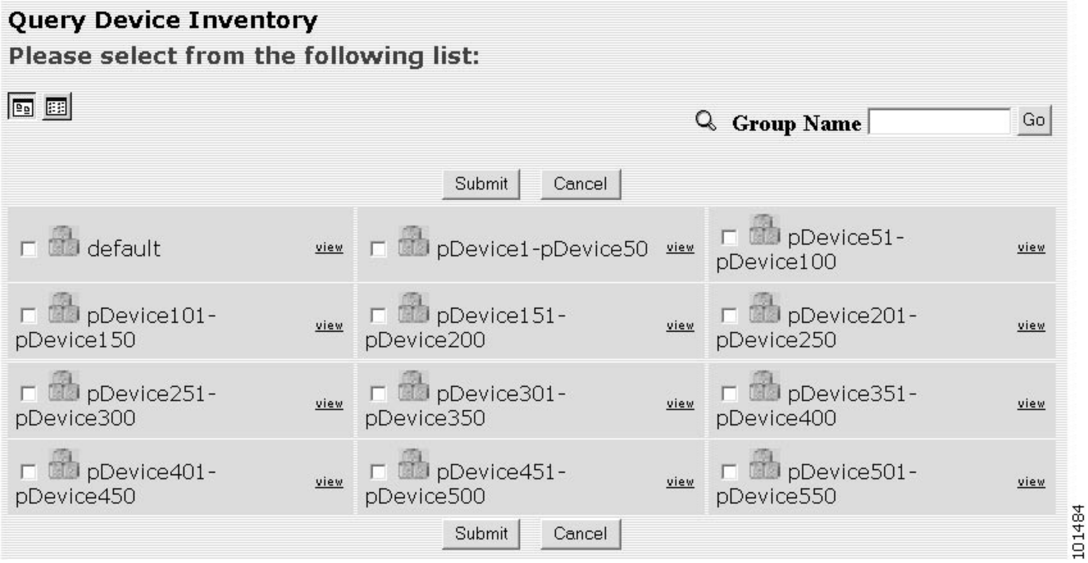
- Running image information
- Hardware information
- File system list

To query device inventory follow these steps:

Step 1 From the Devices Functional Overview page, click **Query Device Inventory**.

The Query Device Inventopry screen appears (see Figure 2-28).

Figure 2-28 Query Device Inventory



Query Device Inventory

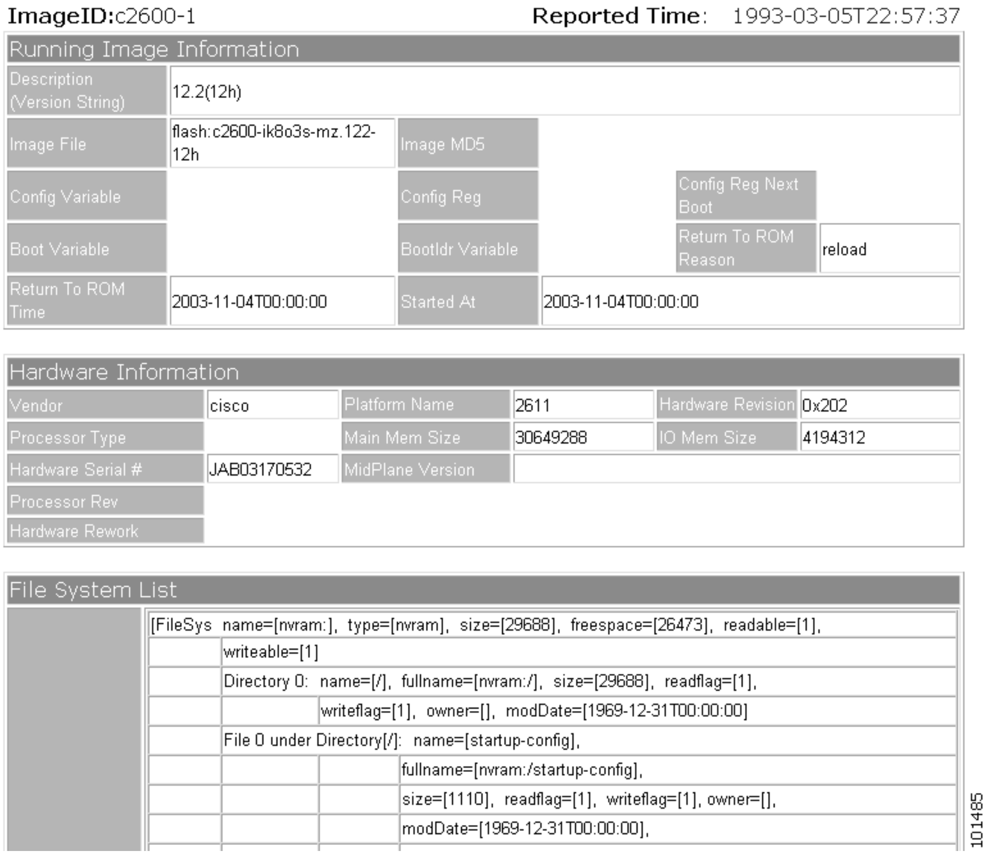
Please select from the following list:

□ default view	□ pDevice1-pDevice50 view	□ pDevice51-pDevice100 view
□ pDevice101-pDevice150 view	□ pDevice151-pDevice200 view	□ pDevice201-pDevice250 view
□ pDevice251-pDevice300 view	□ pDevice301-pDevice350 view	□ pDevice351-pDevice400 view
□ pDevice401-pDevice450 view	□ pDevice451-pDevice500 view	□ pDevice501-pDevice550 view

Step 2 Check the device(s) for which you want to get an inventory report(s), then click **Submit**.

Device inventory report(s) appear (see Figure 2-29)

Figure 2-29 Device Inventory Report



ImageID:c2600-1 Reported Time: 1993-03-05T22:57:37

Running Image Information

Description (Version String)	12.2(12h)				
Image File	flash:c2600-ik8o3s-mz.122-12h	Image MD5			
Config Variable		Config Reg		Config Reg Next Boot	
Boot Variable		Bootldr Variable		Return To ROM Reason	reload
Return To ROM Time	2003-11-04T00:00:00	Started At	2003-11-04T00:00:00		

Hardware Information

Vendor	cisco	Platform Name	2611	Hardware Revision	0x202
Processor Type		Main Mem Size	30649288	IO Mem Size	4194312
Hardware Serial #	JAB03170532	MidPlane Version			
Processor Rev					
Hardware Rework					

File System List

```
[FileSys  name=[nvram:],  type=[nvram],  size=[29688],  freespace=[26473],  readable=[1],
          writeable=[1]
          Directory 0:  name=[/],  fullname=[nvram:/],  size=[29688],  readflag=[1],
                        writeflag=[1],  owner=[],  modDate=[1969-12-31T00:00:00]
          File 0 under Directory[/]:  name=[startup-config],
                                       fullname=[nvram:/startup-config],
                                       size=[1110],  readflag=[1],  writeflag=[1], owner=[],
                                       modDate=[1969-12-31T00:00:00],
```

Step 3 To return to the Devices main menu, click on the **Devices** tab.

How to Manage User Accounts

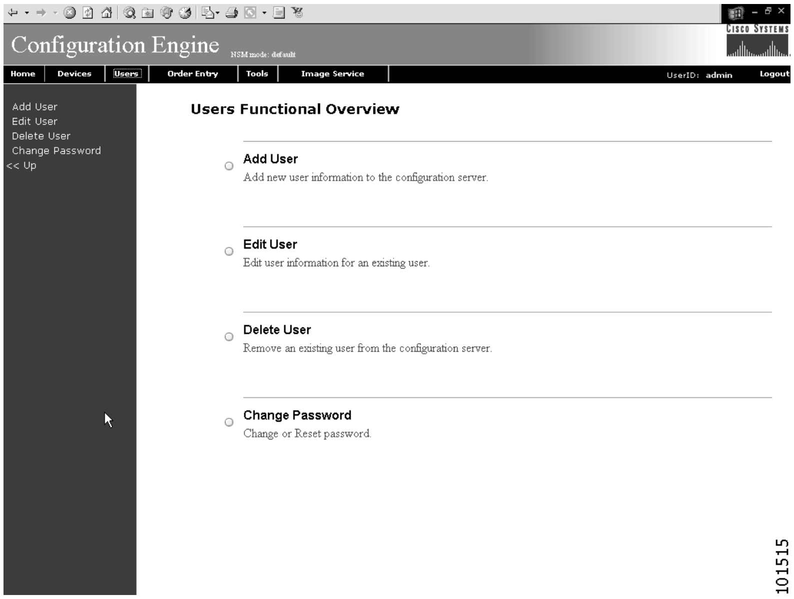
To begin managing user accounts, follow these steps:

Step 1 Login to the system (see "How to Login and Out of the System" section on page 2-1).

Step 2 From the Home page, click on the **Users** tab.

A functional overview of the user administration options appears (see Figure 2-30).

Figure 2-30 User Administration Overview



Users Functional Overview

○ Add User
Add new user information to the configuration server.

○ Edit User
Edit user information for an existing user.

○ Delete User
Remove an existing user from the configuration server.

○ Change Password
Change or Reset password.

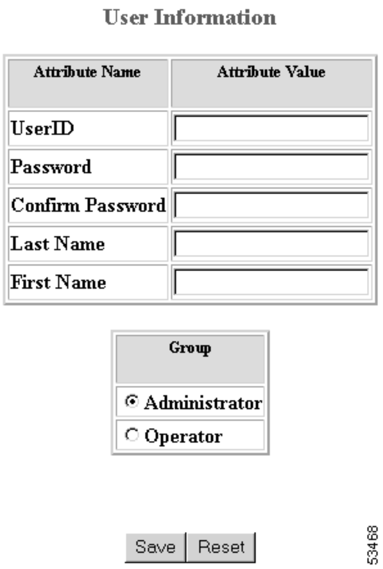
How to Add a User Account

To add a user account, follow these steps:

Step 1 From the User Administration page, click **Add User**.

The User Information dialog box appears (see Figure 2-31).

Figure 2-31 User Information



User Information

Attribute Name	Attribute Value
UserID	
Password	
Confirm Password	
Last Name	
First Name	

Group
● Administrator
○ Operator

Step 2 Enter a valid value (no spaces) in the **UserID** field.

Table 2-9 lists valid values for these fields.

Table 2-9 Valid Values for Add User Account

Attribute	Description	Valid Values
UserID	ID that allows user to login to the user interface.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Password	Password	Printable characters with a length of 6 – 12
Confirm Password	Password	Printable characters with a length of 6 – 12
Last Name	Last name of registered user.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
First Name	First name of registered user.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 Enter a password in the **Password** field.

Step 4 Confirm the password by entering it again in the **Confirm Password** field.

Step 5 Enter the user's last name in the **Last Name** field.

Step 6 Enter the user's first name in the **First Name** field.

Step 7 In the Group pane, click the radio button that classifies the privilege level (**Administrator**, **Operator**) of this user.

Step 8 To clear your entries, click **Reset**.

Step 9 To save your entries, click **Save**.

Step 10 To return to the Users main menu, click on the **Users** tab.

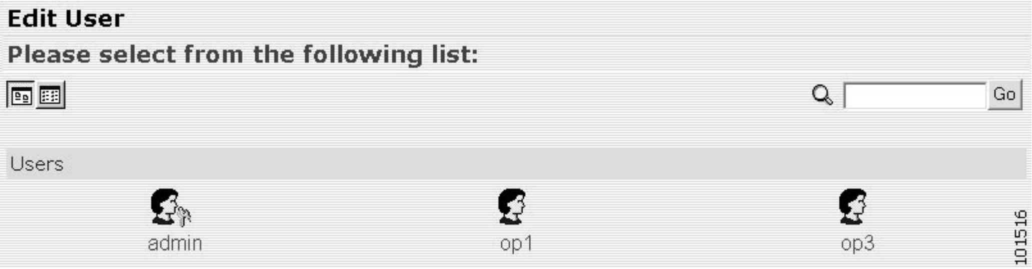
How to Edit a User Account

To edit a user account, follow these steps:

Step 1 From the User Administration page, click **Edit User**.

A list of users appears (see Figure 2-32).

Figure 2-32 User List



Edit User

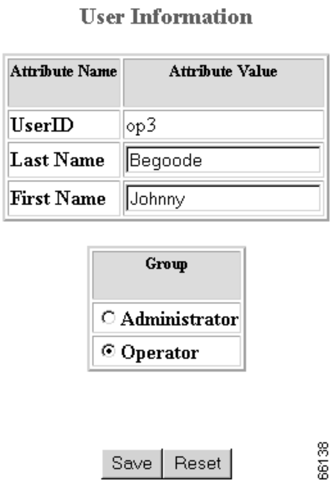
Please select from the following list:

Step 2 From the User List, click on the icon for the user account you wish to edit.

Note Administrator-level users are shown with a key icon associated with the figure icon.

The User Information page appears (see Figure 2-33).

Figure 2-33 User Information



User Information

Attribute Name	Attribute Value
UserID	op3
Last Name	Begoode
First Name	Johnny

Group
○ Administrator
● Operator

Step 3 To modify the user ID, enter a valid value (no spaces) in the **UserID** field.

Table 2-10 list valid values for these fields.

Table 2-10 Valid Values for User Information

Attribute	Description	Valid Values
UserID	ID that allows user to login to the user interface.	Information only
Password	Password	Printable characters with a length of 6 – 12
Confirm Password	Password	Printable characters with a length of 6 – 12
Group	Administrator or Operator level	Radio Button

Step 4 To modify the user's last name, edit the **Last Name** field.

Step 5 To modify the user's first name, edit the **First Name** field.

Step 6 To modify the user group status, click the appropriate radio button in the **Group** pane.

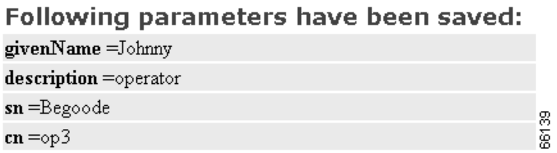
Step 7 To clear your entries, click **Reset**.

Step 8 To save your entries, click **Save**.

User information update status appears (see Figure 2-34).

Step 9 To return to the Users main menu, click on the **Users** tab.

Figure 2-34 User Information Update Status



Following parameters have been saved:

givenName =Johnny
description =operator
sn =Begoode
cn =op3

How to Delete a User Account

To delete a user account, follow these steps:

Step 1 From the User Administration page, click **Delete User**.

Step 2 From the user list (see Figure 2-32), click on the icon for the user account you wish to delete.

Step 3 To return to the Users main menu, click on the **Users** tab.

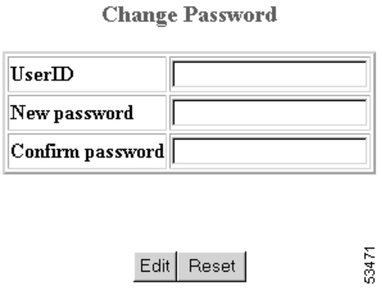
How to Change or Reset a User Password

To change or reset a user password, follow these steps:

Step 1 From the User Administration page, click **Change Password**.

The Change Password dialog box (see Figure 2-35) appears.

Figure 2-35 Change Password



Change Password

UserID	
New password	
Confirm password	

Step 2 Enter the **UserID** for the user account password you want to change or reset.

Table 2-11 lists valid values for these fields.

Table 2-11 Valid Values for Change Password by Administrator

Attribute	Description	Valid Values
UserID	ID that allows user to login to the user interface.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Password	Password	Printable characters with a length of 6 – 12
Confirm Password	Password	Printable characters with a length of 6 – 12

Step 3 Enter the new password in the **New password** field.

Step 4 Enter the new password again in the **Confirm password** field.

Step 5 To clear your entries, click **Reset**.

Step 6 To save the new password, click **Edit**.

Step 7 To return to the Users main menu, click on the **Users** tab.

How to Change Account Privilege Level

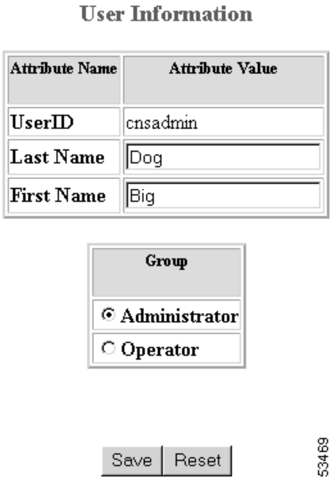
To change the privilege level of a user account, follow these steps:

Step 1 From the User Administration page, click **Edit User**.

Step 2 Choose the user in question from the user list (see Figure 2-32).

The User Information page appears (see Figure 2-36).

Figure 2-36 User Information



User Information

Attribute Name	Attribute Value
UserID	cnsadmin
Last Name	Dog
First Name	Big

Group
● Administrator
○ Operator

Step 3 In the Group pane, click the radio button that classifies the privilege level (Administrator, Operator) of this user.

Step 4 To clear your entries, click **Reset**.

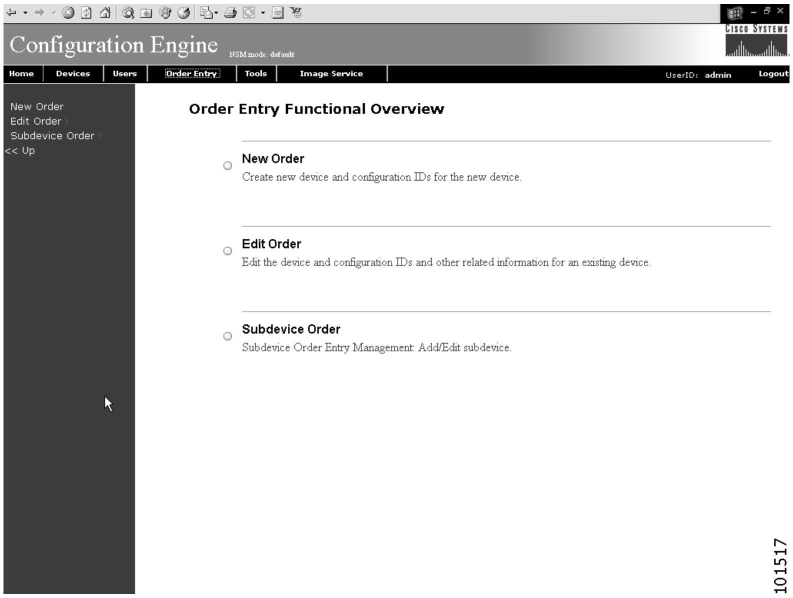
Step 5 To save your entries, click **Save**.

Step 6 To return to the Users main menu, click on the **Users** tab.

Device Configuration Order Entry

To conduct device configuration order entry tasks, from the Home page, click the **Order Entry** tab. The Order Entry page appears (see Figure 2-37).

Figure 2-37 Device Configuration Order Entry



Order Entry Functional Overview

○ **New Order**
Create new device and configuration IDs for the new device.

○ **Edit Order**
Edit the device and configuration IDs and other related information for an existing device.

○ **Subdevice Order**
Subdevice Order Entry Management: Add/Edit subdevice.

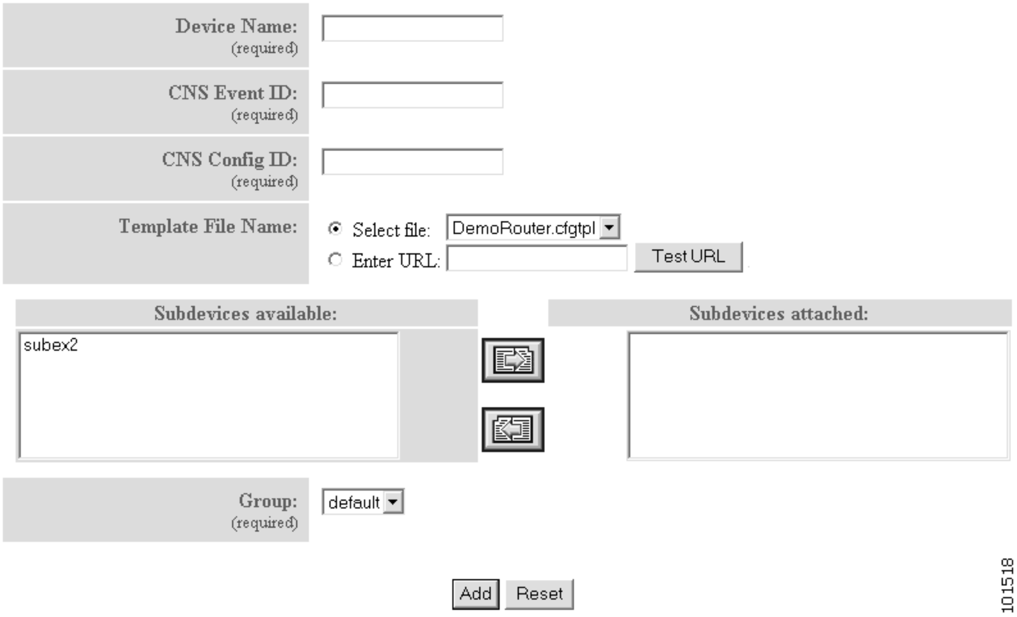
How to Enter an Order for a New Device Configuration

To enter a new device configuration order, follow these steps:

Step 1 From the Order Entry Functional Overview page, click **New Order**.

The order information dialog box appears (see Figure 2-38).

Figure 2-38 New Device Configuration Order



Device Name: (required)	
CNS Event ID: (required)	
CNS Config ID: (required)	
Template File Name:	● Select file: DemoRouter.cfgtpl ○ Enter URL: [Test URL]

Subdevices available:	Subdevices attached:
subex2	

Group: (required)	default

[Add] [Reset]

Step 2 Enter a valid value (no spaces) in the **Device Name** field.

Table 2-12 list valid values for these fields.

Table 2-12 Valid Values for Order Entry New Device

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
CNS EventID	Event ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
CNS ConfigID	Configuration ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Template File Name	Name of the configuration template to associate with the device.	From drop-down list
Subdevices Available	List of modular router subdevices available for this device.	From list
Subdevices Attached	List of modular router subdevices attached to this device.	From list
Group	Names of groups with which this device can be associated.	From drop-down list

Step 3 Enter a valid value (no spaces) in the **Event ID** field.

Step 4 Enter a valid value (no spaces) in the **Config ID** field.

Step 5 Choose a template file.

To use a template on your Cisco CNS Configuration Engine 1.4:

a. Choose **Select file**.

b. Use the drop-down menu to choose a template.

OR

To use an external template:

a. Choose **Enter URL**.

b. Enter the full URL for the server, directory, and filename where the template is stored. Currently, only **http** is supported.

c. To test access to the external template, click **Test URL**.

If the server is unavailable or the external template cannot be accessed, an error appears. You can still save this logical device, but the template is not available until you have access to the external template.

Step 6 Choose a group.

Tip Use the Group Manager under DAT (see "How to Add a Group" section on page 4-15) to set up groups before you add a device.

Step 7 To clear your entries, click **Reset**.

Step 8 To add this device, click **Add**.

Confirmation page appears.

Step 9 Click **Update Contact Information**.

Contact information page appears.

Step 10 To update contact information, fill in all applicable field.

Step 11 To clear your entries, click **Reset**.

Step 12 To continue, click **Add**.

Confirmation page appears.

Step 13 Click **Edit Parameters**.

If there are parameters in the configuration template, they appear. Otherwise, skip.

Step 14 Enter values for parameters.

Step 15 Click Apply Template.

A confirmation page appears.

Step 16 To save, but not apply, click **Save**.

Step 17 To save and apply, **Save and Apply**.

Step 18 To clear your entry, click **Reset**.

Step 19 To return to the Order Entry main menu, click on the **Order Entry** tab.

Editing an Existing Configuration Order

To edit an existing configuration order, follow these steps:

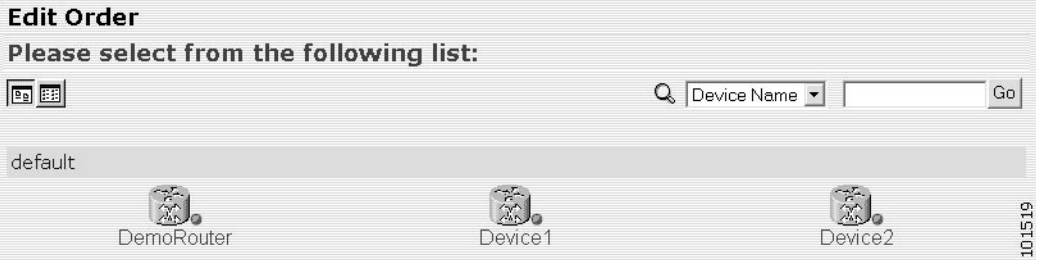
Step 1 From the Order Entry Functional Overview page, click Edit Order.

The Edit Order page appears (see Figure 2-39).

Step 2 Click on the icon for the device configuration order you wish to edit.

The device configuration order editor appears with a menu of edit functions in the left pane.

Figure 2-39 Edit Order Device List



Edit Order

Please select from the following list:

How to Edit Existing Order Information

To edit existing order information, follow these steps:

Step 1 From the Order Editor page, click Edit Information.

The order information dialog box appears.

Step 2 To modify the device name, enter a valid value (no spaces) in the **Device Name** field.

Step 3 To modify the EventID, enter a valid value (no spaces) in the **Event ID** field.

Step 4 To modify the ConfigID, enter a valid value (no spaces) in the **Config ID** field.

Step 5 To modify the template filename, choose a new template filename.

Step 6 Modify the template file as required.

Step 7 To clear your entries, click **Reset**.

Step 8 To save your edits, click **Modify**.

Step 9 To return to the Order Entry main menu, click on the **Order Entry** tab.

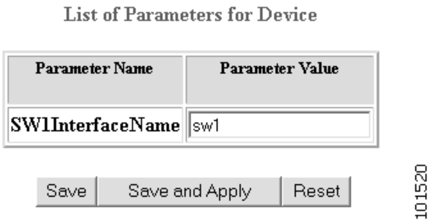
How to Edit Parameters

To edit parameter for an order, follow these steps:

Step 1 From the Order Editor page, click **Edit Parameters**.

The parameter editor appears (see Figure 2-40).

Figure 2-40 Parameter Editor



List of Parameters for Device

Parameter Name	Parameter Value
SW1InterfaceName	sw1

Step 2 Edit the value(s) of all applicable fields.

Table 2-13 list valid values for these fields.

Table 2-13 Valid Values for List of Parameters for Device

Attribute	Description	Valid Values
Parameter Name	Name of parameter set for the device	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

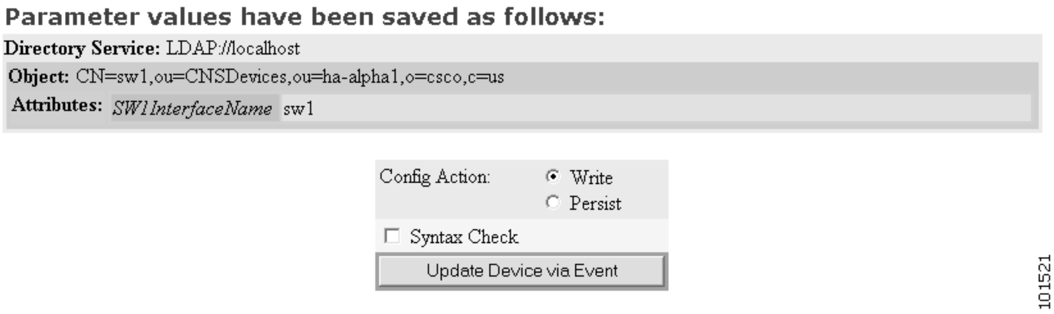
Step 3 To save, but not apply, click **Save**.

Step 4 To save and apply, **Save and Apply**.

Step 5 To clear your entry, click **Reset**.

A parameter save and apply status page appears.

Figure 2-41 Parameter Save Status



Parameter values have been saved as follows:

Directory Service: LDAP://localhost

Object: CN=sw1,ou=CNSDevices,ou=ha-alpha1,o=csco,c=us

Attributes: *SW1InterfaceName* sw1

Config Action: ● Write ○ Persist

□ Syntax Check

Step 6 Use the radio buttons to choose a Config Action, then click **Update Device via Event**.

Step 7 To return to the Order Entry main menu, click on the **Order Entry** tab.

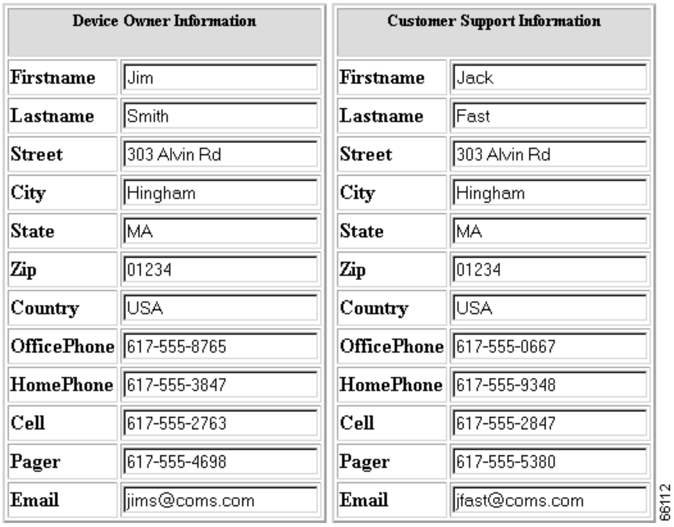
How to Edit Contact Information

To edit contact information for an existing order, follow these steps:

Step 1 From the Order Editor page, click **Edit ContactInfo**.

The contact information appears (see Figure 2-42).

Figure 2-42 Contact Information (Partial View)



Device Owner Information		Customer Support Information	
Firstname	Jim	Firstname	Jack
Lastname	Smith	Lastname	Fast
Street	303 Alvin Rd	Street	303 Alvin Rd
City	Hingham	City	Hingham
State	MA	State	MA
Zip	01234	Zip	01234
Country	USA	Country	USA
OfficePhone	617-555-8765	OfficePhone	617-555-0667
HomePhone	617-555-3847	HomePhone	617-555-9348
Cell	617-555-2763	Cell	617-555-2847
Pager	617-555-4698	Pager	617-555-5380
Email	jims@coms.com	Email	jfast@coms.com

Step 2 Edit all active fields as required.

Table 2-14 list valid values for these fields.

Table 2-14 Valid Values for Contact Information

Attribute	Description	Valid Values
All Fields	Contact information fields	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 To clear your entries, click **Reset**.

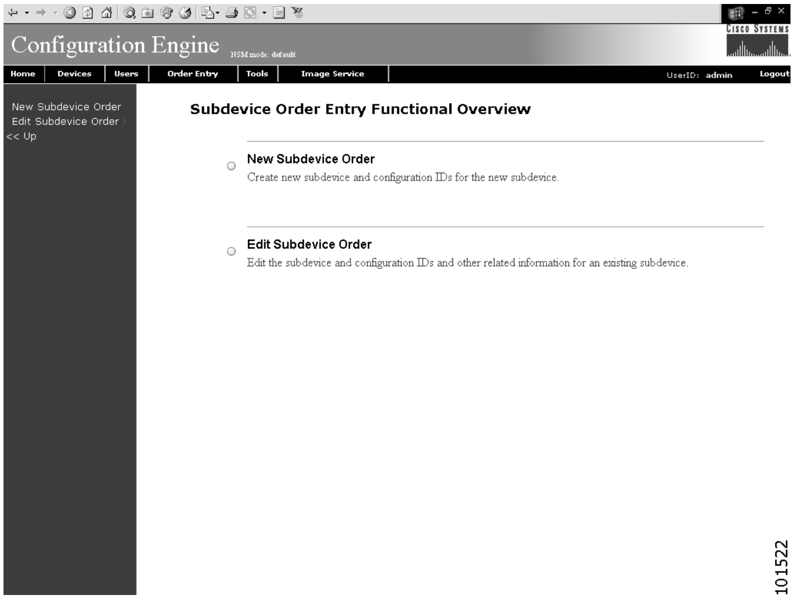
Step 4 To save your edits, click **Update**.

Step 5 To return the to the Order Entry main menu, click on the **Order Entry** tab.

Managing Subdevice Configuration Orders

To enter new subdevice configuration orders or edit existing ones, from the Order Entry page, click **Subdevice Order**. The subdevice order entry page appears (see Figure 2-43).

Figure 2-43 New Subdevice Order Entry



Subdevice Order Entry Functional Overview

○ **New Subdevice Order**
Create new subdevice and configuration IDs for the new subdevice.

○ **Edit Subdevice Order**
Edit the subdevice and configuration IDs and other related information for an existing subdevice.

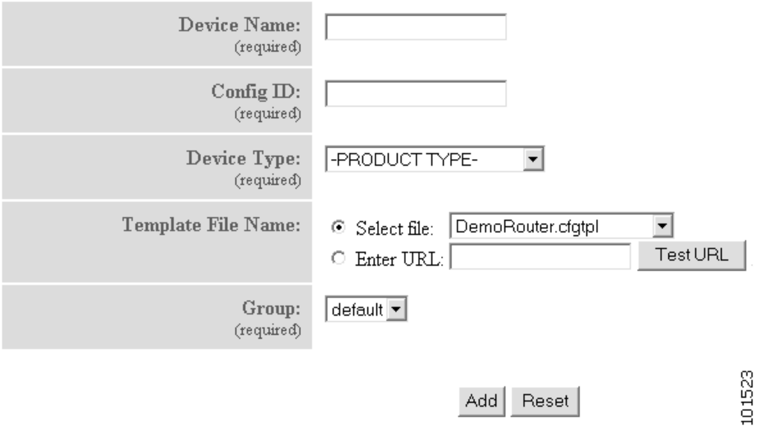
How to Enter an Order for a New Subdevice Configuration

To enter an order for a new subdevice configuration, follow these steps:

Step 1 From the Subdevice Order page, click **New Subdevice Order**.

The subdevice information page appears (see Figure 2-44).

Figure 2-44 New Subdevice Order Entry Information



Device Name: (required)	
Config ID: (required)	
Device Type: (required)	-PRODUCT TYPE-
Template File Name:	● Select file: DemoRouter.cfgtpl ○ Enter URL:
Group: (required)	default

Step 2 Enter a valid value (no spaces) in the **Device Name** field.

Table 2-15 list valid values for these fields.

Table 2-15 Valid Values for Add Subdevice

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Config ID	Unique ID of the device.	Default or a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Device Type	Type of device	From drop-down list
Template File Name	Name of the configuration template to associate with the device.	From drop-down list
Group	Group to which this subdevice belongs.	From drop-down list

Step 3 Accept the default value that appears or enter another valid value (no spaces) in the **Config ID** field.

Step 4 From the **Device Type** drop-down menu, choose the type of device to which this subdevice is associated.

Step 5 Choose a template file.

To use a template on your Cisco CNS Configuration Engine 1.4:

a. Choose **Select file**.

b. Use the drop-down list to choose a template.

OR

To use an external template:

a. Choose **Enter URL**.

b. Enter the full URL for the server, directory, and filename where the template is stored. Currently, only **http** is supported.

c. To test access to the external template, click **Test URL**.

If the server is unavailable or the external template cannot be accessed, an error appears. You can still save this logical subdevice, but the template is not available until you have access to the external template.

Step 6 Choose a group.

Step 7 To clear your entries, click **Reset**.

Step 8 To add this device, click **Add**.

Step 9 To return to the Order Entry main menu, click on the **Order Entry** tab.

How to Edit an Existing Order for a Subdevice Configuration

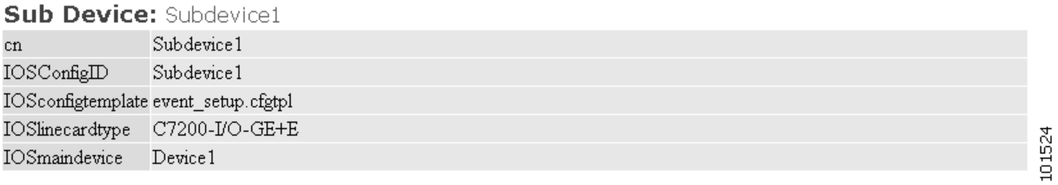
To edit an existing order for a new subdevice configuration, follow these steps:

Step 1 From the Subdevice Order page, click **Edit Subdevice Order**.

Step 2 From the Subdevice List page, click on the icon for the subdevice you wish to edit.

The subdevice configuration appears with a menu of edit functions in the left pane (see Figure 2-45).

Figure 2-45 ESubdevice Order



Sub Device: Subdevice1

cn	Subdevice1
IOSConfigID	Subdevice1
IOSconfigtemplate	event_setup.cfgtpl
IOSlinecardtype	C7200-I/O-GE+E
IOSmaindevice	Device1

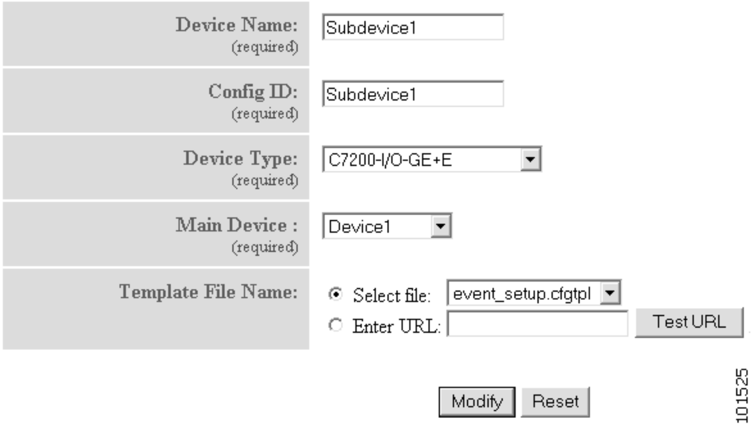
How to Edit Subdevice Information

To edit subdevice information, follow these steps:

Step 1 From the Edit Subdevice page, click **Edit Information**.

The subdevice information editor dialog box appears (see Figure 2-46).

Figure 2-46 Subdevice Information Editor



Device Name: (required)	Subdevice1
Config ID: (required)	Subdevice1
Device Type: (required)	C7200-I/O-GE+E
Main Device : (required)	Device1
Template File Name:	● Select file: event_setup.cfgtpl ○ Enter URL:

Step 2 To modify the device name, enter a valid value (no spaces) in the **Device Name** field.

Table 2-16 list valid values for these fields.

Table 2-16 Valid Values for Edit Subdevice

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Config ID	Unique ID of the device.	Default or a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Device Type	Type of device	From drop-down list
Main Device	Device in which this subdevice resides.	From drop-down list
Template File Name	Name of the configuration template to associate with the device.	From drop-down list

Step 3 To modify the ConfigID, enter a valid value (no spaces) in the **Config ID** field.

Step 4 To modify the device type, choose the appropriate device.

Step 5 To modify the template filename, choose a new template filename.

Step 6 Modify the template file as required.

Step 7 Use the Arrow buttons to modify the status of subdevices attached to this device.

Step 8 To clear your entries, click **Reset**.

Step 9 To update device information, click **Modify**.

Step 10 To return to the Order Entry main menu, click on the **Order Entry** tab.

How to Edit Subdevice Parameters

To edit subdevice parameters, follow these steps:

Step 1 From the Edit Subdevice page, click **Edit Parameter**.

The parameters editor appears.

Step 2 Modify parameters values as required.

Step 3 To save your edits, click **Save Parameters**.

Step 4 To return to the Order Entry main menu, click on the **Order Entry** tab.

How to Edit Contact Information

To edit contact information related to the physical location of a device, follow these steps:

Step 1 From the Edit Device page, click **Edit ContactInfo**.

The contact information appears.

Step 2 Edit all active fields as required.

Step 3 To clear your entries, click **Reset**.

Step 4 To save your edits, click **Update**.

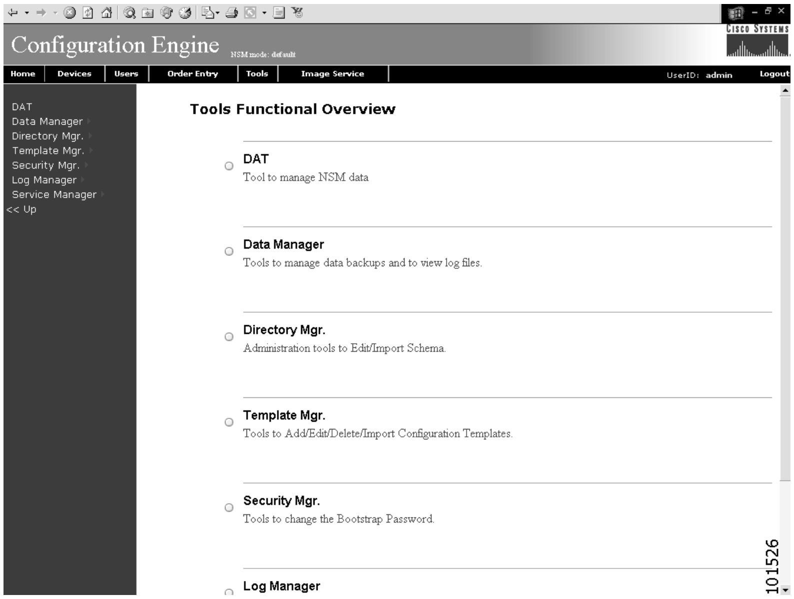
Step 5 To return the to the Order Entry main menu, click on the **Order Entry** tab.

Management Tools

To use the management tools, from the Home page, click on the Tools tab.

The Tools page appears (see Figure 2-47).

Figure 2-47 Management Tools



Tools Functional Overview

○ DAT
Tool to manage NSM data

○ Data Manager
Tools to manage data backups and to view log files.

○ Directory Mgr.
Administration tools to Edit/Import Schema.

○ Template Mgr.
Tools to Add/Edit/Delete/Import Configuration Templates.

○ Security Mgr.
Tools to change the Bootstrap Password.

○ Log Manager

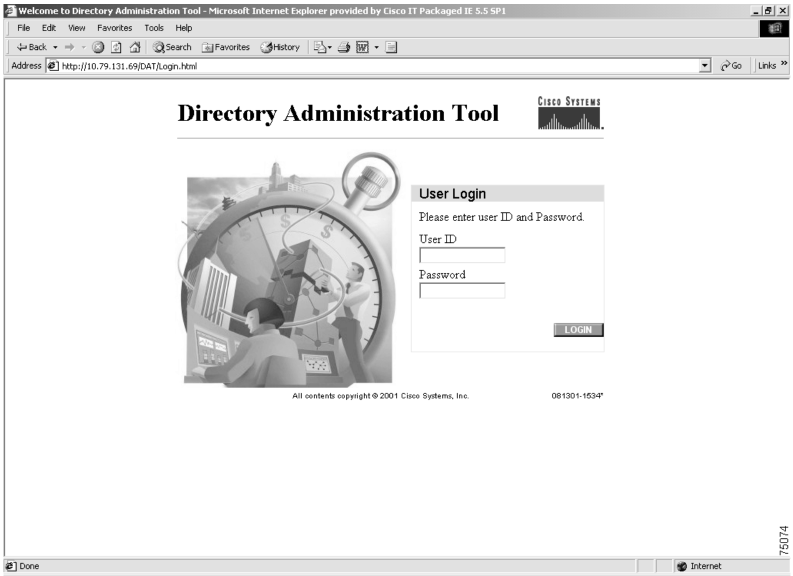
How to Use DAT

To connect to the user interface for the Directory Administration Tool (DAT), follow these steps:

Step 1 From the Tools main menu, click **DAT**.

The login window appears (see Figure 2-48).

Figure 2-48 Directory Administration Tool Login Window



Welcome to Directory Administration Tool - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
Directory Administration Tool
Cisco Systems
User Login
LOGIN
Done
Internet
75074

http://10.79.131.69/DAT/Login.html

Please enter user ID and Password.

User ID

Password

All contents copyright © 2001 Cisco Systems, Inc. 081301-1534*

Step 2 Enter your **User ID**.

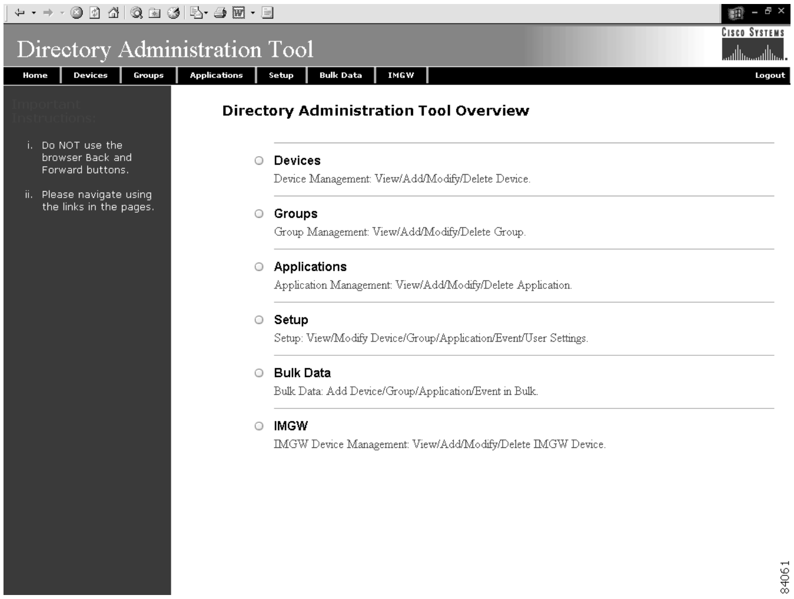
This is the LDAP proxy user name for the Cisco CNS Configuration Engine 1.4 administrative account that you entered during **Setup**.

Step 3 Enter your LDAP proxy password.

Step 4 Click **LOGIN**.

The Directory Administration Tool Overview page appears (see Figure 2-49).

Figure 2-49 DAT Home Page



Important Instructions:

i. Do NOT use the browser Back and Forward buttons.

ii. Please navigate using the links in the pages.

Directory Administration Tool Overview

○ **Devices**
Device Management: View/Add/Modify/Delete Device.

○ **Groups**
Group Management: View/Add/Modify/Delete Group.

○ **Applications**
Application Management: View/Add/Modify/Delete Application.

○ **Setup**
Setup: View/Modify Device/Group/Application/Event/User Settings.

○ **Bulk Data**
Bulk Data: Add Device/Group/Application/Event in Bulk.

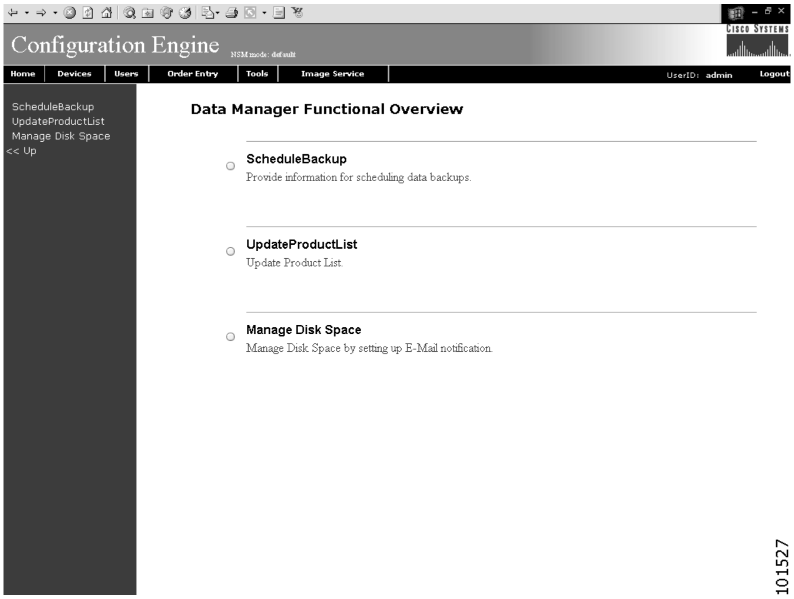
○ **IMGW**
IMGW Device Management: View/Add/Modify/Delete IMGW Device.

Step 5 From here, go to Chapter 4, “Directory Administration Tool” and follow the procedures for the tasks you want to run.

Managing Data

From the Tools page, click **Data Manager**. The Data Manager page appears (see Figure 2-50).

Figure 2-50 Data Manager



Data Manager Functional Overview

○ ScheduleBackup
Provide information for scheduling data backups.

○ UpdateProductList
Update Product List.

○ Manage Disk Space
Manage Disk Space by setting up E-Mail notification.

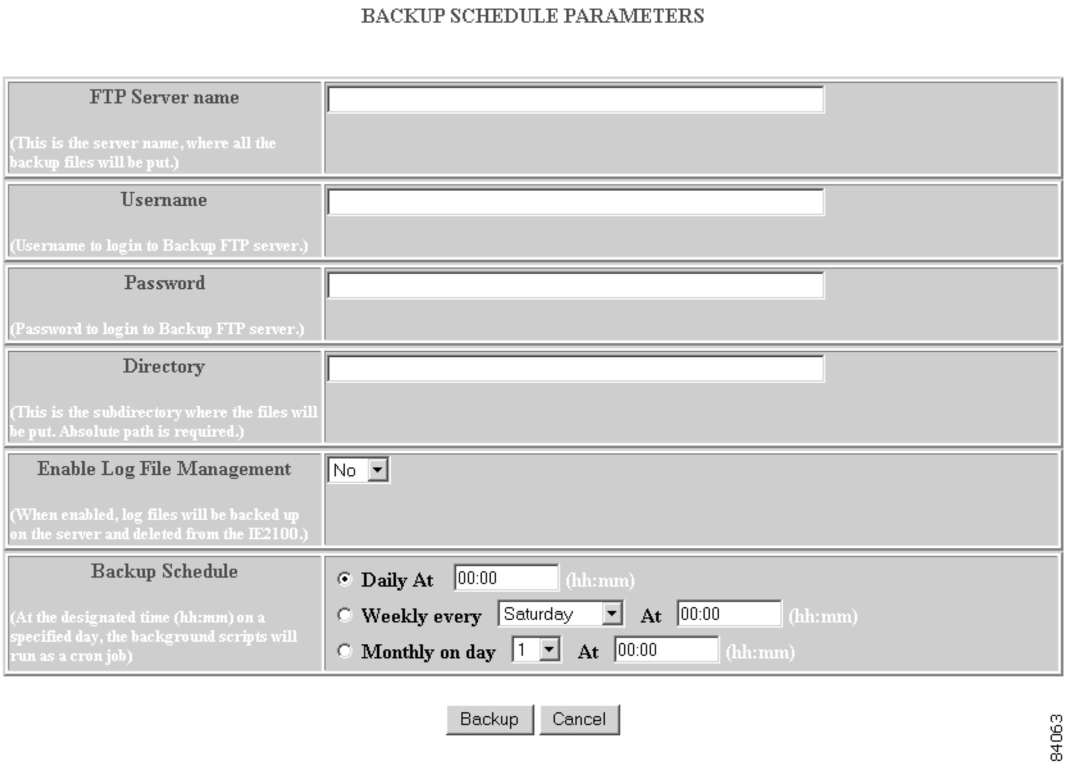
How to Schedule Data Backup

To schedule a data backup, follow these steps:

Step 1 From the Data Manager Overview page, click **ScheduleBackup**.

The backup information dialog box appears (see Figure 2-51).

Figure 2-51 Backup Schedule Parameters



BACKUP SCHEDULE PARAMETERS

FTP Server name (This is the server name, where all the backup files will be put.)	
Username (Username to login to Backup FTP server.)	
Password (Password to login to Backup FTP server.)	
Directory (This is the subdirectory where the files will be put. Absolute path is required.)	
Enable Log File Management (When enabled, log files will be backed up on the server and deleted from the IE2100.)	No
Backup Schedule (At the designated time (hh:mm) on a specified day, the background scripts will run as a cron job)	● Daily At 00:00 (hh:mm) ○ Weekly every Saturday At 00:00 (hh:mm) ○ Monthly on day 1 At 00:00 (hh:mm)

Step 2 To specify where you want the backup data to be stored, enter the FTP server name in the **FTP Server Name** field.

Table 2-17 list valid values for these fields.

Table 2-17 Valid Values for Backup Schedule Parameters

Attribute	Description	Valid Values
FTP Server name	Server name where all backup files will be put.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Username	Login username for the FTP server.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Password	Password for FTP server.	Printable characters with a length of 6 – 12
Directory	Subdirectory into which all backup files will be put.	Absolute path

Table 2-17 Valid Values for Backup Schedule Parameters (continued)

Attribute	Description	Valid Values
Enable Log File Management	determines whether files will be deleted from CNS 2100 Series system after backup.	From drop-down list
Backup Schedule	Date and time fields.	As required

Step 3 To specify the username to login to the FTP server, enter a valid username in the **Username** field.

Step 4 To specify the password to use to login to the FTP server, enter a valid value in the **Password** field.

Step 5 To specify the subdirectory where the data file is put, enter the absolute path in the **Directory** field.

Step 6 Choose whether to **Enable Log File Management**.

Step 7 To specify the backup schedule, complete the fields in the **Backup Schedule** pane.

Note The time base for the CNS 2100 Series system should be set to Coordinated Universal Time (UTC).

Step 8 To cancel the backup operation, click **Cancel**.

Step 9 To start the backup operation, click **Backup**.

Step 10 To return to the Tools main menu, click on the **Tools** tab.

For more information about backup and restore, refer to the *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*.

How to Update Product List

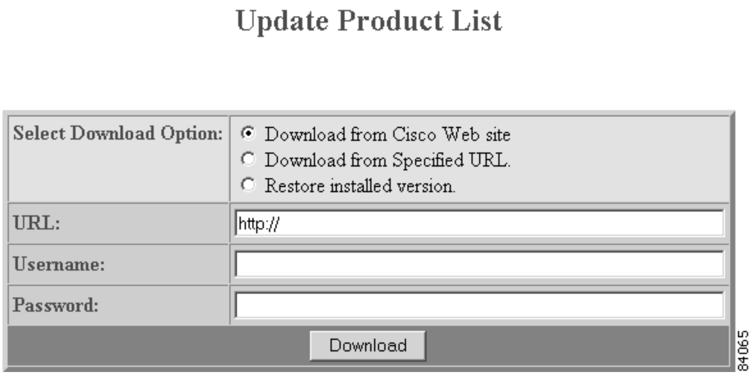
The product list is a mapping between product name of the network modules as specified in the pricing list and the numeric identification number stored in EPROM. As new products are added, this list grows and hence the need for the Cisco CNS Configuration Engine 1.4 to update this list whenever new products are added. This list can be downloaded from the Cisco web site at: http://www.cisco.com.

To update the product list, follow these steps:

Step 1 From the Data Manager page, click **Update Product List**.

The Update Product List dialog box appears (see Figure 2-52).

Figure 2-52 Update Product List



Update Product List

Select Download Option:	● Download from Cisco Web site ○ Download from Specified URL. ○ Restore installed version.
URL:	http://
Username:	
Password:	

Download

Step 2 Select the appropriate download option.

Table 2-18 list valid values for these fields.

Table 2-18 Valid Values for Update Product List

Attribute	Description	Valid Values
Select Download Option	Available download options	Radio Button
URL	Target URL	Valid URL as per RFC 1738.
Username	Your username	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Password	Your password	Printable characters with a length of 6 – 12

Step 3 Enter the target URL.

Step 4 Enter your username and password.

Step 5 To download the product list, click **Download**.

Step 6 To return to the Tools main menu, click on the **Tools** tab.

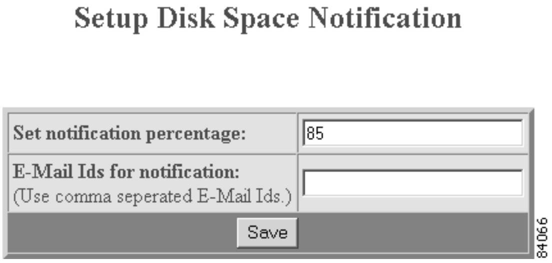
How to Manage Disk Space

To setup disk space e-mail notification of disk space usage, follow these steps:

Step 1 From the Group Manager page, click **Manage Disk Space**.

The Setup Disk Space Notification dialog box appears (see Figure 2-53).

Figure 2-53 Disk Space Notification



Setup Disk Space Notification

Set notification percentage:	85
E-Mail Ids for notification: (Use comma seperated E-Mail Ids.)	

Step 2 Set the notification percentage to the value that triggers an e-mail notification.

Table 2-19 list valid values for these fields.

Table 2-19 Valid Values for Setup Disk Space Notification

Attribute	Description	Valid Values
Set notification percentage	Notification percentage that triggers an e-mail notification.	0 – 100
E-Mail Ids for notification:	E-mail address to send notification.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 Set the appropriate e-mail address for notification e-mail.

Step 4 To save these entries, click **Save**.

Step 5 To return to the Tools main menu, click on the **Tools** tab.

How to Manage Directory Content

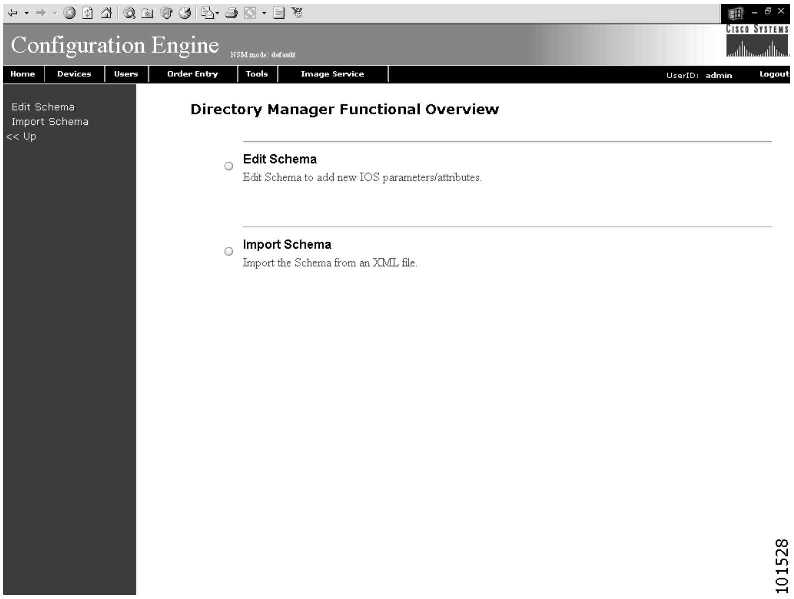
With the directory manager you can:

- Edit the schema
- Import a schema from an XML file

To use the directory manager tool, click **Directory Mgr**.

The Directory Manager page appears (see Figure 2-54).

Figure 2-54 Directory Manager



Directory Manager Functional Overview

○ **Edit Schema**
Edit Schema to add new IOS parameters/attributes.

○ **Import Schema**
Import the Schema from an XML file.

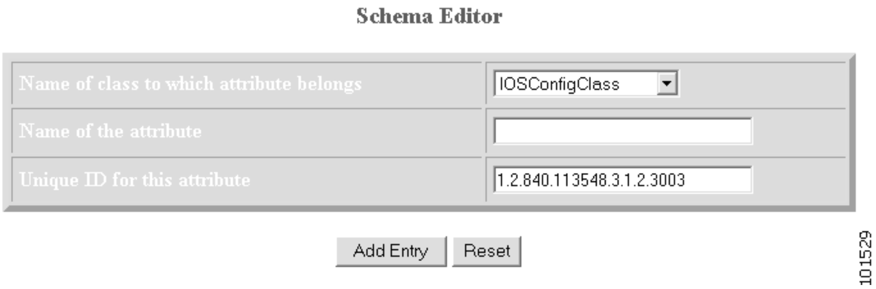
How to Edit the Schema

To edit the schema, follow these steps:

Step 1 From the Directory Manager page, click **Edit Schema**.

The schema editor appears (see Figure 2-55).

Figure 2-55 Schema Editor



Schema Editor

Name of class to which attribute belongs	IOSConfigClass
Name of the attribute	
Unique ID for this attribute	1.2.840.113548.3.1.2.3003

Step 2 From drop-down list, select name of class to which attribute belongs.

Table 2-20 list valid values for these fields.

Table 2-20 Valid Values for Schema Editor

Attribute	Description	Valid Values
Name of class to which attribute belongs	Class name to which attribute belongs	From drop-down list
Name of the attribute	Name of the attribute	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Unique ID for this attribute	Unique ID for this attribute	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 Enter the name of the new attribute

Step 4 Accept or modify the **Unique ID** for this attribute.

Step 5 To clear your entries, click **Reset**.

Step 6 To add this attribute to the schema, click **Add Entry**.

Step 7 To return to the Tools main menu, click on the **Tools** tab.

How to Import Schema

You can import a schema accessible from your computer. However, the file must be in XML format and conform to the definitions specified in the document type definition (DTD) file shown here:

```
<!-- DTD for DAML             -->
<!-- Last updated: 2000-10-03 -->

<!ELEMENT daml (schema)>

<!-- SCHEMA -->
<!ELEMENT schema (class+,attribute-type+,link*)>

<!-- element types common to class and attribute-type -->

<!ELEMENT class (auxclass*,attribute+)>
<!ATTLIST class
  name      (#PCDATA)    #REQUIRED
  id        ID           #IMPLIED
  superior  IDREF    #IMPLIED
  type      (structural|abstract|auxiliary)  #REQUIRED
  description? #IMPLIED
>

<!ELEMENT auxclass EMPTY>
<!ATTLIST auxclass
  ref  IDREF        #REQUIRED
>
```

```
<!ELEMENT attribute EMPTY>
<!ATTLIST attribute
  ref       IDREF  #REQUIRED
  required  (true|false)  #REQUIRED
>

<!ELEMENT attribute-type EMPTY>
<!ATTLIST attribute-type
  name              (#PCDATA) #REQUIRED
  id                ID        #REQUIRED
  single-value      (true|false) "false"
  syntax            (string|integer|boolean|binary|key) "string"
>

<!ELEMENT link EMPTY>
<!ATTLIST link
  fromclass     IDREF         #REQUIRED
  fromattr      IDREF         #REQUIRED
  toclass       IDREF         #REQUIRED
  toattr        IDREF         #REQUIRED
>
```

For example, a valid schema would look like:

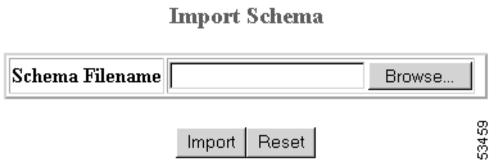
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE dsml SYSTEM "dsml.dtd">
<dsml complete="true">
  <directory-schema>
   <attribute-type id="IOSe1ipaddress" single-value="true" obsolete="false"
user-modification="true">
     <name>IOSe1ipaddress</name>
     <object-identifier>1.2.840.113548.3.1.2.20</object-identifier>
     <syntax>string</syntax>
   </attribute-type>
   <class id="IOSConfigClass" superior="top" type="structural" obsolete="false">
     <name>IOSConfigClass</name>
     <object-identifier>1.2.840.113548.3.2.2.1</object-identifier>
     <attribute ref="1.2.840.113548.3.1.2.20" required="false"/>
   </class>
  </directory-schema>
</dsml>
```

To import a schema from an XML file accessible from your computer, follow these steps:

Step 1 From the Directory Manager page, click **Import Schema**.

The import schema dialog box appears (see Figure 2-56).

Figure 2-56 Import Schema



Step 2 Enter the filename of the schema you want to import in the **Schema Filename** field.

Table 2-21 list valid values for these fields.

Table 2-21 Valid Values for Import Schema

Attribute	Description	Valid Values
Schema Filename	Name of schema file to import.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Use the browse function to locate the file, if needed.

Step 3 To clear your entries, click **Reset**.

Step 4 To import the file, click **Import**.

Step 5 To return to the Tools main menu, click on the **Tools** tab.

Templates and Template Management

When creating a template, it is possible to specify variables that will be contextually substituted. Many of these variables are available in the drop-down menu in the Template Editor (see Figure 2-60). It is also possible to create these files offline without the Template Editor and still use these variables.

The basic format of a template file is simply the text of the configuration to be downloaded to your device (see “Sample Template” section on page 2-57). However, you can put variable substitutions of the following form (for example, the variable name could be *iosipaddress*):

```
Internal directory mode:
   ${LDAP://this:attrName=iosipaddress}
External directory mode:
   ${LDAP://10.1.2.3/cn=Device1,ou=CNSDevices,o=cisco,c=us:attrName=iosipaddress}
```

It is possible to create segments of templates that can be included in other templates. For example, you might have an Ethernet configuration that would be used by multiple devices. In each device template, you could have:

```
#include /opt/CSCOcnsie/Templates/ethernet_setup.cfgtpl
```

Now, you could centralize all the administration for Ethernet configuration in one file.

Caution Circular includes of template files are not allowed.

Sample Template

The following sample is the configuration template for the DemoRouter (*DemoRouter.cfgtpl*), which is pre-loaded on your system:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname DemoRouter
!
boot system flash c7200-is-mz
enable secret 5 $1$cMdI$.e37TH540MWB2GW5gMOn3/
enable password cisco
!
ip subnet-zero
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
 half-duplex
!
interface Ethernet1/0
 ip address 10.10.1.1 255.255.255.240
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Ethernet1/2
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Ethernet1/3
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.1.1
ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Configuration Control Templates

To restart a device with a new image, you need Configuration Control templates that contain the required CLI commands for image activation on particular devices.

For example, if you want to restart a Cisco 3600 Series router with an image named *3600.image*, from the device console, you would issue the following CLI commands:

no boot system
boot system flash:3600.image

The content of the Configuration Control template for image activation should contain the CLI commands that you would normally enter from the device console to activate a new image on the device.

Templates for Modular Routers

The template mechanism for the devices has been enhanced to support modular routers. A modular router chassis includes slots in which you can install modules. You can install any module into any available slot in the chassis. Some modules like 2 Ethernet 2 WAN card slot module can in turn have sub slots to install interface cards or line cards. Device management has been extended to support subdevices representing line cards.

Additional attributes representing line card number, line card type, and subdevices have been added to the existing device object structure in the directory server in order to have the same structure to represent the main device or the subdevice.

Currently, card type is a string that maps to the product code of the network module. Since the EPROM data in the card stores part numbers only, not product codes, the part numbers are mapped to product codes. The user uses part numbers and the configuration server maps part number to product codes.

In the context of main device, the line card number and line card type fields make no sense and hence are set to NULL value. The subdevices field in the sub device (representing the line card) is set to NULL value.

New interface variable support has been added. These variables are included in the templates, which are parameterize with the interface numbers in the template. These are not attributes. They are special format variables that are replaced by the configuration server based on the interface information, which comes from the device. These variables only specify the relative position of the interface on the module and are replaced by the actual slot number, shelf-ID or port number. The interface variables are wrapped in percent sign (%) characters and specify the type, if any, and the relative position. The configuration server replaces these variables with the interface numbers. The interface type still has to be specified in the CLI using the following syntax:

Interface Variable = %[InterfaceType] RelativePosition%

For example:

%FastEthernet 0% for interface FastEthernet

%Serial 0% interface Serial

%T1 0% controller T1

%E1 0% controller E1

%voice-port 0% voice-port

Example 1:

A network module with two FastEthernet ports plugged in Slot 2 would be referred in the configuration CLI as FastEthernet 2/0 and FastEthernet 2/1 and referred in the template as FastEthernet %FastEthernet 0% and FastEthernet %FastEthernet 1%:

```
!
interface FatsEthernet 2/0
    ip address 10.10.1.1 255.255.255.0
!
interface FatsEthernet 2/1
    ip address 20.20.1.1 255.255.255.0
!
```

Templates for these CLIs would be:

```
!
interface FastEthernet %FastEthernet 0%
    ip address 10.10.1.1 255.255.255.0
!
interface FastEthernet %FastEthernet 1%
    ip address 20.20.1.1 255.255.255.0
!
```

Example 2 (Voice card with two ports plugged in slot 3):

```
!
voice-port 3/0/0
    description 4082224444
!
voice-port 3/0/0
    description 4082225555
!
```

Templates for these CLIs would be:

```
!
voice-port  %voice-port 0%
    description 4082224444
!
voice-port %voice-port 1%
    description 4082225555
!
```

The main device template does not include links to the subdevice templates. The subdevice templates are appended to the main device template. The line card number are a parameter in the subdevice templates.

All the CLI commands which reference a line card interface are specified in the subdevice template for that line card. This implies that any command in the global configuration mode, or otherwise, that refers to a particular line card interface is in the template for that subdevice (line card) and not in the main device template.

Only the CLI commands in the global configuration mode, and not pertaining to the any specific interface, are specified in the main device template.

The port number and channel number are not be template parameters since these are fixed for a given line card. The network administrator can configure specific channels on the interfaces by explicitly specifying the channels in the subdevice templates.

For example:

interface Serial %Serial 0%:0

Sample Templates for Modular Router

The names of the attributes for slot, slot-unit, line card type and so forth, are used for demonstration purposes.

Main Device Template

```
!
version 12.2
no parser cache
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2600
!
logging rate-limit console 10 except errors
!
memory-size iomem 25
ip subnet-zero
!
!
!
no ip dhcp-client network-discovery
lcp max-session-starts 0
!
ip classless
no ip http server
!
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login
line vty 5 15
 login
!
```

Fastethernet Template

```
Interface FastEthernet %FastEthernet 0%

ip address 10.0.0.1 255.0.0.0
shutdown
speed auto
```

Voice-port Template

```
voice-port  %voice-port 0%
playout-delay mode adaptive
!
voice-port %voice-port 1%
!
dial-peer voice 10 pots
destination-pattern 200
port %voice-port 0%
forward-digits all


voice-port  %voice-port 0%
!
dial-peer voice 20 pots
destination-pattern 100
port %voice-port 0%
!
voice-port  %voice-port 1%
```

Modular Router Events

Modular router events are published to the event bus and are accessible to applications connected to the bus. The IOS device publishes the system hardware configuration in the *cisco.cns.config.device-details* event after hardware discovery. The Cisco CNS Configuration Engine 1.4 is configured to listen for this event, retrieve it and extract the hardware configuration of the device.

Following is the DTD of the *cisco.cns.config.device-details* event that the Cisco IOS device sends:

```
    <!ELEMENT device-details (config-id, connect-interface?, card-info*>
    <!ELEMENT config-id (#PCDATA)>
    <!ELEMENT connect-interface (#PCDATA)>
    <!ELEMENT card-info (card-info+)>
    <!ELEMENT card-info
(card-type,card-desc?,slot,daughter?,serial-number,part-number,hw-version?,board-revision?
,ports?,controller?,rma-number?,test-history?,eeprom-version?,eeprom-data?,interface?,cont
roller?,voice-port?)>
    <!ELEMENT card-type (#PCDATA)>
    <!ELEMENT card-desc (#PCDATA)>
    <!ELEMENT slot (#PCDATA)>
    <!ELEMENT daughter (#PCDATA)>
    <!ELEMENT serial-number (#PCDATA)>
    <!ELEMENT part-number (#PCDATA)>
    <!ELEMENT hw-version (#PCDATA)>
    <!ELEMENT board-revision (#PCDATA)>
    <!ELEMENT ports (#PCDATA)>
    <!ELEMENT controller (#PCDATA)>
    <!ELEMENT rma-number (#PCDATA)>
    <!ELEMENT test-history (#PCDATA)>
    <!ELEMENT eeprom-version (#PCDATA)>
    <!ELEMENT eeprom-data (#PCDATA)>
    <!ELEMENT interface (#PCDATA)>
    <!ELEMENT controller (#PCDATA)>
```

```
<!ELEMENT voice-port (#PCDATA)>
```

Dynamic Templates

There may be times when the actual contents of a template needs to be dynamically generated. To do this, you would use the **#call** mechanism. This executes a JavaScript program whose output becomes part of the template. The program is re-executed each time a device asks for the template.

For example, you might want to distribute the load across the various event gateway processes without permanently assigning a device to a particular event gateway. This is useful because of the limit of 500 devices per event gateway daemon instance.

Let us take the following template as an example:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname DemoRouter
#call /opt/CSCOcnsie/Templates/event_setup.js
```

Here is an example of an *event_setup.js* that one might use:

```
/*
 * An instance of Event Gateway resides on every odd port from 11011 to 11031.
 * This will choose a random one in this range so that devices are spread out
 * evenly among the various ports. Adjust the IP address in the println
 * statement to be the address of the IE2100 itself.
 */
var port = Math.floor(Math.random() * 11) * 2 + 11011;
println("cns event 10.1.6.131 " + port.toString());
```

The result of this combination would be a template that appears as follows:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname DemoRouter
cns event 10.1.6.131 11017
```

The last line is programmatically determined and recalculated every time the template is requested by the device. So the next time a device requests this template, the last line might be:

```
cns event 10.1.6.131 11023
```

Simple modifications to *event_setup.js* could even be used to distribute devices across multiple CNS 2100 Series devices (by dynamically generating the IP address). It could also be used to affect any part of the device configuration—be it DNS servers or routing tables. Anything that is printed out by the JavaScript program becomes a dynamic part of the template.

Control Structures

The configuration template can include simple control structures such as, *if*, *else* and *elseif*. By using these control structures, the user can include or exclude a block of CLI commands based on a parameter stored in the directory.

The syntax for these # preprocessing control structures is as follows:

Syntax Description

#if <*URL*> = *constant*

cli-command(s)

#elseif <*URL*> = *constant*

cli-command(s)

#else

cli-command(s)

#endif

Where *constant* is an integer, boolean or a string in single quotes and the <*URL*> is a URL pointing to an attribute in the Directory or Database.

Note Nested **#if** and **#elseif** is NOT supported.

Usage Guidelines

The configuration template can include **#define** entries to define short names for long URLs.

The syntax for the **#define** preprocessing command is as follows

#define *definition-name* <*URL*> | *constant*

where <*URL*> is a reference to an attribute in the directory.

The configuration template can contain another # preprocessing command **#include,** which allows the inclusion of other configuration templates or the results of an ASP page.

The syntax for the # preprocessing command is as follows:

#include <*URL*> | '<*Filename*>' | <*Filename*>

Whenever an **#include** directive is encountered, it is replaced by the content of the file.

The following configuration template sample includes either IP sub-template or ISDN sub-template based on the value of the parameter protocol in the directory or database.

Examples

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ${LDAP://this:attrName=IOShostname}
#if ${LDAP://this:attrName=IOSIPprotocol} = true then
    #include ${LDAP://this:attrName=IPsubTemplate}
```

```
#else
    #include ${LDAP://this:attrName=ISDNsubTemplate}
#endif
```

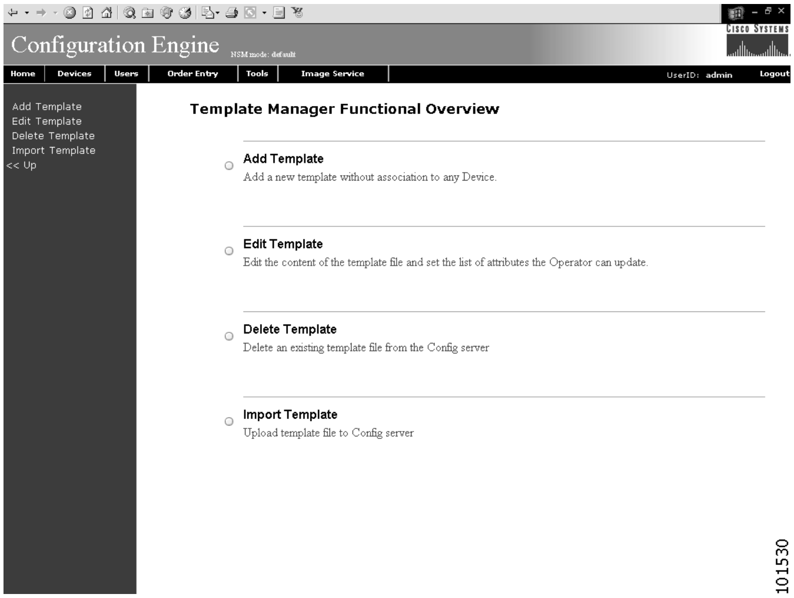
The parameter, `${LDAP://this:attrName=IPsubTemplate}` contains the location of the file.

How to Manage Templates

To use the template manager tool, click **Template Mgr**.

The Template Manager page appears (see Figure 2-57).

Figure 2-57 Template Manager



Template Manager Functional Overview

○ **Add Template**
Add a new template without association to any Device.

○ **Edit Template**
Edit the content of the template file and set the list of attributes the Operator can update.

○ **Delete Template**
Delete an existing template file from the Config server

○ **Import Template**
Upload template file to Config server

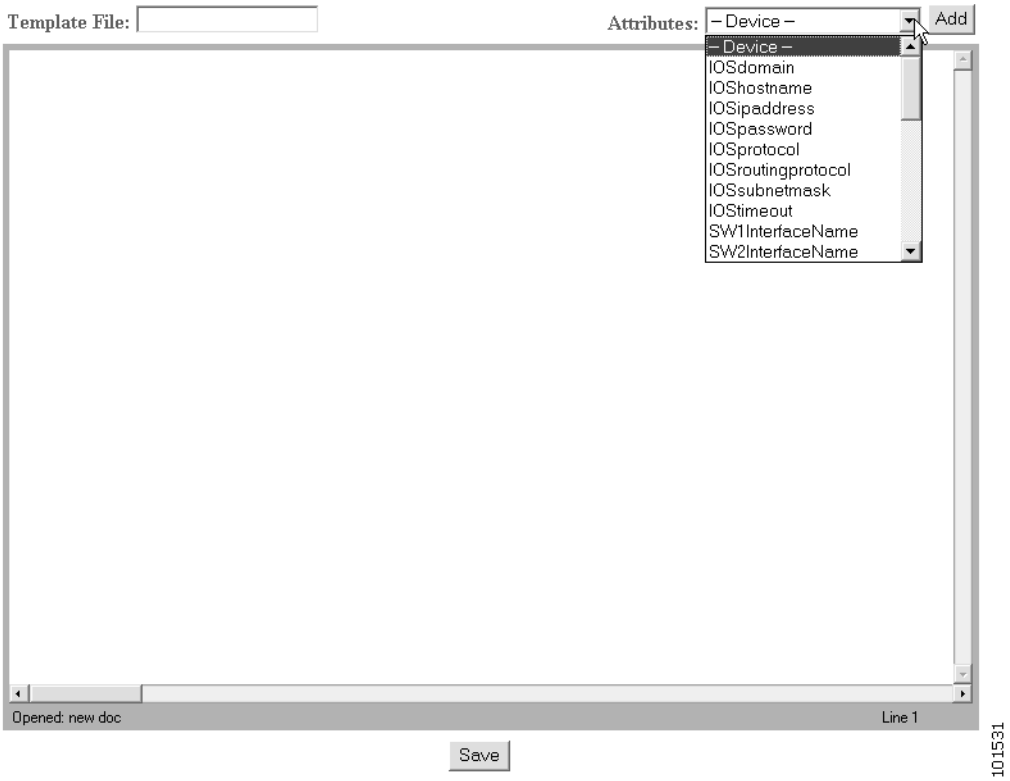
How to Add a Template

To add a template to the directory, follow these steps:

Step 1 From the Template Manager page, click **Add Template**.

A blank template page appears (see Figure 2-58).

Figure 2-58 Add Template



Step 2 Enter the filename for this template in the **Template File** field.

Table 2-22 list valid values for these fields.

Table 2-22 Valid Values for Add Template

Attribute	Description	Valid Values
Template File	Filename of template	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Attributes	Available attributes	From drop-down list

Step 3 To choose the attributes you want to be included in this template, use the **Attributes** menu.

Step 4 To save your entries, click **Save**.

Step 5 To return to the Tools main menu, click on the **Tools** tab.

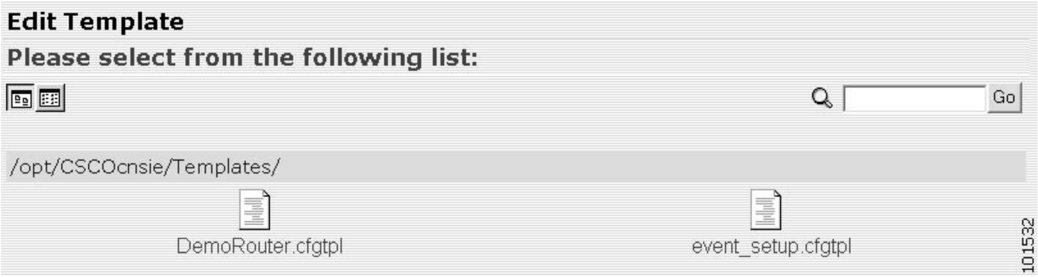
How to Edit a Template

To edit parameters (attribute information) and the content of a template, follow these steps:

Step 1 From the Template Manager page, click **Edit Template**.

The Edit Template list appears (see Figure 2-59).

Figure 2-59 Edit Template List



Edit Template

Please select from the following list:

/opt/CSCOcnsie/Templates/

DemoRouter.cfgtpl

event_setup.cfgtpl

Step 2 Click on the icon for the template file you wish to edit.

The template file appears.

Step 3 To edit parameters (attribute information), follow these steps:

a. From the template file page, click **Edit AttributeInfo**.

b. Edit the desired parameter fields.

Only selected (see check box) parameters appear in Order Entry.

The Display Name and Default Value appear when an operator edits parameters by means of Order Entry.

c. To clear your entries, click **Reset**.

d. To save your changes, click **Save**.

Step 4 To save and apply, **Save and Apply**.

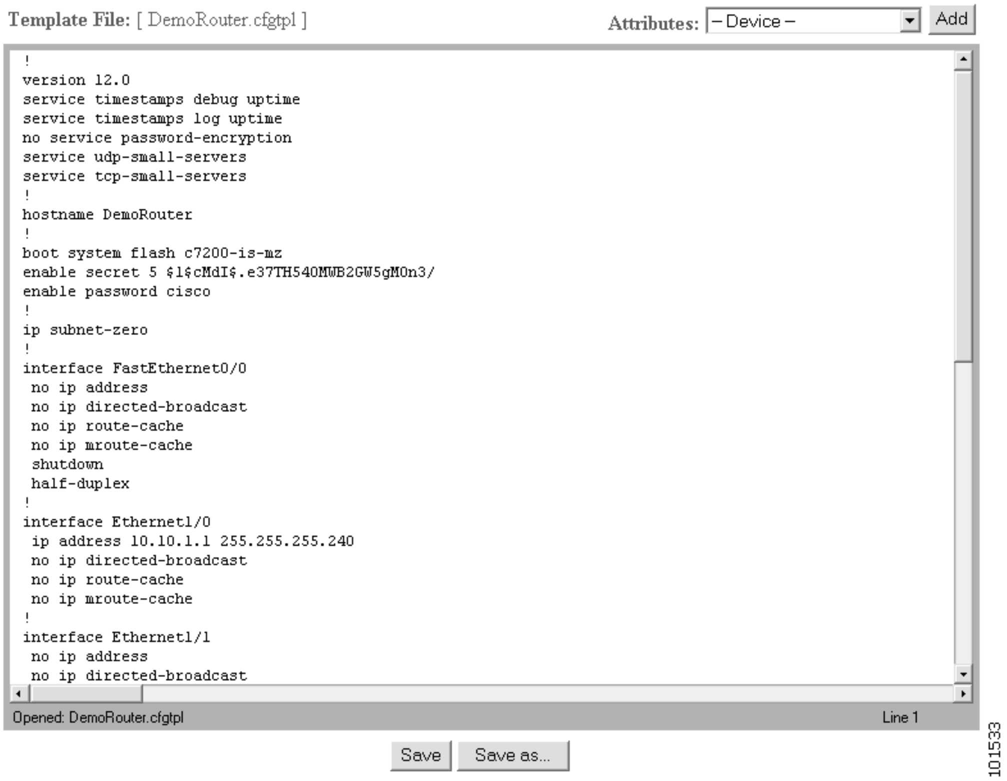
e. To return to the Tools main menu, click on the **Tools** tab.

Step 5 To edit template content, follow these steps:

a. To edit the content of a template, from the template file page, click **Edit Content**.

The template content appears (see Figure 2-60).

Figure 2-60 Template Content



Template File: [DemoRouter.cfgtpl]
Attributes: – Device –
Add
Opened: DemoRouter.cfgtpl
Line 1
Save
Save as...
101533

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname DemoRouter
!
boot system flash c7200-is-mz
enable secret 5 $1$cMdI$.e37TH540MWB2GW5gM0n3/
enable password cisco
!
ip subnet-zero
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
 half-duplex
!
interface Ethernet1/0
 ip address 10.10.1.1 255.255.255.240
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/1
 no ip address
 no ip directed-broadcast
```

b. Edit the content by adding or deleting attributes.

c. To save your edits, click **Save**.

d. To save as a new template, click **Save as**.

e. To return to the Tools main menu, click on the **Tools** tab.

How to Delete a Template

To delete a template, follow these steps:

Step 1 From the Template Manager page, click **Delete Template**.

The template file list appears.

Step 2 Select the template you wish to delete.

Step 3 Delete the desired template file.

Step 4 To return to the Tools main menu, click on the **Tools** tab.

How to Import a Template

To import a template file to the configuration server from another location, follow these steps:

Step 1 From the Template Manager page, click **Import Template**.

Step 2 In the dialog box that appears, enter the name of the template file in the **Filename** field, if known, or browse your directory tree to choose the filename you desire.

Step 3 To clear the field, click **Reset**.

Step 4 To upload the template file, click **Upload**.

Step 5 To return to the Tools main menu, click on the **Tools** tab.

Security Manager

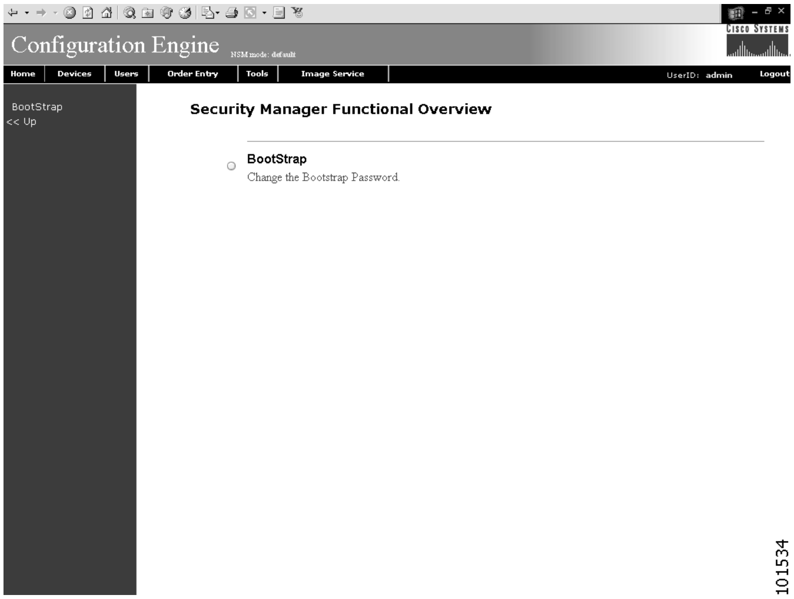
With the security manager tool you can change the bootstrap password.

The bootstrap password is used to authenticate a Cisco IOS device before it connects to the Event Gateway. For additional information see “Authentication settings” section on page 2-7)

To use the security manager tool, from the Tools page, click **Security Mgr**.

The Security Manager page appears (see Figure 2-61).

Figure 2-61 Security Manager



Security Manager Functional Overview

○ BootStrap
Change the Bootstrap Password.

How to Change Bootstrap Password

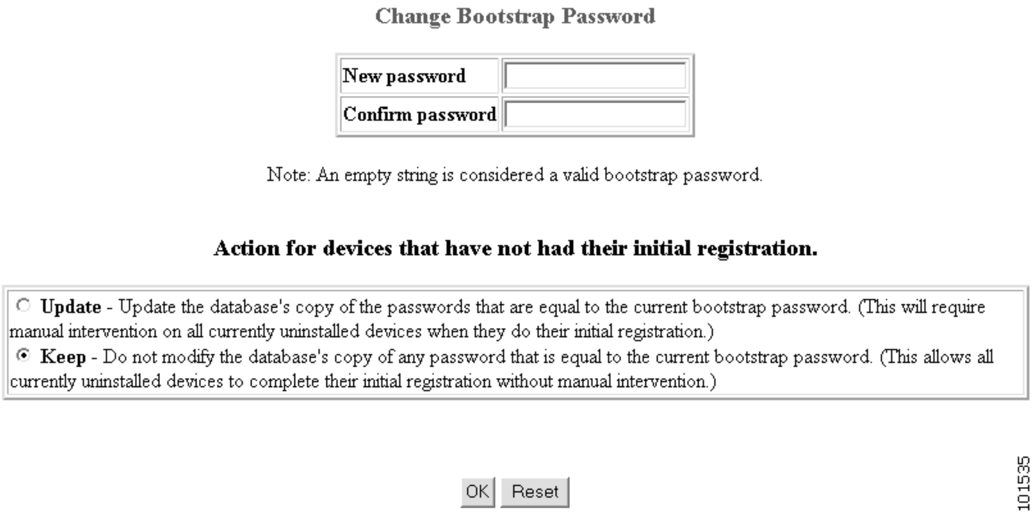
The bootstrap password is used where multiple devices are deployed in a batch. In this case, all devices in a particular batch are given the same (bootstrap) password to use when they each start up on the network for the first time. The bootstrap password can be changed for different batches of devices by using the Security Manager.

To change the bootstrap password, follow these steps:

Step 1 From the Security Management page, click **BootStrap**.

The Change Bootstrap Password page appears (see Figure 2-62).

Figure 2-62 Change Bootstrap Password



Change Bootstrap Password

New password	
Confirm password	

Note: An empty string is considered a valid bootstrap password.

Action for devices that have not had their initial registration.

○ **Update** - Update the database's copy of the passwords that are equal to the current bootstrap password. (This will require manual intervention on all currently uninstalled devices when they do their initial registration.)

● **Keep** - Do not modify the database's copy of any password that is equal to the current bootstrap password. (This allows all currently uninstalled devices to complete their initial registration without manual intervention.)

Step 2 In the password dialog box, enter the new password.

Table 2-23 list valid values for these fields.

Table 2-23 Valid Values for Change Bootstrap Password

Attribute	Description	Valid Values
New password	Bootstrap password	Printable characters with a length of 6 – 12
Confirm password	Bootstrap password	Printable characters with a length of 6 – 12
Update	Modifies the database copy of the password that is equal to the current bootstrap password. This will require manual intervention on all currently uninstalled devices when they do their initial registration.	Radio button
Keep	Does not modify the database copy of any password that is equal to the current bootstrap password. This allows all currently uninstalled devices to complete their initial registration without manual intervention.	Radio button

Step 3 Confirm the new password.

Step 4 Choose (**Keep**, **Update** radio buttons) the subsequent action to the database regarding any password that is equal to the bootstrap password.

Step 5 To clear all entries, click **Reset**.

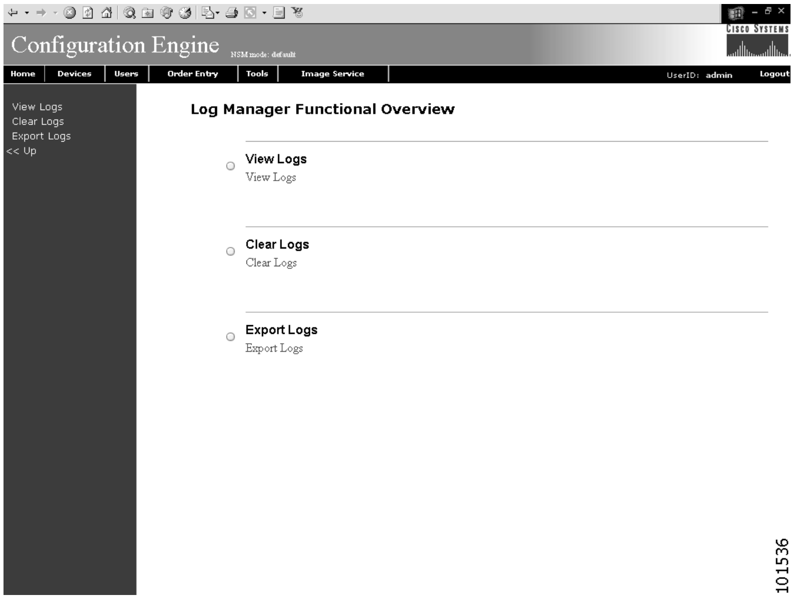
Step 6 To save the new password, click **OK**.

Step 7 To return to the Tools main menu, click on the **Tools** tab.

Log Manager

To view various log files, from the Tools Page, click **Log Manager**. The Log Manager page appears (see Figure 2-63).

Figure 2-63 Log Manager



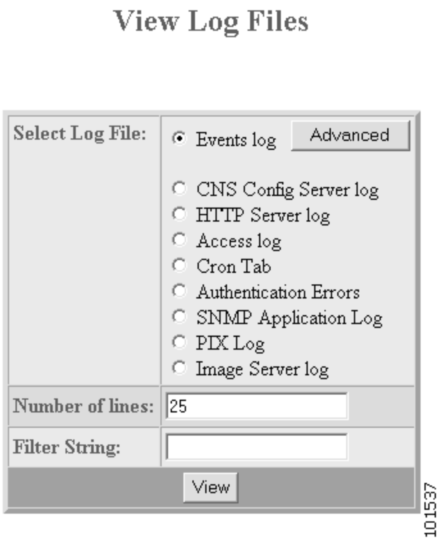
How to View Log Files

To view various log files, follow these steps:

Step 1 From the Log Manager page, click **View Logs**.

The View Log Files dialog box appears (see Figure 2-64).

Figure 2-64 Log File Viewer



View Log Files

Select Log File:
- ● Events log
- ○ CNS Config Server log
- ○ HTTP Server log
- ○ Access log
- ○ Cron Tab
- ○ Authentication Errors
- ○ SNMP Application Log
- ○ PIX Log
- ○ Image Server log

Number of lines: 25

Filter String:

Step 2 Choose the log file you want to view.

Table 2-24 list valid values for these fields.

Table 2-24 Valid Values for View Log Files

Attribute	Description	Valid Values
Select Log Files	List of available log files.	Radio button
Number of lines	Number of lines displayed.	
Filter String	Filter string	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 Set the number lines you want to display.

Step 4 To limit the report to display only specific entries, set a case-sensitive keyword filter, or leave blank.

Step 5 Click **View**.

A report displays.

Step 6 To return to the Tools main menu, click on the **Tools** tab.

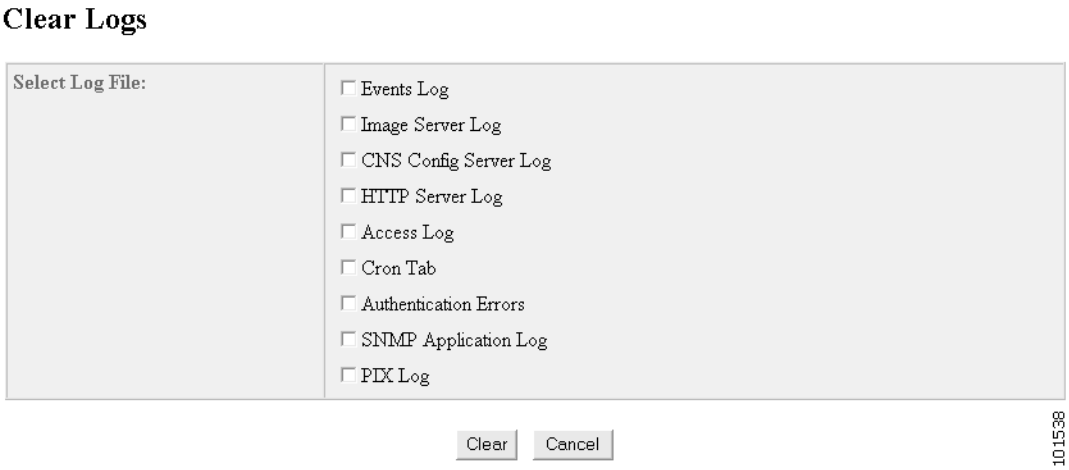
How to Clear Logs

To clear various log files, follow these steps:

Step 1 From the Log Manager page, click **Clear Logs**.

The Clear Log Files dialog box appears (see Figure 2-64).

Figure 2-65 Clear Logs



Clear Logs

Select Log File:

- □ Events Log
- □ Image Server Log
- □ CNS Config Server Log
- □ HTTP Server Log
- □ Access Log
- □ Cron Tab
- □ Authentication Errors
- □ SNMP Application Log
- □ PIX Log

Step 2 Check the log files you wish to clear.

Step 3 To cancel this operation, click **Cancel**.

Step 4 To clear the selected log files, click **Clear**.

Step 5 To return to the Tools main menu, click on the **Tools** tab.

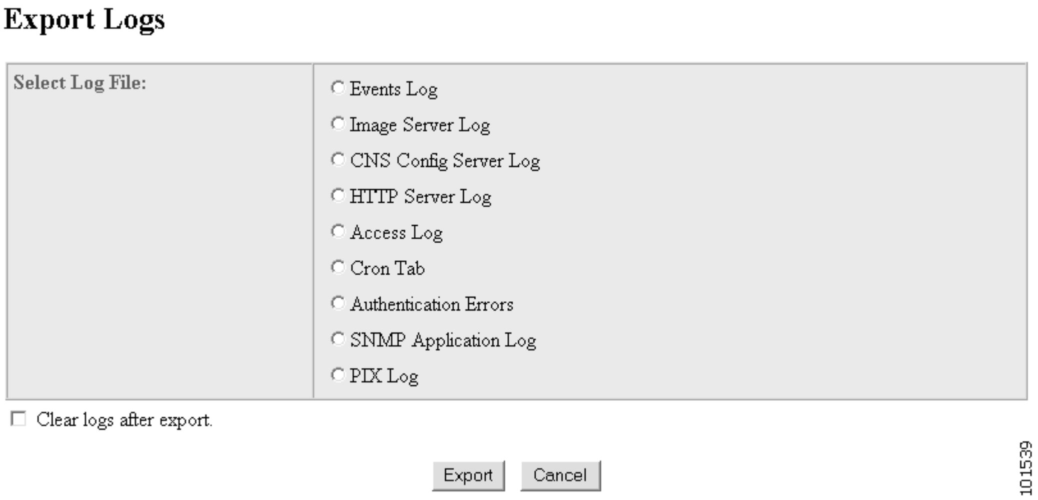
How to Export Logs

To export various log files, follow these steps:

Step 1 From the Log Manager page, click **Export Logs**.

The Export Log Files dialog box appears (see Figure 2-66).

Figure 2-66 Export Logs



Export Logs

Select Log File:

- ○ Events Log
- ○ Image Server Log
- ○ CNS Config Server Log
- ○ HTTP Server Log
- ○ Access Log
- ○ Cron Tab
- ○ Authentication Errors
- ○ SNMP Application Log
- ○ PIX Log

□ Clear logs after export.

Step 2 Check the log files you wish to export.

Step 3 To clear logs after export, check the check box.

Step 4 To cancel this operation, click **Cancel**.

Step 5 To export the selected log files, click **Export**.

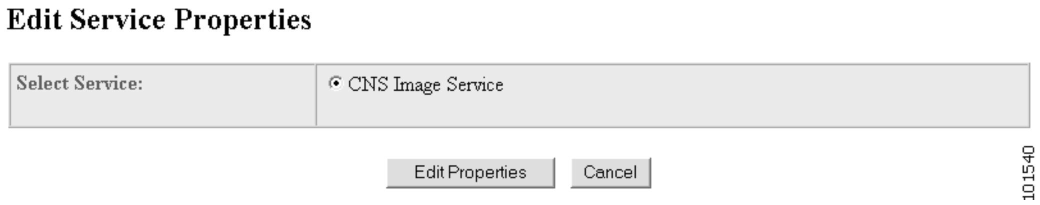
Step 6 To return to the Tools main menu, click on the **Tools** tab.

Service Manager

The Service Manager allows you to edit service properties for various services provided by CNS Configuration Engine 1.4.

From the Service Manager Functional Overview page, click Edit Service Properties. The Edit Service Properties page appears (see Figure 2-67).

Figure 2-67 Edit Service Properties



Edit Service Properties

Select Service: ● CNS Image Service

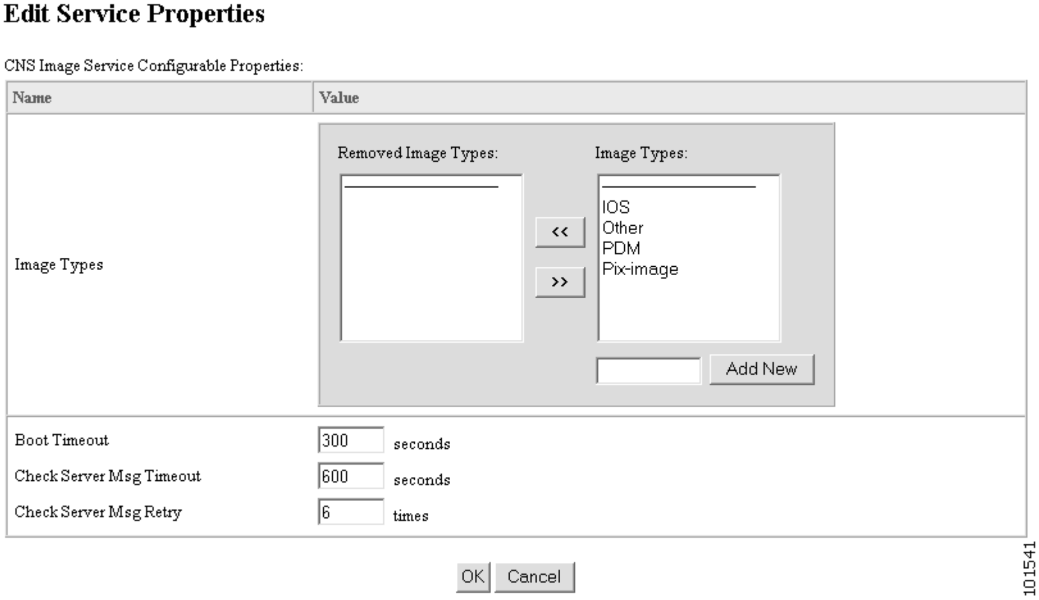
How to Edit CNS Image Service Properties

To edit CNS Image Service Properties, follow these steps:

Step 1 From the Edit Service Properties page, select CNS Image Service by clicking the associated radio button.

The service properties page for CNS Image Service appears (see Figure 2-68).

Figure 2-68 CNS Image Service Properties



Edit Service Properties

CNS Image Service Configurable Properties:

Name	Value
Image Types	Removed Image Types: Image Types: IOS, Other, PDM, Pix-image
Boot Timeout	300 seconds
Check Server Msg Timeout	600 seconds
Check Server Msg Retry	6 times

Step 2 To Edit Image Types: Click the move button (<<) to move an image type to the Removed Image Types column.

Step 3 To Edit Boot Timeout: Enter a new value in the text box.

Step 4 To Edit Check Server Msg Timeout: Enter a new value in the text box.

Step 5 To Edit Check Server Msg Retry: Enter a new value in the text box.

Step 6 To clear this operation, click **Cancel**.

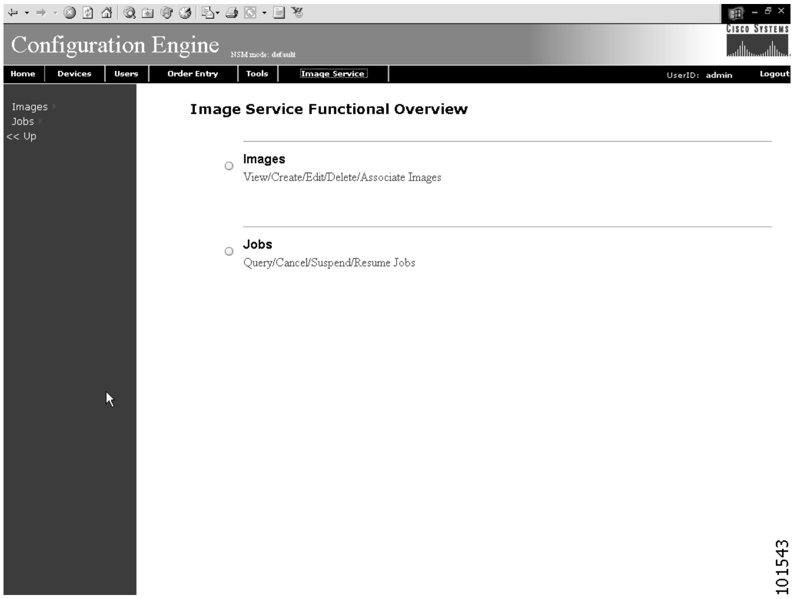
Step 7 To submit the changes, click **Ok**.

Step 8 To return to the Tools main menu, click the **Tools** tab.

CNS Image Service

To access the CNS Image Service feature, click the **Image Service** tab. The Image Service Functional Overview page appears (see Figure 2-69).

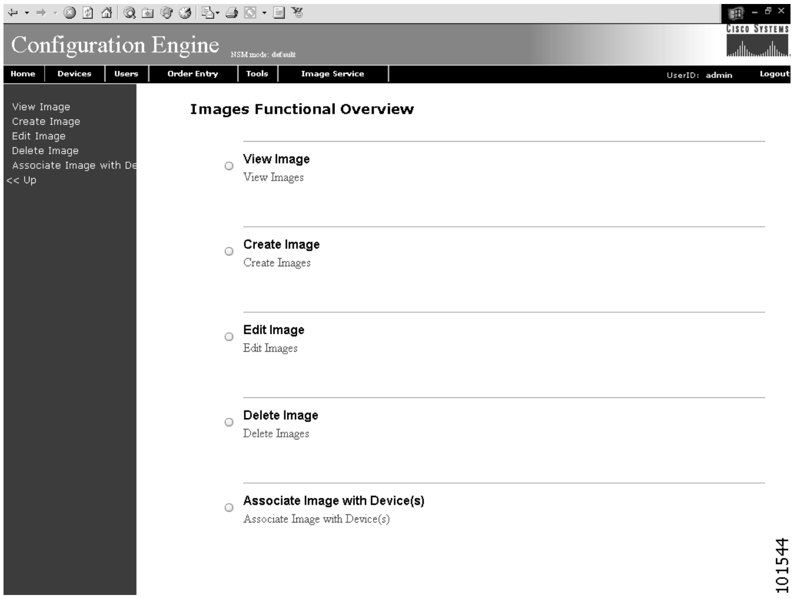
Figure 2-69 CNS Image Service



Working with Images

From the Image Service Functional Overview page, click **Images**. The Images Functional Overview page appears (see Figure 2-70).

Figure 2-70 Images



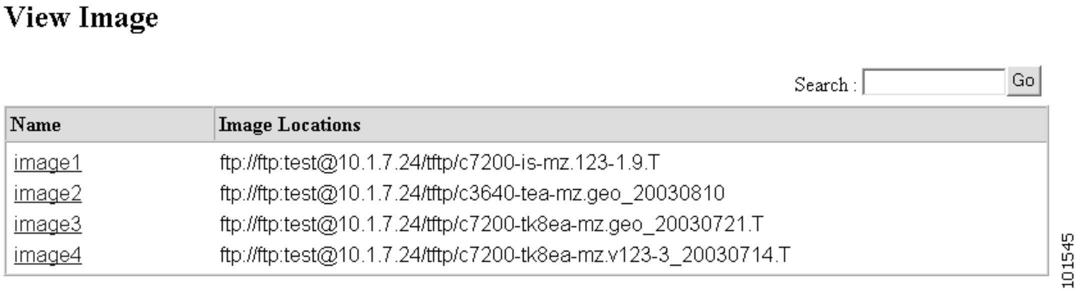
How to View an Image

To view an image, follow these steps:

Step 1 From the Images Functional Overview page, click **View Image**.

The list of images to view appears (see Figure 2-71).

Figure 2-71 View Image List



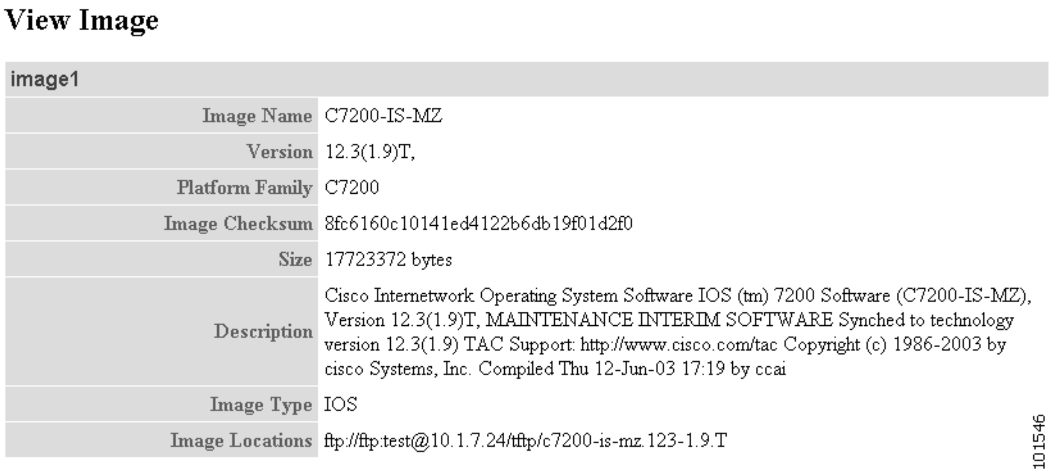
View Image

Name	Image Locations
image1	ftp://ftp:test@10.1.7.24/tftp/c7200-is-mz.123-1.9.T
image2	ftp://ftp:test@10.1.7.24/tftp/c3640-tea-mz.geo_20030810
image3	ftp://ftp:test@10.1.7.24/tftp/c7200-tk8ea-mz.geo_20030721.T
image4	ftp://ftp:test@10.1.7.24/tftp/c7200-tk8ea-mz.v123-3_20030714.T

Step 2 From the Name column, select the image you want to view.

The image information appears (see Figure 2-72).

Figure 2-72 View Image Information



View Image

image1	
Image Name	C7200-IS-MZ
Version	12.3(1.9)T,
Platform Family	C7200
Image Checksum	8fc6160c10141ed4122b6db19f01d2f0
Size	17723372 bytes
Description	Cisco Internetwork Operating System Software IOS (tm) 7200 Software (C7200-IS-MZ), Version 12.3(1.9)T, MAINTENANCE INTERIM SOFTWARE Synched to technology version 12.3(1.9) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Thu 12-Jun-03 17:19 by ccai
Image Type	IOS
Image Locations	ftp://ftp:test@10.1.7.24/tftp/c7200-is-mz.123-1.9.T

Step 3 To return to the Image Service main menu, click the **Image Service** tab.

How to Create an Image

To create an image, follow these steps:

Step 1 From the Image Service Functional Overview page, click **Create Image**.

The Create Image page appears (see Figure 2-73).

Figure 2-73 Create Image

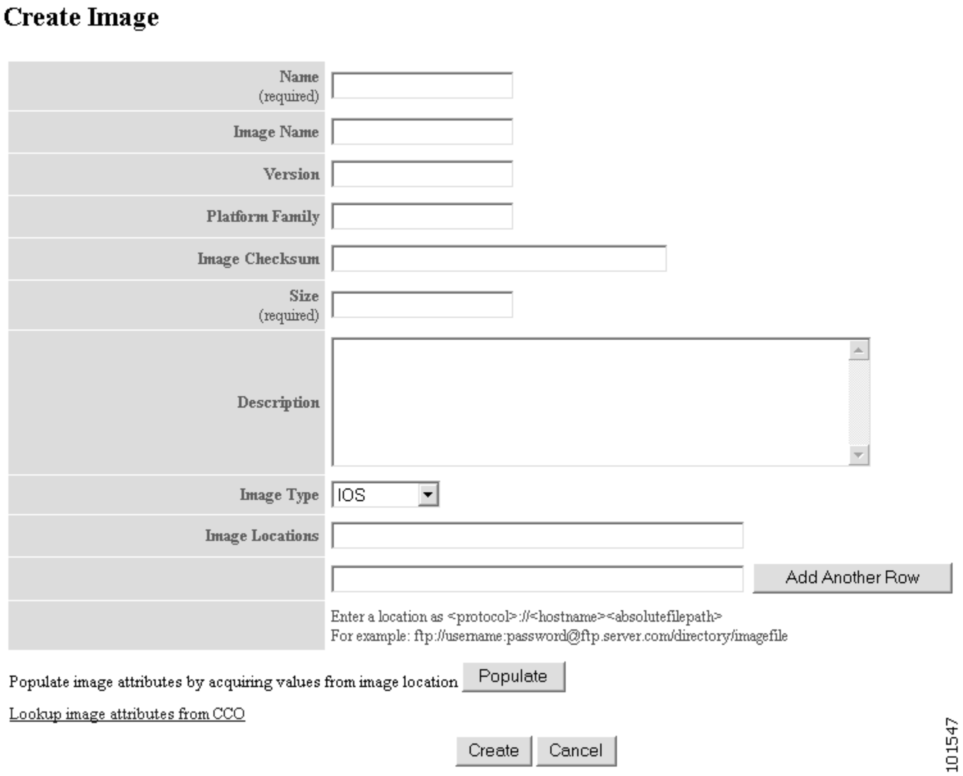


Image Type: IOS

Enter a location as <protocol>://<hostname><absolutefilepath>
For example: ftp://username:password@ftp.server.com/directory/imagefile

Populate image attributes by acquiring values from image location

There are two methods for creating an Image Object:

Manual data entry

To enter image information manually, jump to Step 2.

Timesaver You can get image attributes for manual entry by clicking the link: **Lookup image attributes from CCO**.

Automatic data entry

To automatically populate all required fields with image information from an actual image, follow these steps:

a. In the **Image Location** field, enter a valid URL for the desired image.

b. Click **Populate**.

Step 2 Enter the name of the image used by Image Service to identify this image object in the **Name** field.

Table 2-25 list valid values for these attributes.

Table 2-25 Valid Values for Create Image

Attribute	Description	Valid Values
Name	The name used my Image Services to identify this image object.	a-z A-Z 0-9 # _ (under-score) - (hyphen)
Image Name	The actual Image name.	a-z A-Z 0-9 - (hyphen)
Version	Version of the image.	a-z A-Z 0-9 . (period) ((open braces)) (close braces)
Platform Family	Platform family of the image.	a-z A-Z 0-9 - (hyphen)
Image Checksum	Checksum generated by MD5 hashing algorithm	128-bit hex number
Size	File size	0 – 9
Description	Description of the image.	Any text except Ctrl characters.
Image Type	(i) PDM (ii) QDM (iii) VDM (iv) Other (v) Pix-image	From drop-down list.
Image Location	- Any Valid URL: (i) http (ii) https (iii) ftp (iv) tftp - rcp	Valid URL as per RFC 1738.

Step 3 Enter the actual image name in the **Image Name** field.

Step 4 Enter the version of the image in the **Version** field.

Step 5 Enter the name of the platform family in the **Platform Family** field.

Step 6 Enter the image checksum for the image in the **Image Checksum** field.

Step 7 Enter the size of this file in the **Size** field.

Step 8 Enter a description of the image in the space provided.

Step 9 Select an image type from the **Image Type** drop-down list.

Step 10 Enter a valid URL for the image location in the **Image Location** field.

Follow the proper syntax as described.

Note You can create an image without specifying a location. You can add a location later by using the **Edit Image** function.

Step 11 To add another row for image location, click **Add Another Row**.

You can locate multiple copies of an image on separate servers. This allows you to do load-sharing when updating a large number of devices. Each device in a large group can be associated with a copy of the image (see“How to Add a Device” section on page 2-9) located at one of many server locations.

Step 12 To clear this operation, click **Cancel**.

Step 13 To create this image, click **Create**.

Step 14 To return to the Image Service main menu, click the **Image Service** tab.

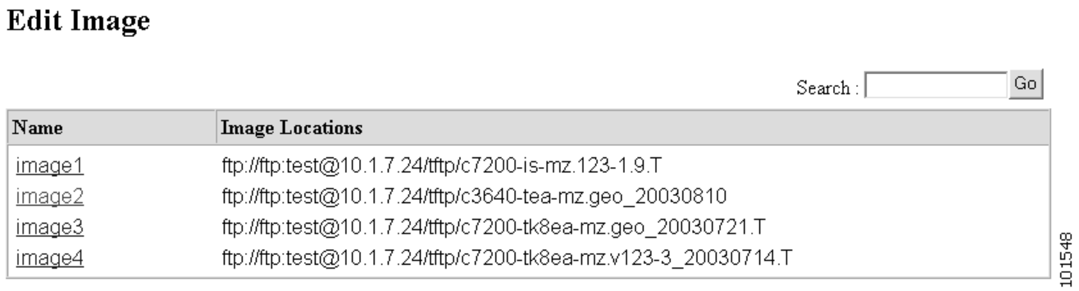
How to Edit an Image

To edit an image, follow these steps:

Step 1 From the Image Service Functional Overview page, click **Edit Image**.

The Edit Image page appears (see Figure 2-74).

Figure 2-74 Edit Image



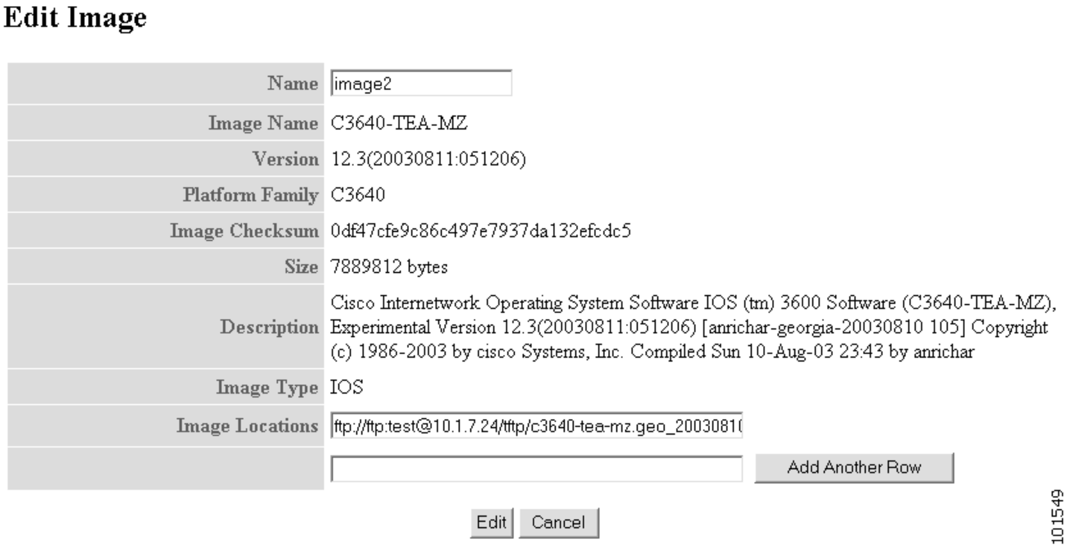
Edit Image

Name	Image Locations
image1	ftp://ftp:test@10.1.7.24/tftp/c7200-is-mz.123-1.9.T
image2	ftp://ftp:test@10.1.7.24/tftp/c3640-tea-mz.geo_20030810
image3	ftp://ftp:test@10.1.7.24/tftp/c7200-tk8ea-mz.geo_20030721.T
image4	ftp://ftp:test@10.1.7.24/tftp/c7200-tk8ea-mz.v123-3_20030714.T

Step 2 Select the image you want to edit by clicking the Image Name.

The Edit Image information page appears (see).

Figure 2-75 Edit Image Information



Edit Image

Name	image2
Image Name	C3640-TEA-MZ
Version	12.3(20030811:051206)
Platform Family	C3640
Image Checksum	0df47cfe9c86c497e7937da132efcdc5
Size	7889812 bytes
Description	Cisco Internetwork Operating System Software IOS (tm) 3600 Software (C3640-TEA-MZ), Experimental Version 12.3(20030811:051206) [anrichar-georgia-20030810 105] Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Sun 10-Aug-03 23:43 by anrichar
Image Type	IOS
Image Locations	ftp://ftp:test@10.1.7.24/tftp/c3640-tea-mz.geo_2003081(

Step 3 To edit the image name, enter a new value in the **Name** field.

Table 2-26 Valid Values for Edit Image

Attribute	Description	Valid Values
Name	The name used my Image Services to identify this image object.	a-z A-Z 0-9 # _ (under-score) - (hyphen)
Image Location	- Any Valid URL: (i) http (ii) https (iii) ftp (iv) tftp - rcp	Valid URL as per RFC 1738.

Step 4 To edit the image location, enter a valid URL in the **Image Location** field.

Step 5 To clear this operation, click **Cancel**.

Step 6 To make these changes, click **Edit**.

Step 7 To return to the Image Service main menu, click the **Image Service** tab.

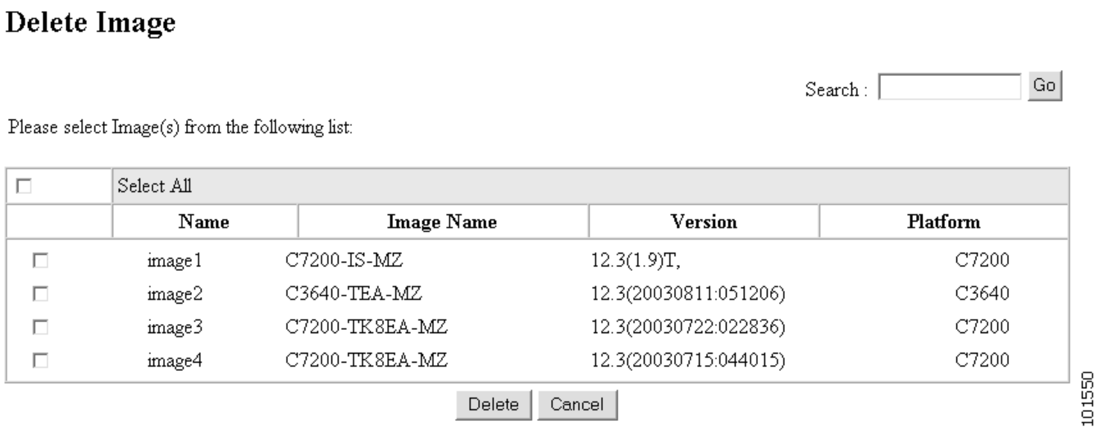
How to Delete an Image

To view images, follow these steps:

Step 1 From the Image Service Functional Overview page, click **Delete Image**.

The Delete Image page appears (see Figure 2-76).

Figure 2-76 Delete Image



Delete Image

Search : [ ] Go

Please select Image(s) from the following list:

□	Select All			
	Name	**Image Name**	**Version**	**Platform**
□	image1	C7200-IS-MZ	12.3(1.9)T,	C7200
□	image2	C3640-TEA-MZ	12.3(20030811:051206)	C3640
□	image3	C7200-TK8EA-MZ	12.3(20030722:022836)	C7200
□	image4	C7200-TK8EA-MZ	12.3(20030715:044015)	C7200

Step 2 Check the image(s) you wish to delete.

Step 3 To clear this operation, click **Cancel**.

Step 4 To make these changes, click **Delete**.

Step 5 To return to the Image Service main menu, click the **Image Service** tab.

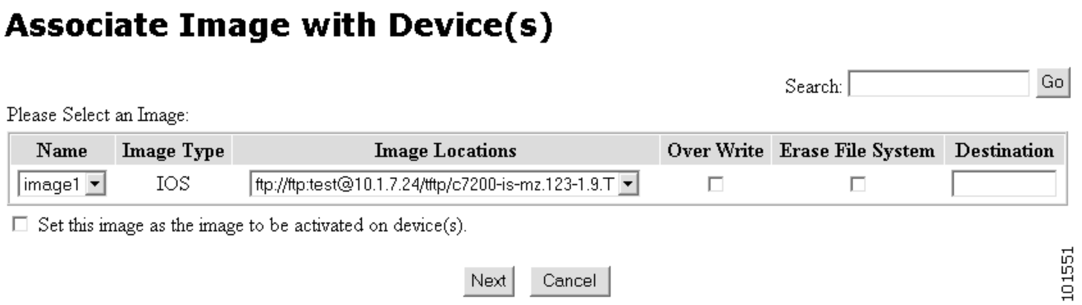
How to Associate Images with Devices

To associate images with devices, follow these steps:

Step 1 From the Image Service Functional Overview page, click **Associate Image with Device(s)**.

The Associate Image with Device(s) page appears (see Figure 2-77).

Figure 2-77 Associate Image with Device(s)



Associate Image with Device(s)

Search: [ ] Go

Please Select an Image:

Name	Image Type	Image Locations	Over Write	Erase File System	Destination
image1 ▾	IOS	ftp://ftp:test@10.1.7.24/tftp/c7200-is-mz.123-1.9.T ▾	□	□	[ ]

□ Set this image as the image to be activated on device(s).

Step 2 Select the image from the **Name** drop-down list.

The **Image Type** field and **Image Location** drop-down box are populated with corresponding information for the image.

Step 3 From the **Image Location** drop-down list, select the desired location.

Step 4 In the Destination field, enter a valid URL where the image will be copied.

For example:

disk0:/c7200-mz

Step 5 To assign this image to be the active image after distribution, check **Set this image as the Image to be activated on device**.

Step 6 To clear this operation, click **Cancel**.

Step 7 To continue, click **Next**.

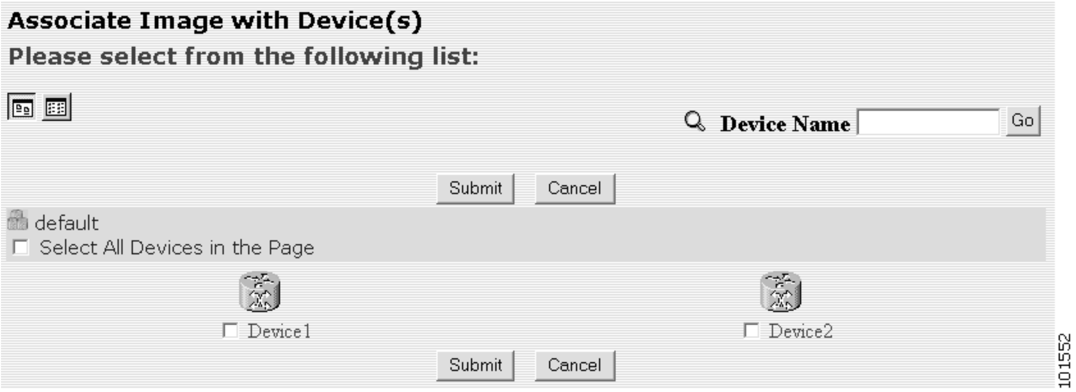
The Group list page appears.

Step 8 To associate this image with a group of devices, check the group, then click **Submit**.

Step 9 To associate this image with specific devices, click **View**.

The Device list page appears (see Figure 2-78).

Figure 2-78 Device List



Associate Image with Device(s)

Please select from the following list:

Step 10 Check the desired device(s).

Step 11 To clear this operation, click **Cancel**.

Step 12 To associate this image to the selected devices, click **Submit**.

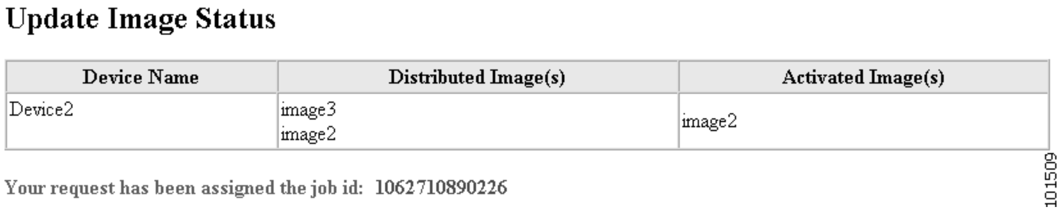
A confirmation page appears.

Step 13 To return to the Image Service main menu, click the **Image Service** tab.

Image Update Jobs

Each Image Update job takes a considerable amount of time. Therefore, when you choose to update the image on a device from Devices -> Update Device -> Update Image (see “How to Update Device Image” section on page 2-21), the system provides you with a Job ID, which is associated with the request.

Figure 2-79 Update Image Job ID



Update Image Status

Device Name	Distributed Image(s)	Activated Image(s)
Device2	image3 image2	image2

Your request has been assigned the job id: 1062710890226

Working with Image Update Jobs

You can perform the following operations with the Jobs feature:

- Query Jobs
- Cancel/Stop Jobs
- Restart Jobs

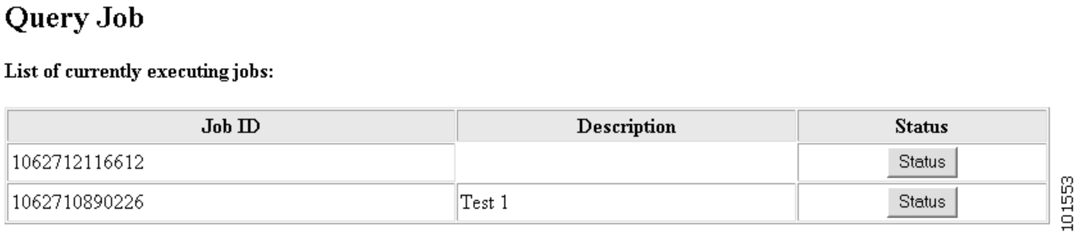
How to Query Jobs

To query job status, follow these steps:

Step 1 From the Image Service Functional Overview page, click Query Job.

The Query Job page appears (see Figure 2-80).

Figure 2-80 Query Jobs



Query Job

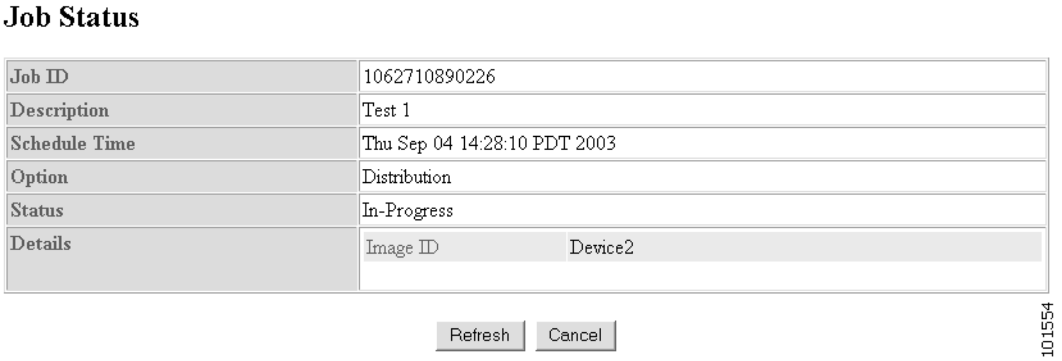
List of currently executing jobs:

Job ID	Description	Status
1062712116612		Status
1062710890226	Test 1	Status

Step 2 To check the status of a job, for the desired job, click Status.

The Job Status page appears (see Figure 2-81).

Figure 2-81 Job Status



Job Status

Job ID	1062710890226
Description	Test 1
Schedule Time	Thu Sep 04 14:28:10 PDT 2003
Option	Distribution
Status	In-Progress
Details	Image ID Device2

Step 3 To clear this operation, click **Cancel**.

Step 4 To update the status page, click **Refresh**.

Step 5 To return to the Image Service main menu, click the **Image Service** tab.

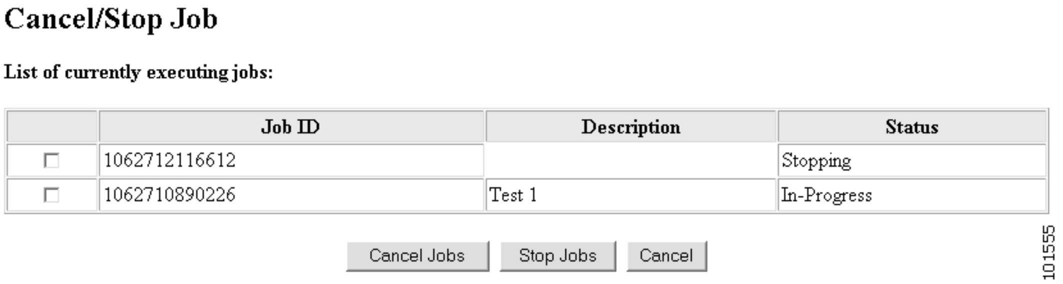
How to Cancel or Stop a Job

To cancel or stop a job, follow these steps:

Step 1 From the Image Service Functional Overview page, click Cancel/Stop Job.

The (see Figure 2-82).

Figure 2-82 Cancel or Stop Job.



Cancel/Stop Job

List of currently executing jobs:

	Job ID	Description	Status
□	1062712116612		Stopping
□	1062710890226	Test 1	In-Progress

Step 2 Check the job you want to cancel or stop.

Step 3 To Cancel the job, click **Cancel Job**.

The job is permanently canceled.

Step 4 To stop the job, click **Stop Job**.

You can restart the job at a later time.

Step 5 To clear this operation, click **Cancel**.

Step 6 To return to the Image Service main menu, click the **Image Service** tab.

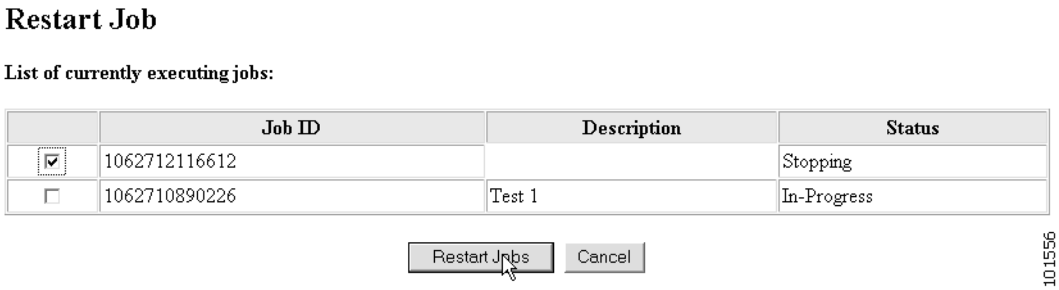
How to Restart a Job

To restart a job, follow these steps:

Step 1 From the Image Service Functional Overview page, click Restart Job.

The Restart Job page appears (see Figure 2-83).

Figure 2-83 Restart Job



Restart Job

List of currently executing jobs:

	Job ID	Description	Status
☑	1062712116612		Stopping
□	1062710890226	Test 1	In-Progress

Step 2 Check the job you want to restart.

Step 3 To clear this operation, click **Cancel**.

Step 4 To restart this job, click **Restart**.

Step 5 To return to the Image Service main menu, click the **Image Service** tab.

CNS Agent Enabled to Non-CNS Agent Enabled Up/Downgrade

With the Image Service feature, you can not only update the Cisco IOS image on a device, you can revert back to an earlier version of the image. When you do this, the availability of CNS agents on the device may change. This means you might have to use IMGW to simulate agents to update configurations and images on the device.

CNS agents at the device-level are a function of the particular version of Cisco IOS running on that device:

- 12.0 or earlier – No CNS agents on the device.
- 12.2 – CNS Configuration Agent and CNS Event Agent but not the CNS Image Agent.
- 12.3(3) or later – CNS Configuration Agent, CNS Event Agent, and CNS Image Agent.

Things to Know

- IMGW can simulate different agent types:
  - CNS Configuration Agent only
  - CNS Image Agent only
  - both CNS Configuration Agent and CNS Image Agent

  Make sure to select the correct agent for your purpose when creating IMGW devices.

- You should always have one set of the same agents running for the same device object. The common mistake when upgrading/downgrading to a different version of an image is:
  - Upgrading: after enabling a certain agent on the device, you still have an IMGW device that is simulating the same agent on the CNS Configuration Engine 1.4, or the other way around.
  - Downgrading: a certain agent is not available on the device anymore, but the IMGW device is not simulating this agent. The next update will fail.

12.0 -> 12.2

To update an image from 12.0 to 12.2, the image needs to use IMGW to simulate both CNS Configuration Agent and CNS Image Agent.

Procedure

Step 1 Create a template for configuration update. This template only applies to a device when you do a configuration update.

Step 2 Create a template for image activation.

The activation template should include the boot image information. For example, if you want to copy image *c837-k9o3y6-mz.122-13.ZH2.bin* to flash and run it as the active image, the following CLI commands should be in the active template:

no boot system

boot system flash flash: c837-k9o3y6-mz.122-13.ZH2.bin

Step 3 Create the image for the device:

a. Setup an FTP/TFTP server.

b. Copy the image onto the FTP/TFTP server.

c. Login to the CNS Configuration Engine 1.4, go to I**mage Service** -> **Images** -> **Create Image**.

d. Enter image information on the page or just enter **Name** and **Image Locations** on the FTP/TFTP server, then click on **Populate** to get image information.

e. Click on **Create**.

f. To verify, go to **Image Service** -> **Images** -> **View Image**, select the image and verify the image information.

Step 4 Create an IMGW device with device hop info. Make sure to select an agent type to simulate both CNS Configuration Agent and CNS Image Agent:

a. Login to the CNS Configuration Engine 1.4, click on **Tools** -> **DAT**, login to DAT.

b. Click on **IMGW** -> **Add IMGW Device**.

c. Enter Device Name followed by:

Gateway ID (CNS Configuration Engine 1.4 hostname by default unless changed at **Setup**)

Device Type

Agent Type (Please select ConfigAgent; ImageAgent.)

Hop Information (Select the Hop Type and enter hop info)

d. Click **Add** to add the IMGW device.

e. To verify, click on **View IMGW Devices**. You should see the added IMGW device in the list. Click on the device, you should see all the IMGW device information.

Step 5 Create a device object on the CNS Configuration Engine 1.4:

a. Login to the CNS Configuration Engine 1.4, go to **Devices** -> **Add Device**.

b. Enter Device name (same as IMGW Device Name in Step 4) followed by:

Unique ID (same as Device Name by default.)

Device Type

Template File Name (The template for configuration update)

Group

c. Click on **Next**.

d. Enter Event ID (same as Device Name and Unique ID by default) followed by:

Config ID (same as Device Name and Unique ID by default).

Agent ID (same as Device Name and Unique ID by default).

e. Click on **Next**. (If you click **Finish**, you need to associate image with device later. Please see “How to Associate Images with Devices” section on page 2-82 for instructions.

f. In Step 3, select image from Image Drop list. Select **OverWrite** and **EraseFileSystem** if you want to over write the existing image file or erase the file system before copying the file. Enter image destination.

g. Click **Finish**.

Step 6 Update image:

a. Login to the CNS Configuration Engine 1.4, go to **Devices** -> **Update Device** -> **Update Image**.

b. Select the group where the device belong to and click on **view**.

c. Select the device from the list and click **Submit**.

d. Finish all four steps on the Update Image page and click **Update** to summit the image update job.

Step 7 To check the updating status, go to **Image Service** -> **Jobs** -> **Query Job**, click **Status** to check the job status.

Step 8 To see more debug message on the job, go to **Tools** -> **Log Manager** -> **View Logs** and select the log to view.

Step 9 Now you should have 12.2 image running on the device. If you want to enable CNS Configuration Agent and CNS Event Agent on the device, put the following CLI commands in device configuration template that you created in Step 1, then do **Update Confi**g from CNS Configuration Engine 1.4:

cns config partial server_ipaddress port

cns event server_ipaddress port

Step 10 To verify, go to the View Device page on CNS Configuration Engine 1.4, you should be able to see a green indicator next to this device object.

Note In order to use CNS Configuration Agent and CSN Event Agent to do configuration updates, you should delete the IMGW device object from DAT since it should never have two sets of the same agent for the device on the CNS Configuration Engine 1.4.

12.0 -> 12.3(3) or later

To update image from 12.0 to 12.3(3) or later image you need to use IMGW to simulate both CNS Configuration Agent and CNS Image Agent.

The image update procedure is the same as 12.0 -> 12.2 except in Step 9. To enable the image agent on the device, you can also add the following line to the configuration template and update the configuration to the device:

cns image server http://*server_ipaddress*/cns/HttpMsgDispatcher status http://*server_ipaddress*/cns/HttpMsgDispatcher

Note In order to use CNS Configuration Agent, CNS Event Agent, and image agent to do configuration and image updates, you should delete the IMGW device object from DAT since it should never have two sets of the same agent for a device on the CNS Configuration Engine 1.4.

12.2 -> 12.3(3) or later

There are two ways to update the image from 12.2 to 12.3(3) or later image:

1. No agents enabled on the device and use IMGW to simulate both CNS Configuration Agent and CNS Image Agent. The procedure is same as update from 12.0 -> 12.2.
2. Enable CNS Event Agent and CNS Configuration Agent on devices to update activation template and use IMGW to simulate image agent only.

Procedure

Step 1 On the device, make sure to enable CNS Configuration Agent with the following commands (it can be done from router command line or from CNS Configuration Engine 1.4 configuration update):

cns event ***server_ipaddress prot***

cns config partial ***server_ipaddress prot***

Step 2 Repeat the procedure in 12.0 -> 12.2 except in Step 4. When creating the IMGW device, make sure to select **Image Agent** for Agent Type.

Step 3 To enable the image agent on the device, you can also add the following line to configuration template and update configuration to the device:

Cns image server http://*server_ipaddress*/cns/HttpMsgDispatcher status http://*server_ipaddress*/cns/HttpMsgDispatcher

Note In order to use CNS Configuration Agent, CNS Event Agent, and CNS Image Agent to do configuration and image updates, you should delete the IMGW device object from DAT since it should never have two sets of the same agent for a device on the CNS Configuration Engine 1.4.

12.3(3) or later -> 12.3(3) or later

Image upgrading from 12.3(3) or later -> 12.3(3) later images can be done with CNS agents enabled on device. There is no need for IMGW.

Procedure

Step 1 On the device, make sure to enable the CNS Configuration Agent with the following commands (it can be done from router command line or from CNS Configuration Engine 1.4 configuration update):

cns event *server_ipaddress prot*

cns config partial *server_ipaddress prot*

cns image server http://*server_ipaddress***/cns/HttpMsgDispatcher status http://***server_ipaddress***/cns/HttpMsgDispatcher**

Step 2 Create a template for configuration updates.

Step 3 Create a template for image activation.

Step 4 Create an image for device:

a. Setup FTP/TFTP server.

b. Copy image on FTP/TFTP server.

c. Login to the CNS Configuration Engine 1.4, go to **Image Service** -> **Images** -> **Create Image**.

d. Enter image information on the page or just enter **Name** and **Image Locations** on the FTP/TFTP server then click **Populate** to get image information.

e. Click on **Create**.

f. To verify, go to **Image Servic**e -> **Images** -> **View Image**, select the image and verify the image information.

Step 5 Create a device object on CNS Configuration Engine 1.4:

a. Login to the CNS Configuration Engine 1.4, then go to **Devices** -> **Add Device**.

b. Enter Device name (same as the Device Name in Step 4) followed by:

Unique ID (same as Device Name by default.)

Device Type

Template File Name (The template for configuration update)

Group

c. Click **Next**.

d. Enter Event ID (same as Device Name and Unique ID by default) followed by:

Config ID (same as Device Name and Unique ID by default)

Agent ID (same as Device Name and Unique ID by default)

e. Click **Next**. (If you click **Finish**, you need to associate image with device later. Please see "How to Associate Images with Devices" section on page 2-82 for instructions.)

f. In Step 3, select image from Image Drop list. Select **OverWrite** and **EraseFileSystem** if you want to over write the existing image file or erase the file system before copying the file. Enter the image destination.

g. Click **Finish**.

Step 6 Update image:

a. Login to the CNS Configuration Engine 1.4, then go to **Devices** -> **Update Device** -> **Update Image**

b. Select the group where the device belongs, then click on **view**.

c. Select the device from the list and click **Submit**.

d. Finish all four steps on the Update Image page, then click **Update** to summit the image update job.

Step 7 To check the updating status, go to **Image Service** -> **Jobs** -> **Query Job**, click the **Status** to check the job status.

Step 8 To see more debug messages on the job, go to **Tools** -> **Log Manager** -> **View Logs** and select the log to view.

12.3(3) or later -> 12.2

This is the same as upgrading from 12.2 -> 12.3(3) or later images. There are several things that you should check before submitting the update:

- If you are using the second option in 12.2->12.3(3), which uses IMGW to simulate only the CNS Image Agent, but not the CNS Configuration Agent and CNS Event Agent, make sure there is only CNS Event Agent and CNS Configuration Agent enabled on the device but no CNS Image Agent; even though it is running 12.3(3) or later image that has all the agents. The IMGW on the server side will simulate the CNS Image Agent.
- If there is already a device on the CNS Configuration Engine 1.4, you only need to add an IMGW device from DAT with the same device name as device object on CNS Configuration Engine 1.4.
- Please remove any commands in your configuration template to configuration CNS Image Agent.

12.3(3) or later -> 12.0

Same as upgrading from 12.0 -> 12.3(3) or later image. There are serveral things that users should check before submit the update:

Step 1 Make sure there is no agent enabled on router even it runs 12.3(3) or later image that has all the agents. The IMGW on server side will simulate both CNS Configuration Agent and CNS Image Agent.

Step 2 If there is already device object on the CNS Configuration Engine 1.4, users only need to add IMGW device from DAT with the same device name as device object on CNS Configuration Engine 1.4.

Step 3 Please remove them if you have any command in your configuration template to configure CNS Configuration Agent, CNS Event Agent, or CNS Image Agent.

Backup and Restore

The Backup and Restore function allows you to backup directory data (configuration templates, device and user information, and so forth) to a remote location.

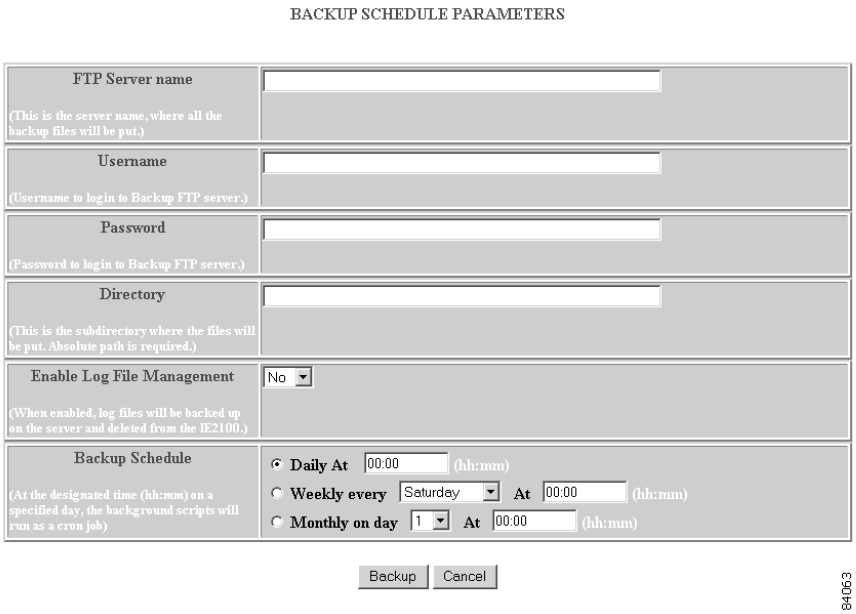
Backup Procedure

Step 1 Login into CNS Configuration Engine 1.4 user interface.

Step 2 Go to **Tools** ⇒**Data Manager** ⇒ **Schedule Backup**.

The backup information dialog box appears (see Figure 2-84).

Figure 2-84 Backup Schedule Parameters



BACKUP SCHEDULE PARAMETERS

FTP Server name (This is the server name, where all the backup files will be put.)	
Username (Username to login to Backup FTP server.)	
Password (Password to login to Backup FTP server.)	
Directory (This is the subdirectory where the files will be put. Absolute path is required.)	
Enable Log File Management (When enabled, log files will be backed up on the server and deleted from the IE2100.)	No
Backup Schedule (At the designated time (hh:mm) on a specified day, the background scripts will run as a cron job)	● Daily At 00:00 (hh:mm) ○ Weekly every Saturday At 00:00 (hh:mm) ○ Monthly on day 1 At 00:00 (hh:mm)

Step 3 To specify where you want the backup data to be stored, enter the FTP server name in the **FTP Server Name** field.

Table 2-27 list valid values for these fields.

Table 2-27 Valid Values for Backup Schedule Parameters

Attribute	Description	Valid Values
FTP Server name	Server name where all backup files will be put.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Username	Login username for the FTP server.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Password	Password for FTP server.	

Table 2-27 Valid Values for Backup Schedule Parameters (continued)

Attribute	Description	Valid Values
Directory	Subdirectory into which all backup files will be put.	Absolute path
Enable Log File Management	determines whether files will be deleted from CNS 2100 Series system after backup.	From drop-down list
Backup Schedule	Date and time fields.	As required

Step 4 To specify the username to login to the FTP server, enter a valid username in the **Username** field.

Step 5 To specify the password to use to login to the FTP server, enter a valid value in the **Password** field.

Step 6 To specify the subdirectory where the data file is put, enter the absolute path in the **Directory** field.

Step 7 Choose whether to **Enable Log File Management**.

Step 8 To specify the backup schedule, complete the fields in the **Backup Schedule** pane.

Note The time base for the CNS 2100 Series system should be set to Coordinated Universal Time (UTC).

Step 9 To cancel the backup operation, click **Cancel**.

Step 10 To start the backup operation, click **Backup**.

Step 11 To return to the main menu, click on the **Tools** tab.

Data Restore Procedure

Step 1 Login to the Cisco CNS 2100 Series Intelligence Engine.

Step 2 Type **datarestore** at the command line, then press **Enter**.

Step 3 Provide inputs to following prompts:

Notes

Sample user inputs are shown in **bold** text.

```
Entering Data Restore section
Type ctrl-c to exit

Enter FTP server (hostname.domainname or IP address): 10.1.19.108
Enter username used for FTP server: admin
Enter FTP password: *****
Re-enter FTP password: *****
Enter absolute pathname of backup file on FTP server: /tmp/backup-20030819.tar.gz
```

Definitions

FTP Server: The IP address or hostname of the FTP server on which the backup file is located.

FTP Username: The username used to login to the FTP server.

FTP Password: The password used to login to the FTP server.

Absolute pathname of backup file on FTP server: Fully specified path of the backup file stored on the FTP server.

Redefining Hostname, Domain Name, and Country Code

If you want to redefine CNS 2100 Series system network information; such as hostname, domain name, and country/location code without destroying the directory data and templates, use the **relocate** command.

The **relocate** command is designed to backup and erase existing directory data so that you can redefine the CNS 2100 Series system network information using the **Setup** program.

To change CNS 2100 Series system network information, follow these steps:

Step 1 Log in as root.

Use your root password.

Step 2 Type **relocate**.

This program performs the same tasks as reinitialize, except that it backs up all data that you can restore when you run **Setup**. It also saves the configuration templates.

Step 3 Run **Setup** to redefine the desired system network information (refer to *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*).

Data Migration from Release 1.3 to 1.4

The Data Migration function allows you to upgrade your system to from Release 1.3, 1.3.1, or 1.3.2 to Release 1.4, then populate your directory with the data you established for the prior release.

This is a three-step process:

1. Export data to a remote FTP site.
2. Install Release 1.4 software.
3. Retrieve data from the FTP site and setup the system.

Export Data to a Remote FTP Site

Before exporting the data, it is assumed that the CNS 2100 Series has already been setup and is up running.

Step 1 Insert the Release 1.4 CD-ROM into the CD drive of the CNS 2100 Series to be upgraded.

Step 2 To mount the CD, login as root.

Step 3 Type:

mount /mnt/cdrom

Step 4 Change directory into:

/mnt/cdrom/DataExport

Step 5 Issue the data export command:

./dataexport

Tip Make sure you type the period (**.**) prior to the command.

Step 6 Follow the sequence of prompts to enter information of the FTP site and storage location (absolute pathname including filename).

Following are the prompts of **dataexport**:

Notes

Sample user inputs are shown in **bold** text.

```
Entering Data Export
Type ctrl-c to exit

Enter FTP server (hostname.domainname or IP address): sername.cisco.com
Enter DNS server IP address: 171.69.226.120
Enter username used for FTP server: smith
Enter FTP password: *****
Re-enter FTP password: *****
Enter absolute pathname of data file on FTP server: /users/smith/migration.tar
```

Install Release 1.4 Software

To re-image the system, while the Release 1.4 CD-ROM is still in the CD drive:

Step 1 Enter the sync command two times:

[root@mainstreet root]# **sync**

[root@mainstreet root]# **sync**

Step 2 Restart the system by pressing the **Reset** button.

Run datamigrate and Setup the System

After the system rebooted from the new installation, the following prompts appear:

```
This Appliance is not configured.
Please login as setup to configure the appliance.
localhost.localdomain login:
```

To migrate data and setup the CNS 2100 Series system, follow these steps:

Step 1 Login as **root** with password **blender**.

Step 2 Start data migration with the command:

datamigrate

The script proceeds in three stages:

1. Acquire information of the FTP server that stores the migration data and retrieve the data.
2. Start Release 1.4 **Setup** prompts and setup the system.
3. Populate internal directory storage with retrieved data.

Following are the prompts of **datamigrate**:

Notes

Sample user inputs are shown in **bold** text.

```
You must configure eth0 or eth1. Press <Enter> to skip!

Enter eth0 IP address: 10.1.19.102
Enter eth0 network mask: 255.255.255.0
Enter eth0 default gateway IP address: 10.1.19.6
Enter FTP server (hostname.domainname or IP address): sername.cisco.com
Enter DNS server IP address: 171.69.226.120
Enter username used for FTP server: smith
Enter FTP password: *****
Re-enter FTP password: *****
Enter absolute pathname of data file on FTP server: /users/smith/migration.tar
```

Synchronize Clocks

The clock (date and time) on the CNS 2100 Series system and the clock on the PC you use to access the CNS Configuration Engine 1.4 user interface should be synchronized. This is particularly important when scheduling an update-image job for a future time (refer to the *Cisco CNS Configuration Engine 1.4 Administrator Guide*).

For this operation, the client-side check to ensure you have entered a valid time value is done using the clock on the PC with the browser used to access the CNS Configuration Engine 1.4 user interface. Consequently, if the CNS 2100 Series system clock is behind the PC clock, the user interface does not allow the job to be scheduled.

For example, if the CNS 2100 Series system clock read 11:10 while the PC clock read 12:10, the user interface will not allow a job to be scheduled before 12:10. It will issue an error message: **Please input a future time**.

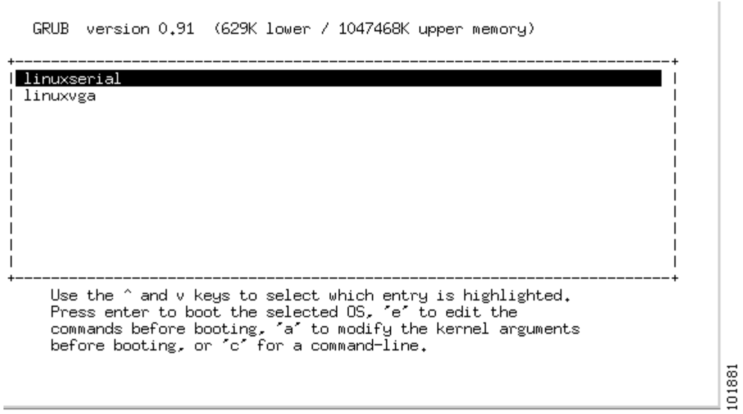
Recovering Your CNS Password

To recover your CNS password to the CNS 2100 Series system, follow these steps:

Step 1 Restart the CNS 2100 Series system.

The system shuts down, and restarts. Once the appliance restarts, you should see the boot image screen (Figure 2-85).

Figure 2-85 Boot Images



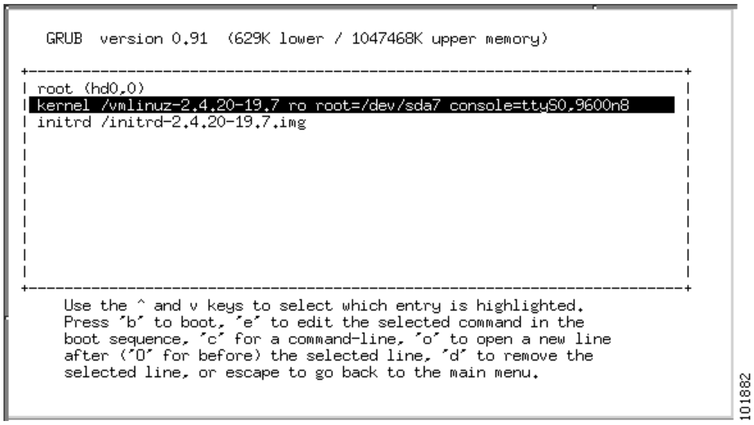
```
   GRUB  version 0.91  (629K lower / 1047468K upper memory)

+-------------------------------------------------------------------------+
| linuxserial                                                             |
| linuxvga                                                                |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
+-------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS, 'e' to edit the
     commands before booting, 'a' to modify the kernel arguments
     before booting, or 'c' for a command-line.
```

Step 2 Use the arrow keys to select (highlight) a boot image.

Select **linuxserial** for setting up the serial port as console. You can select **linuxvga** if you are connected by means of a local VGA connection.

Step 3 Press the **E** key to edit the boot parameters (see Figure 2-86).

Figure 2-86 Boot String



```
   GRUB  version 0.91  (629K lower / 1047468K upper memory)

+-------------------------------------------------------------------------+
| root (hd0,0)                                                            |
| kernel /vmlinuz-2.4.20-19.7 ro root=/dev/sda7 console=ttyS0,9600n8      |
| initrd /initrd-2.4.20-19.7.img                                          |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
|                                                                         |
+-------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press 'b' to boot, 'e' to edit the selected command in the
     boot sequence, 'c' for a command-line, 'o' to open a new line
     after ('O' for before) the selected line, 'd' to remove the
     selected line, or escape to go back to the main menu.
```

Step 4 Using the arrow keys, select the entry **kernel /vmlinuz.2.4.20-19.7 ro root=/dev/sda7 console=ttyS0,9600n8**.

Step 5 Press the **E** key to enter the editor.

Step 6 Go to the end of the line, and add **single** after the parameter **console=ttyS0,9600n8**:

```
kernel /vmlinuz.2.4.20-19.7 ro root=/dev/sda7 console=ttyS0,9600n8 single
```

Step 7 Press **Enter**.

You may not see this parameter added to the previous screen due to screen size.

Note This parameter tells the kernel to start in single user mode.

Step 8 Press the **B** key to start the system in single-user mode.

After the system initialization, you see a root prompt, without having to type in a username or password:

```
[... sys init messages ...]
Turning on user and group quotas for local filesystems: [ OK ]
Enabling swap space: [ OK ]
sh.2.04#
```

Step 9 At this prompt, type the command **passwd** and enter the new (strong) password for the root user:

```
sh.2.04# passwd
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
sh.2.04#
```

Step 10 Once you change the password, type **reboot**, and let the machine start normally.

Step 11 When prompted for a name, type **root**.

Step 12 When prompted for the password, type the new password.

CHAPTER 3

Administration Tasks for External Directory Mode

This chapter describes the Cisco CNS Configuration Engine 1.4 administration tasks for External Directory mode including information about:

- How to Login and Out of the System
- How to View, Re-synchronize, and Update Devices
- Tools

How to Login and Out of the System

You can connect to the system by means of:

- SSH
- System console

How to Login

To login to the system, follow these steps:

Step 1 Launch your web browser.

This user interface is best viewed using Microsoft Internet Explorer, version 5.5 or later.

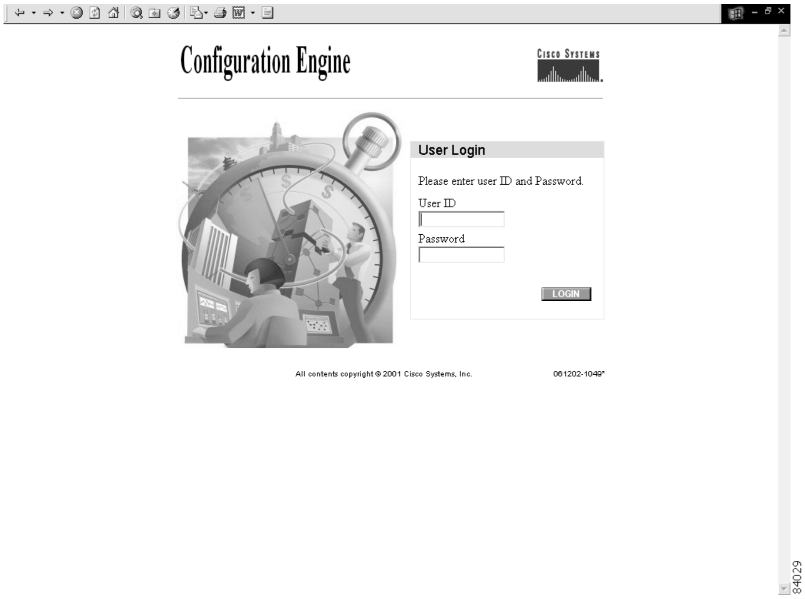
Step 2 Go to the Cisco CNS Configuration Engine 1.4 URL.

For example: **http://<*ip_address*>/config/login.html**

Note If encryption is set during Setup (see "Encryption Settings" section on page 2-6), use **https://<*ip_address*>/config/login.html**.

The login window appears (see Figure 3-1).

Figure 3-1 Logging In to the Configuration Server



Configuration Engine

User Login

Please enter user ID and Password.

User ID

Password

All contents copyright © 2001 Cisco Systems, Inc. 061202-1049*

Step 3 Enter your **User ID**.

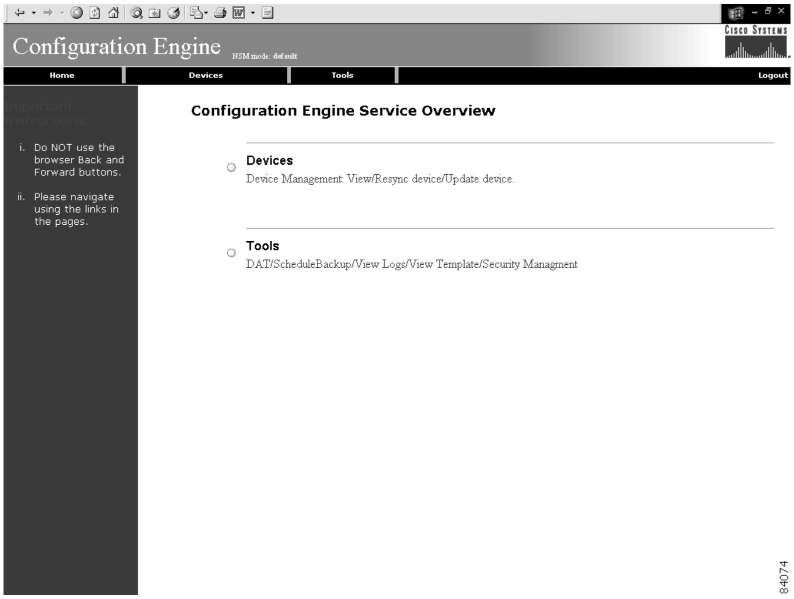
This is the user name for the Cisco CNS Configuration Engine 1.4 administrative account that you entered during **Setup**.

Step 4 Enter your password.

Step 5 Click **LOGIN**.

The Cisco CNS Configuration Engine 1.4 Home page for External Directory mode appears (see Figure 3-2).

Figure 3-2 Cisco CNS Configuration Engine 1.4 External Directory Mode Home Page



Important Instructions:

i. Do NOT use the browser Back and Forward buttons.

ii. Please navigate using the links in the pages.

Configuration Engine Service Overview

○ **Devices**
Device Management: View/Resync device/Update device.

○ **Tools**
DAT/ScheduleBackup/View Logs/View Template/Security Managment

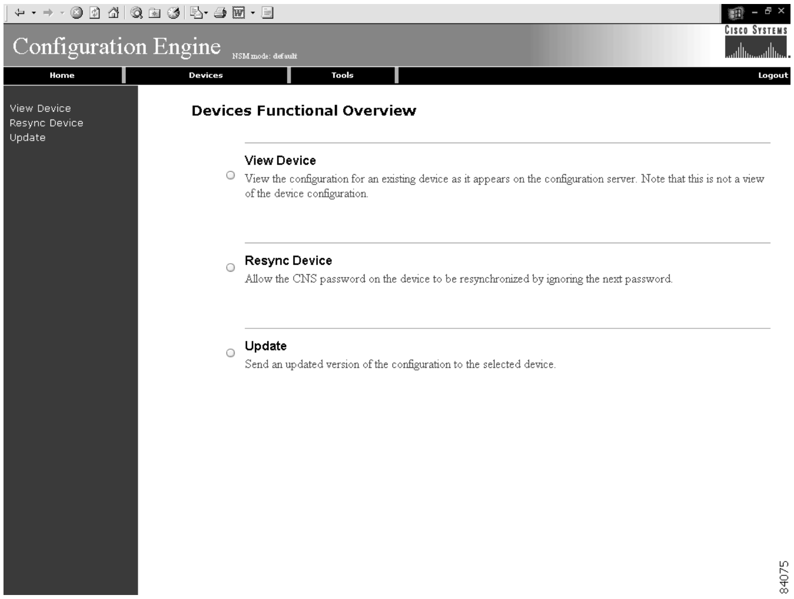
How to Log Out

To log out of the system, click the **Logout** link.

How to View, Re-synchronize, and Update Devices

To view, re-synchronize, and update devices, from the Home page, click **Devices**. The Devices page appears (see Figure 3-3).

Figure 3-3 Devices Page



Devices Functional Overview

○ View Device
View the configuration for an existing device as it appears on the configuration server. Note that this is not a view of the device configuration.

○ Resync Device
Allow the CNS password on the device to be resynchronized by ignoring the next password.

○ Update
Send an updated version of the configuration to the selected device.

How to View Device Configuration

To view a device configuration, follow these steps:

Step 1 From the Home page (Figure 3-2), click on the **Devices** tab.

Step 2 From the Devices Functional Overview page (Figure 3-3), click **View Device**.

The Device List page appears.

Step 3 Click on the icon for the device configuration you wish to view.

The Configuration for that device appears.

Note The device configuration displayed is the configuration as it appears at the configuration server. It may not be the configuration running on the device.

Step 4 To return to the main menu, click on the **Devices** tab.

How to Re-synchronize a Device

To re-synchronize a device, follow these steps:

Step 1 From the Home page (Figure 3-2), click on the **Devices** tab.

Step 2 From the Devices Functional Overview page (see Figure 3-3), click **Resync Device**.

Step 3 From the Device Selection page, click on the icon for the device you wish to re-synchronize.

Step 4 To return to the main menu, click on the **Devices** tab.

How to Update a Device Configuration

To send an updated version of the configuration to a device, or group of devices, follow these steps:

Step 1 From the Home page (Figure 3-2), click on the **Devices** tab.

Step 2 From the Devices Functional Overview page (Figure 3-3), click **Update**.

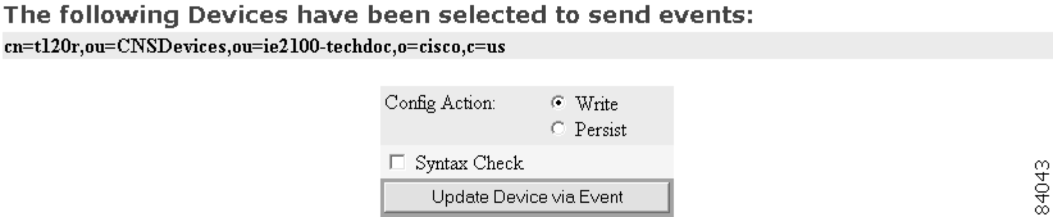
The Device Update List page appears.

Step 3 Click on the check box next to the icon for the device(s) or group(s) you wish to update.

Step 4 Click **Next**.

The update task dialog box appears (see Figure 3-4)

Figure 3-4 Update Task



The following Devices have been selected to send events:

cn=t120r,ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

Config Action: ● Write ○ Persist

□ Syntax Check

Step 5 Choose the **Config Action** and **Syntax Check** tasks you require.

Step 6 Click **Update Device via Event**.

A screen appears showing the event that has been sent to the selected device.

Step 7 To return to the main menu, click on the **Devices** tab.

Tools

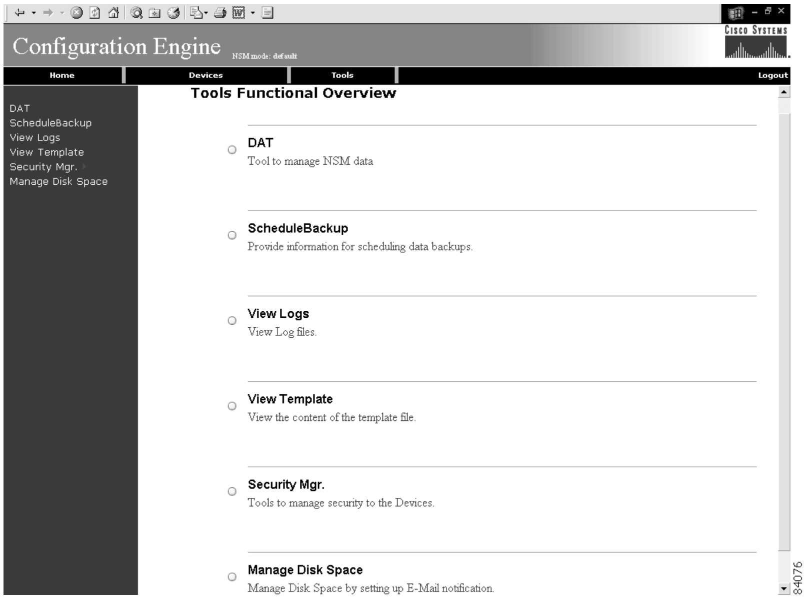
To use the tools feature, from the Home page, click on the **Tools** tab.

The Tools page appears (see Figure 3-5).

From the Tools page, you can access the following functions:

- DAT
- Schedule Backup
- View Logs
- View Templates
- Security Manager
- Manage Disk Space

Figure 3-5 Tools Functional Overview



Tools Functional Overview

○ **DAT**
Tool to manage NSM data

○ **ScheduleBackup**
Provide information for scheduling data backups.

○ **View Logs**
View Log files.

○ **View Template**
View the content of the template file.

○ **Security Mgr.**
Tools to manage security to the Devices.

○ **Manage Disk Space**
Manage Disk Space by setting up E-Mail notification.

How to Use DAT

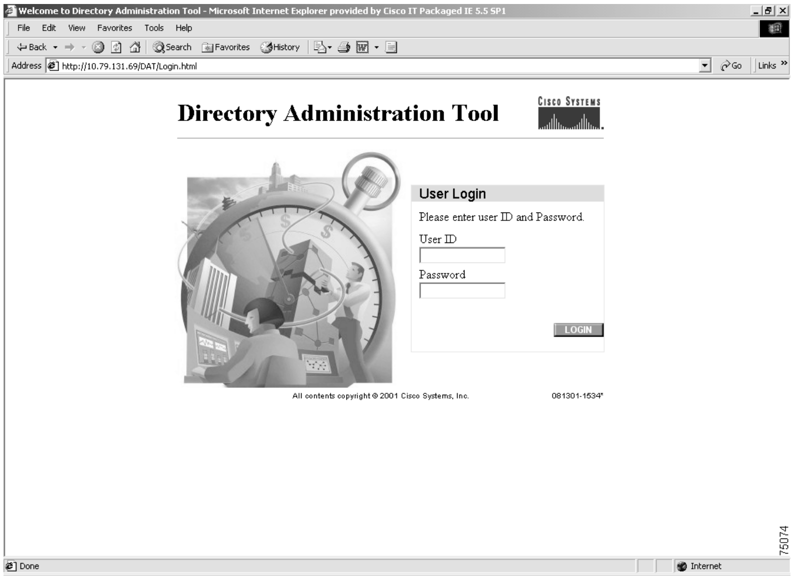
To connect to the user interface for the Directory Administration Tool (DAT), follow these steps:

Step 1 From the Home page (Figure 3-2), click on the **Tools** tab.

Step 2 From the Tools Functional Overview page (Figure 3-5), click **DAT**.

The DAT login window appears (see Figure 3-6).

Figure 3-6 Directory Administration Tool Login Window



Welcome to Directory Administration Tool - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1

Address http://10.79.131.69/DAT/Login.html

Directory Administration Tool

User Login

Please enter user ID and Password.

User ID

Password

All contents copyright © 2001 Cisco Systems, Inc. 081301-1534*

Step 3 Enter your **User ID**.

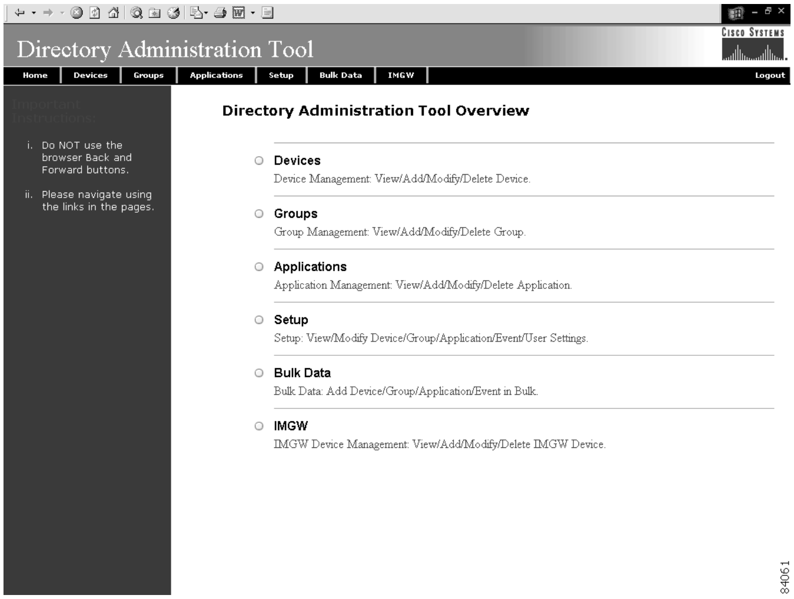
This is the LDAP proxy user name for the Cisco CNS Configuration Engine 1.4 administrative account that you entered during **Setup**.

Step 4 Enter your LDAP proxy password.

Step 5 Click **LOGIN**.

The Directory Administration Tool Home page appears (see Figure 3-7).

Figure 3-7 DAT Home Page



Directory Administration Tool

Important Instructions:

i. Do NOT use the browser Back and Forward buttons.

ii. Please navigate using the links in the pages.

Directory Administration Tool Overview

○ **Devices**
Device Management: View/Add/Modify/Delete Device.

○ **Groups**
Group Management: View/Add/Modify/Delete Group.

○ **Applications**
Application Management: View/Add/Modify/Delete Application.

○ **Setup**
Setup: View/Modify Device/Group/Application/Event/User Settings.

○ **Bulk Data**
Bulk Data: Add Device/Group/Application/Event in Bulk.

○ **IMGW**
IMGW Device Management: View/Add/Modify/Delete IMGW Device.

Step 6 From here, go to Chapter 4, "Directory Administration Tool" and follow the procedures for the tasks you want to run.

How to Schedule Data Backup

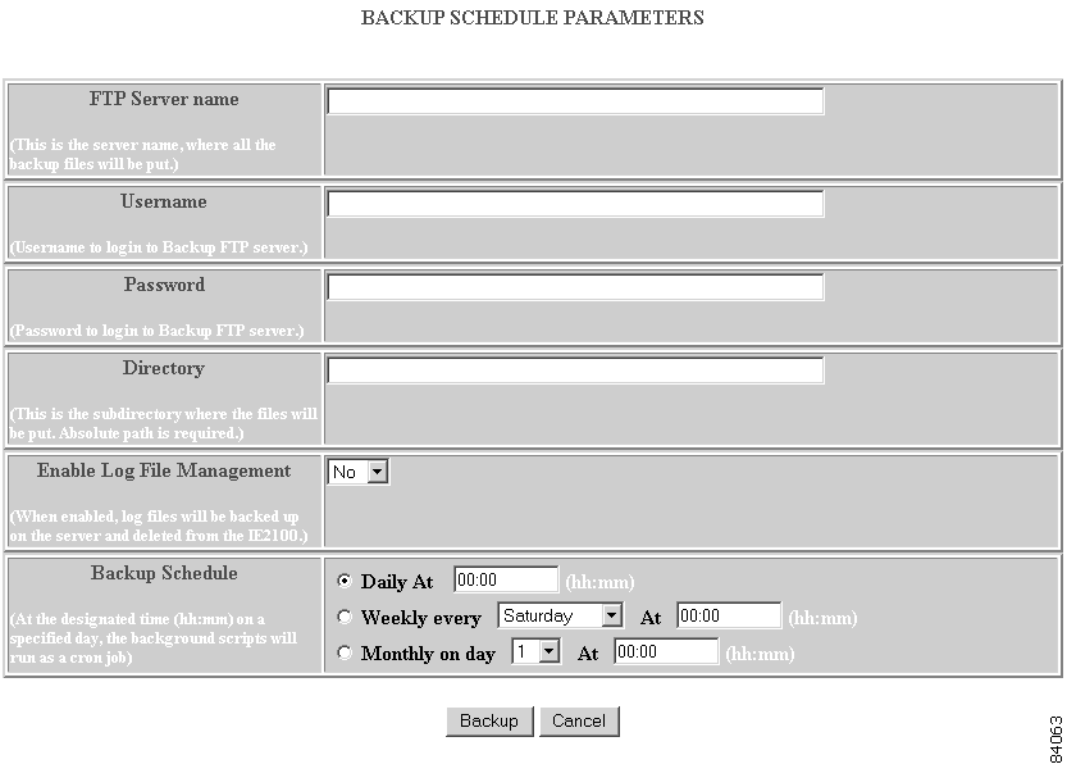
To schedule data backup, follow these steps:

Step 1 From the Home page (Figure 3-2 on page 3-3), click on the **Tools** tab.

Step 2 From the Tools Functional Overview page (Figure 3-5 on page 3-6), click **ScheduleBackup**.

The backup information dialog box appears (see Figure 3-8).

Figure 3-8 Backup Schedule Parameters



BACKUP SCHEDULE PARAMETERS

FTP Server name (This is the server name, where all the backup files will be put.)	
Username (Username to login to Backup FTP server.)	
Password (Password to login to Backup FTP server.)	
Directory (This is the subdirectory where the files will be put. Absolute path is required.)	
Enable Log File Management (When enabled, log files will be backed up on the server and deleted from the IE2100.)	No
Backup Schedule (At the designated time (hh:mm) on a specified day, the background scripts will run as a cron job)	● **Daily At** 00:00 (hh:mm) ○ **Weekly every** Saturday **At** 00:00 (hh:mm) ○ **Monthly on day** 1 **At** 00:00 (hh:mm)

Step 3 To specify where you want the backup data to be stored, enter the FTP server name in the **FTP Server Name** field.

Table 3-1 list valid values for these fields.

Table 3-1 Valid Values for Backup Schedule Parameters

Attribute	Description	Valid Values
FTP Server name	Server name where all backup files will be put.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Username	Login username for the FTP server.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Password	Password for FTP server.	6 – 12
Directory	Subdirectory into which all backup files will be put.	Absolute path
Enable Log File Management	determines whether files will be deleted from CNS 2100 Series system after backup.	From drop-down list
Backup Schedule	Date and time fileds.	As required

Step 4 To specify the username to login to the FTP server, enter a valid username in the **Username** field.

Step 5 To specify the password to use to login to the FTP server, enter a valid value in the **Password** field.

Step 6 To specify the subdirectory where the data file is put, enter the absolute path in the **Directory** field.

Step 7 Choose whether to **Enable Log File Management**.

Step 8 To specify the backup schedule, complete the fields in the **Backup Schedule** pane.

Note The time base for the CNS 2100 Series system should be set to Coordinated Universal Time (UTC).

Step 9 To cancel the backup operation, click **Cancel**.

Step 10 To start the backup operation, click **Backup**.

Step 11 To return to the main menu, click on the **Tools** tab.

For more information about backup and restore, refer to the *Cisco CNS Configuration Engine 1.4 Installation & Setup Guide For Linux*.

How to View Logs

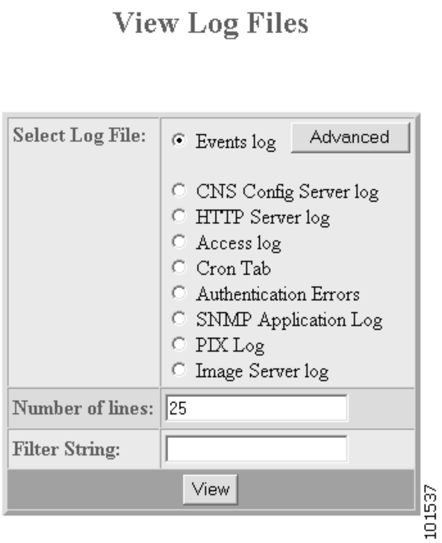
To view various log files, follow these steps:

Step 1 From the Home page (Figure 3-2), click on the **Tools** tab.

Step 2 From the Tools Functional Overview page (Figure 3-5), click **View Logs**.

The View Log Files dialog box appears (see Figure 3-9).

Figure 3-9 Log File Viewer



View Log Files

Select Log File:
● Events log
○ CNS Config Server log
○ HTTP Server log
○ Access log
○ Cron Tab
○ Authentication Errors
○ SNMP Application Log
○ PIX Log
○ Image Server log

Number of lines: 25

Filter String:

Step 3 Choose the log file you want to view.

Table 3-2 list valid values for these fields.

Table 3-2 Valid Values for View Log Files

Attribute	Description	Valid Values
Select Log Files	List of available log files.	Radio button
Number of lines	Number of lines displayed.	??
Filter String	Filter string	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 4 Set the number lines you want to display.

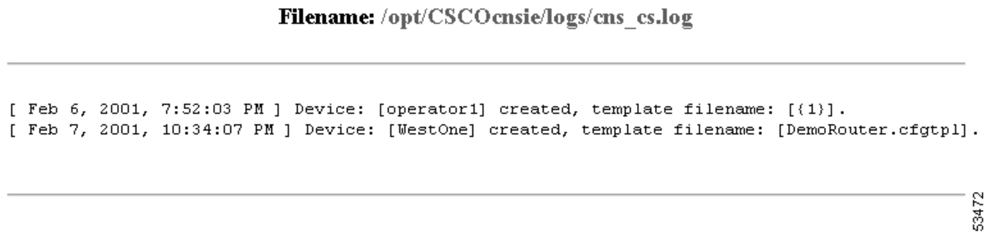
Step 5 To limit the report to display only specific entries, set a case-sensitive keyword filter, or leave blank.

Step 6 Click **View**.

A report displays (for an example see Figure 3-10).

Step 7 To return to the main menu, click on the **Tools** tab.

Figure 3-10 Log File



Filename: /opt/CSCOcnsie/logs/cns_cs.log

```
[ Feb 6, 2001, 7:52:03 PM ] Device: [operator1] created, template filename: [{1}].
[ Feb 7, 2001, 10:34:07 PM ] Device: [WestOne] created, template filename: [DemoRouter.cfgtpl].
```

How to View a Template

To view the content of the template file, follow these steps:

Step 1 From the Home page, click on the **Tools** tab.

Step 2 From the Tools Functional Overview page, click **View Template**.

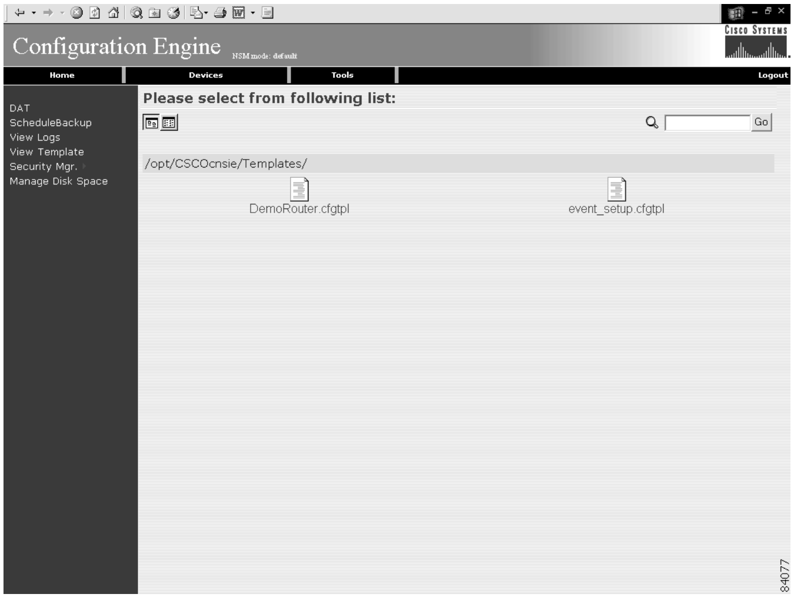
The Template page appears (see Figure 3-11).

Step 3 Click on the icon for the template file you wish to view.

The template file appears.

Step 4 To return to the main menu, click on the **Tools** tab.

Figure 3-11 Template List



Please select from following list:

/opt/CSCOcnsie/Templates/

DemoRouter.cfgtpl

event_setup.cfgtpl

Security Manager

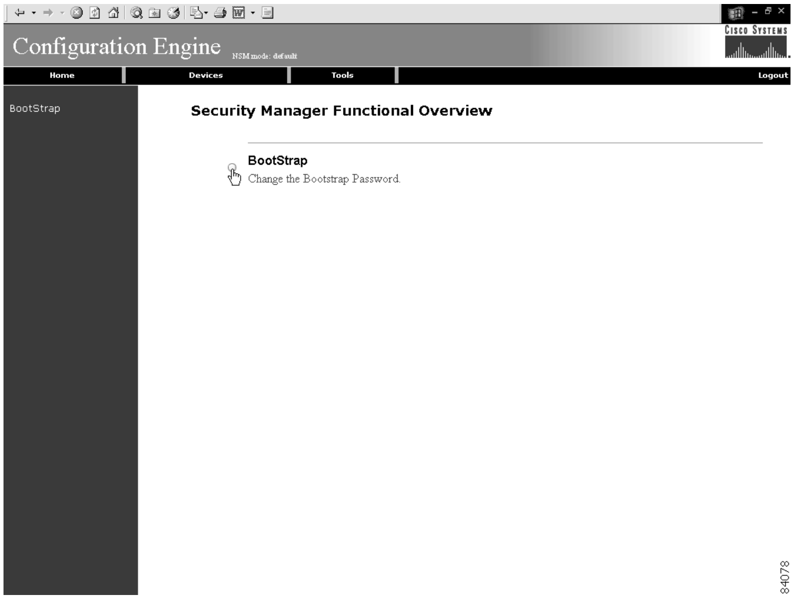
With the security manager tool you can change the bootstrap password.

The bootstrap password is used to authenticate a Cisco IOS device before it connects to the Event Gateway. For additional information see "Authentication settings" section on page 2-7)

To use the security manager tool, from the Tools Functional Overview page, click **Security Mgr**.

The Security Manager page appears (see Figure 3-12).

Figure 3-12 Security Manager



Security Manager Functional Overview

BootStrap
Change the Bootstrap Password.

How to Change Bootstrap Password

To change the bootstrap password, follow these steps:

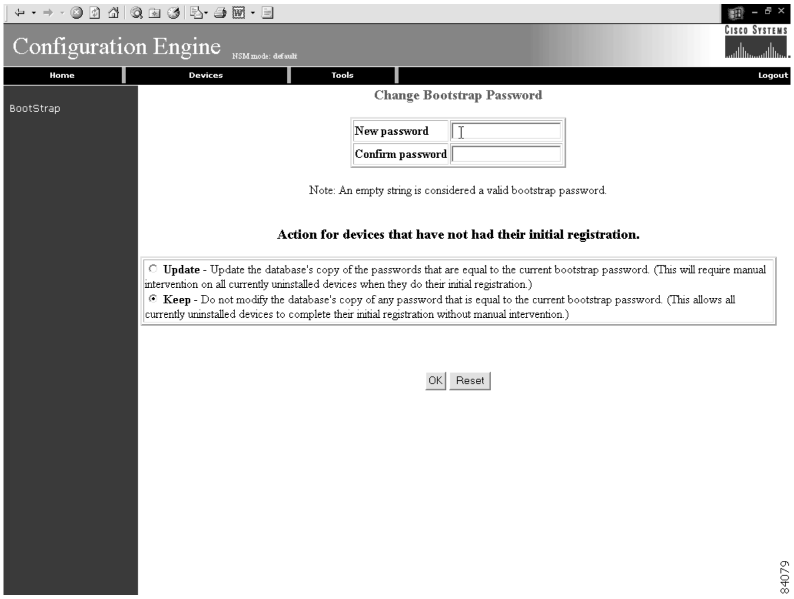
Step 1 From the Home page, click on the **Tools** tab.

Step 2 From the Tools Functional Overview page, click **Security Mgr**.

Step 3 From the Security Manager Functional Overview page, click **BootStrap**.

The Change Bootstrap Password page appears (see Figure 3-13).

Figure 3-13 Change Bootstrap Password



Change Bootstrap Password

New password	
Confirm password	

Note: An empty string is considered a valid bootstrap password.

Action for devices that have not had their initial registration.

○ **Update** - Update the database's copy of the passwords that are equal to the current bootstrap password. (This will require manual intervention on all currently uninstalled devices when they do their initial registration.)

● **Keep** - Do not modify the database's copy of any password that is equal to the current bootstrap password. (This allows all currently uninstalled devices to complete their initial registration without manual intervention.)

Step 4 In the password dialog box, enter the new password.

Table 3-3 list valid values for these fields.

Table 3-3 Valid Values for Change Bootstrap Password

Attribute	Description	Valid Values
New password	Bootstrap password	6 – 12
Confirm password	Bootstrap password	6 – 12
Update	Modifies the database copy of the password.	Radio button
Keep	Does not modify the database copy of password.	Radio button

Step 5 Confirm the new password.

Step 6 Choose (**Keep**, **Update** radio buttons) the subsequent action to the database regarding any password that is equal to the bootstrap password.

Step 7 To clear all entries, click **Reset**.

Step 8 To save the new password, click **OK**.

Step 9 To return to the main menu, click on the **Tools** tab.

How to Manage Disk Space

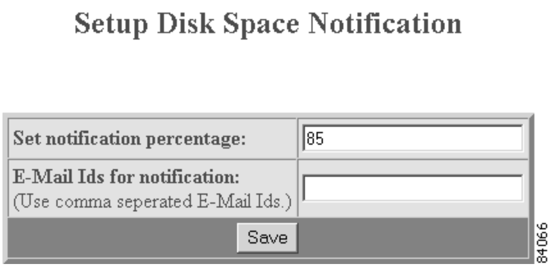
To setup disk space e-mail notification of disk space usage, follow these steps:

Step 1 From the Home page, click on the **Tools** tab.

Step 2 From the Tools Functional Overview page, click **Manage Disk Space**.

The Setup Disk Space Notification dialog box appears (see Figure 3-14).

Figure 3-14 Disk Space Notification



Setup Disk Space Notification

Set notification percentage:	85
E-Mail Ids for notification: (Use comma seperated E-Mail Ids.)	

Step 3 Set the notification percentage to the value that triggers an e-mail notification.

Table 3-4 Valid Values for Setup Disk Space Notification

Attribute	Description	Valid Values
Set notification percentage	Notification percentage that triggers an e-mail notification.	0 – 100
E-Mail Ids for notification:	E-mail address to send notification.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 4 Set the appropriate e-mail address for notification e-mail.

Step 5 To save these entries, click **Save**.

Step 6 To return to the main menu, click on the **Tools** tab.

CHAPTER 4

Directory Administration Tool

This chapter describes the Directory Administration Tool (DAT) including information about:

- How to Login
- How to Manage Devices
- How to Manage Groups
- How to Manage Applications
- Managing Directory Setup
- How to Manage Bulk Data
- Managing IMGW Parameters

The Data administration Tool (DAT) presents you with a web-based user interface that allows you to populate and manage the data in the directories. You can View/Add/Delete/Modify CNS agent-enabled devices and legacy devices and switches devices (see “Intelligent Modular Gateway” section on page 1-10), groups of devices, and applications in the directory. Also, you can View/Add/Delete/Modify events specific to each application. DAT also provides you with the additional capability of bulk data upload.

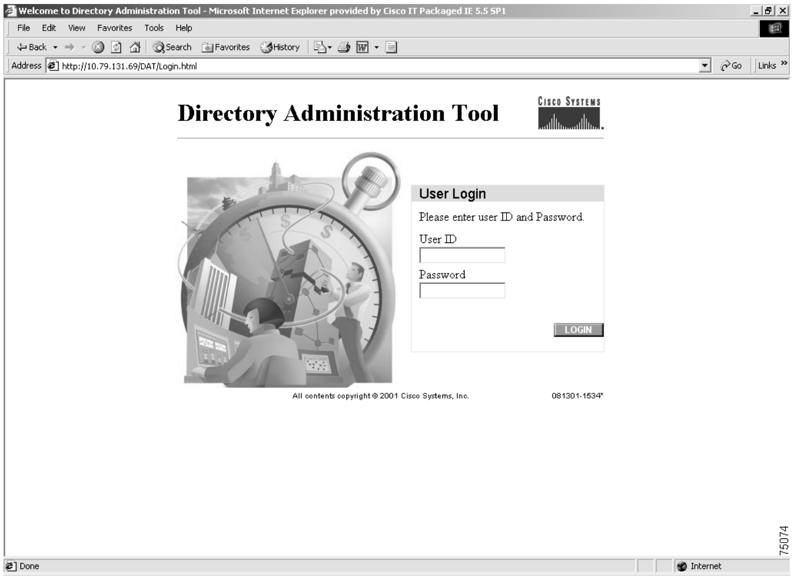
How to Login

To connect to the DAT user interface, follow these steps:

Step 1 From the Tools main menu of the Cisco CNS Configuration Engine 1.4 user interface, click **DAT**.

The login window appears (see Figure 4-1).

Figure 4-1 Directory Administration Tool Login Window


Welcome to Directory Administration Tool - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.79.131.69/DAT/Login.html
Go Links
Cisco Systems
LOGIN
Done
Internet
75074

Directory Administration Tool

User Login

Please enter user ID and Password.

User ID

Password

All contents copyright © 2001 Cisco Systems, Inc. 081301-1534*

Step 2 Enter your **User ID**.

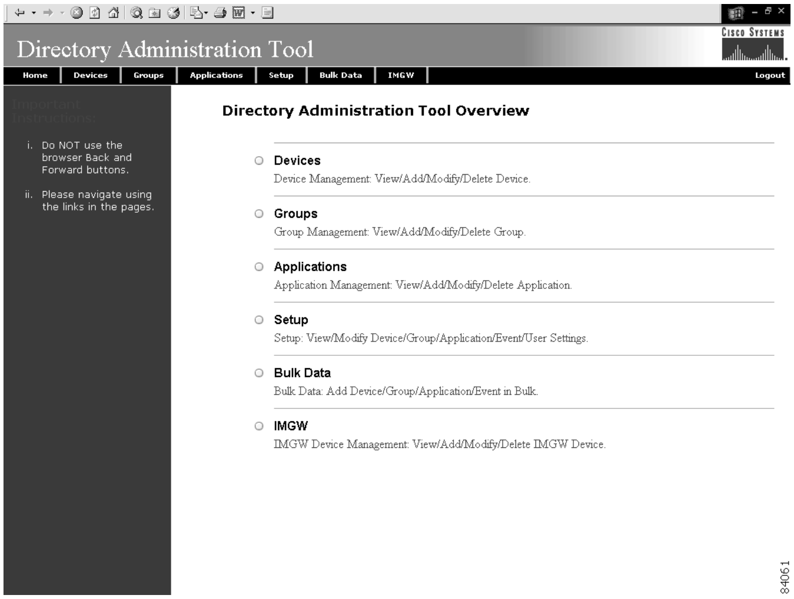
This is the user name for the Cisco CNS Configuration Engine 1.4 administrative account that you entered during **Setup**.

Step 3 Enter your password.

Step 4 Click **LOGIN**.

The Directory Administration Tool Home page appears (see Figure 4-2).

Figure 4-2 Directory Administration Tool Home Page



Directory Administration Tool

Important Instructions:

i. Do NOT use the browser Back and Forward buttons.

ii. Please navigate using the links in the pages.

Directory Administration Tool Overview

- **Devices**
  Device Management: View/Add/Modify/Delete Device.
- **Groups**
  Group Management: View/Add/Modify/Delete Group.
- **Applications**
  Application Management: View/Add/Modify/Delete Application.
- **Setup**
  Setup: View/Modify Device/Group/Application/Event/User Settings.
- **Bulk Data**
  Bulk Data: Add Device/Group/Application/Event in Bulk.
- **IMGW**
  IMGW Device Management: View/Add/Modify/Delete IMGW Device.

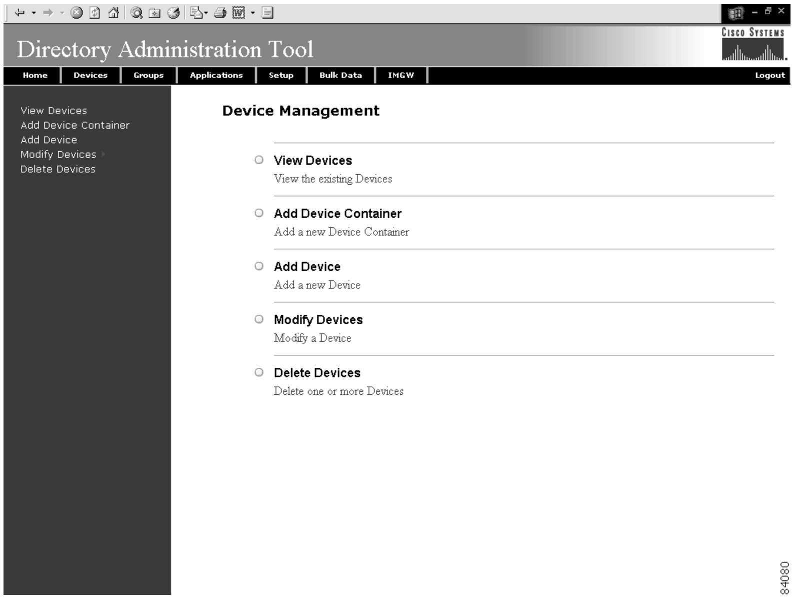
How to Log Out

To log out of the system, click on **Logout** link.

How to Manage Devices

To view and modify devices, from the Home page, click **Devices**. The Device Management page appears (see Figure 4-3).

Figure 4-3 Device Management Page



Device Management

○ **View Devices**
View the existing Devices

○ **Add Device Container**
Add a new Device Container

○ **Add Device**
Add a new Device

○ **Modify Devices**
Modify a Device

○ **Delete Devices**
Delete one or more Devices

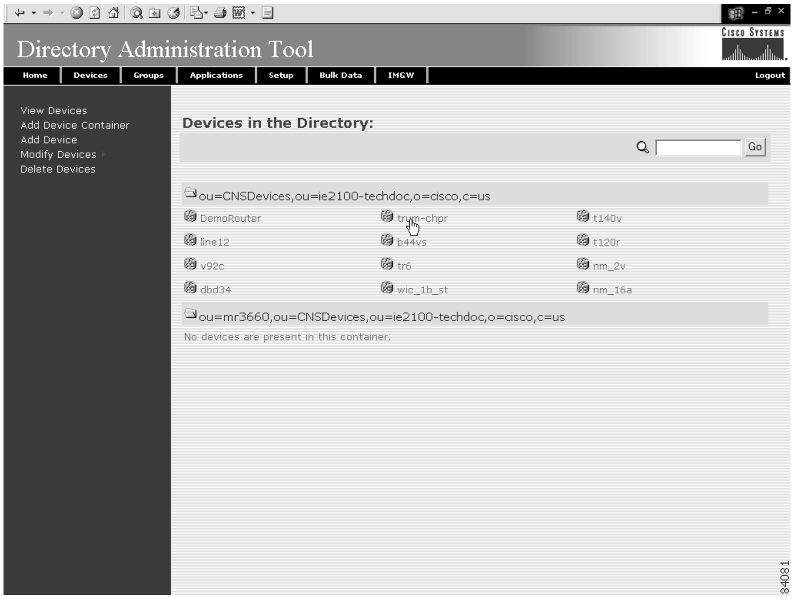
How to View Devices in the System

To view the devices currently in the system, follow these steps:

Step 1 From the Device Management page, click **View Device**.

The Device List page appears (see Figure 4-4).

Figure 4-4 Device List



Devices in the Directory:

ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

DemoRouter	trum-chpr	t140v
line12	b44vs	t120r
v92c	tr6	nm_2v
dbd34	wic_1b_st	nm_16a

ou=mr3660,ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

No devices are present in this container.

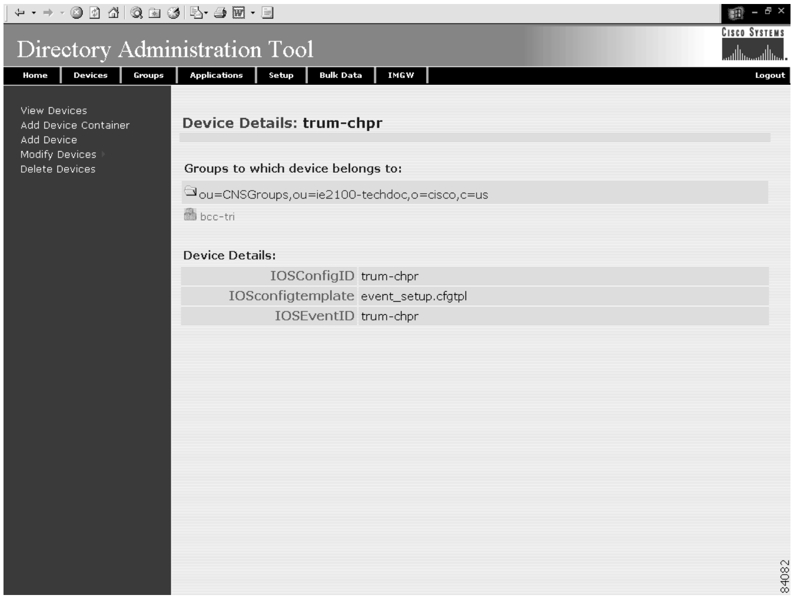
Note Devices with no parent attributes are shown with a dully-shaded icon, so you can easily identify the devices with no groups associated.

Step 2 Click on the icon for the device configuration you wish to view.

Information about that device appears (see Figure 4-5).

Step 3 To return to the main menu, click the **Home** tab.

Figure 4-5 Device Details



Device Details: trum-chpr

Groups to which device belongs to:

ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

bcc-tri

Device Details:

IOSConfigID	trum-chpr
IOSconfigtemplate	event_setup.cfgtpl
IOSEventID	trum-chpr

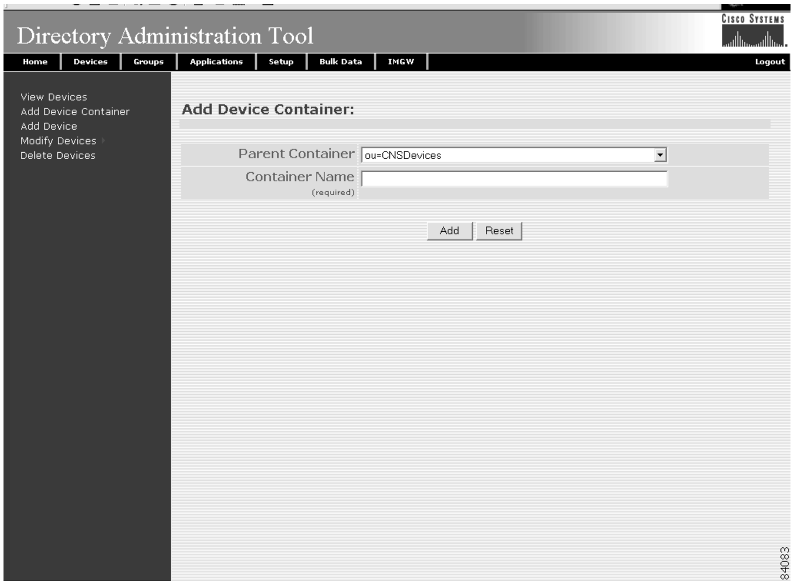
How to Add a Device Container

To add a device container, follow these steps:

Step 1 From the Device Management page, click **Add Device Container**.

The Add Device Container page appears (Figure 4-6).

Figure 4-6 Add Device Container



Add Device Container:

Parent Container	ou=CNSDevices
Container Name (required)	

Step 2 Select the appropriate Parent Container from the drop-down list.

Table 4-1 lists the valid values for this field.

Table 4-1 Valid Values for Add Device Container

Attribute	Description	Valid Values
Parent Container	Parent container for device objects in the context root.	From drop-down list
Container Name	The name used as **ou** (organizational unit) of the container.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 Enter a value in the **Container Name** field.

Step 4 To clear the field and enter a new value, click **Reset**.

Step 5 To add this device container, click **Add**.

Step 6 To return to the main menu, click the **Home** tab.

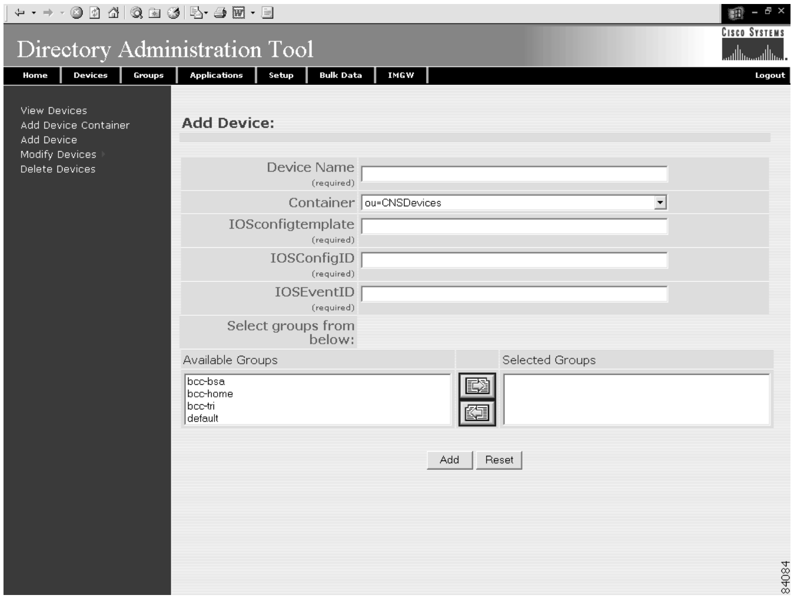
How to Add a Device

To add a device, follow these steps:

Step 1 From the Device Management page, click **Add Device**.

The Add Device page appears (see Figure 4-7)

Figure 4-7 Add Device



Add Device:

Device Name (required)	
Container	ou=CNSDevices
IOSconfigtemplate (required)	
IOSConfigID (required)	
IOSEventID (required)	
Select groups from below:	

Available Groups	Selected Groups
bcc-bsa bcc-home bcc-tri default	

Step 2 Enter a value in the **Device Name** field.

Table 4-2 lists valid values for the fields on this page.

Table 4-2 Valid Values for Add Device

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Container	Container for the device object.	From drop-down list
IOSconfigtemplate	Configuration template to associate with the device.	Non-empty String
IOSConfigID	Configuration ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
IOSEventID	Event ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 Enter a value in the **Device Name** field.

Step 4 Select a container from the Container pull-down menu.

Step 5 Enter a template ID for this device in the **IOSConfigtemplate** field.

Step 6 Enter a value for the unique configuration ID in the **IOSConfigID** field.

Step 7 Enter a value for the unique event ID in the **IOSEventID** field.

Step 8 From the **Available Groups** list, select the groups into which this device belongs.

Step 9 To clear all field and enter new values, click **Reset**.

Step 10 To add this device to the system, click **Add**.

Step 11 To return to the main menu, click the **Home** tab.

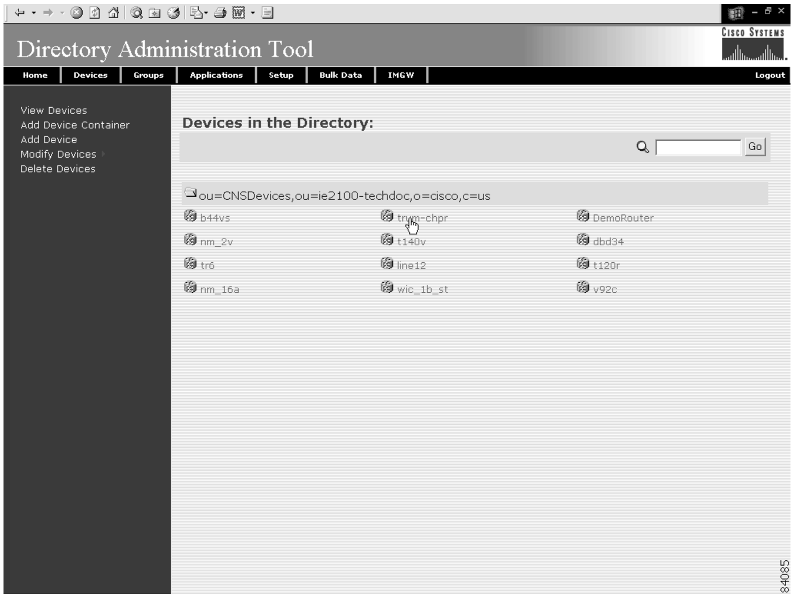
How to Modify Devices Details

To modify a device details, follow these steps:

Step 1 From the Device Management page, click **Modify Devices**.

The Devices in the Directory list appears (see Figure 4-8).

Figure 4-8 Devices in the Directory



Devices in the Directory:

ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

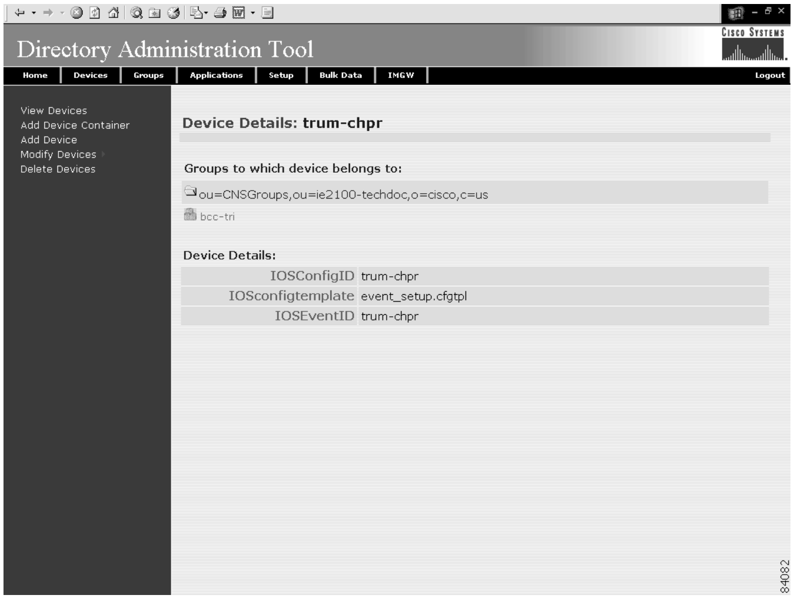
b44vs
trum-chpr
DemoRouter
nm_2v
t140v
dbd34
tr6
line12
t120r
nm_16a
wic_1b_st
v92c

Note Devices with no parent attributes are shown with a dully-shaded icon, so you can easily identify the devices with no groups associated.

Step 2 Click on the icon for the device you wish to modify.

The Device Details page appears (see Figure 4-9)

Figure 4-9 Device Details



Device Details: trum-chpr

Groups to which device belongs to:

ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

bcc-tri

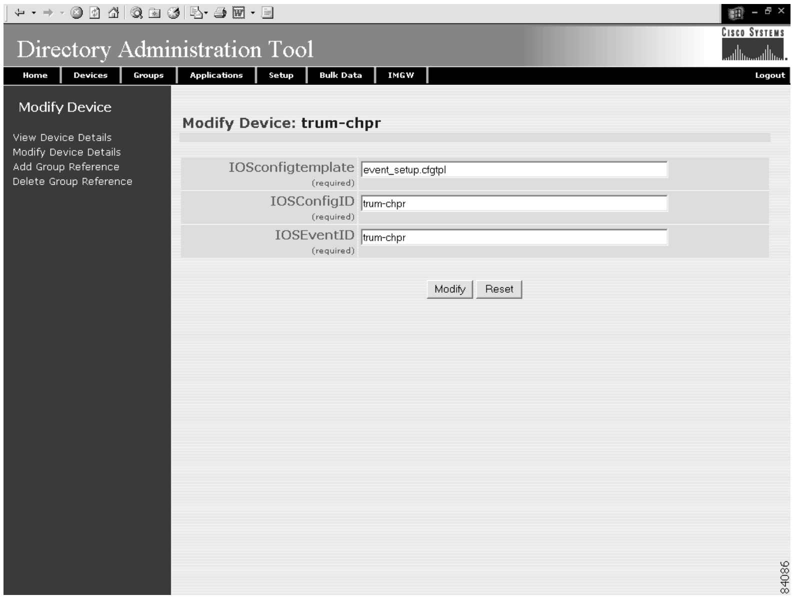
Device Details:

IOSConfigID	trum-chpr
IOSconfigtemplate	event_setup.cfgtpl
IOSEventID	trum-chpr

Step 3 To modify the detail information about this device, in the left side-bar menu, click **Modify Device Details**.

The Modify Device task page appears (see Figure 4-10).

Figure 4-10 Modify Task



Modify Device: trum-chpr

IOSconfigtemplate (required)	event_setup.cfgtpl
IOSConfigID (required)	trum-chpr
IOSEventID (required)	trum-chpr

Step 4 Modify all appropriate fields.

Table 4-3 lists valid values for these fields.

Table 4-3 Valid Values for Modify Device

Attribute	Description	Valid Values
IOSconfigtemplate	Configuration template to associate with the device.	Non-empty String
IOSConfigID	Configuration ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
IOSEventID	Event ID attribute of the device.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 5 To clear all field and enter new values, click **Reset**.

Step 6 To apply these changes to this device, click **Apply**.

Step 7 To return to the main menu, click the **Home** tab.

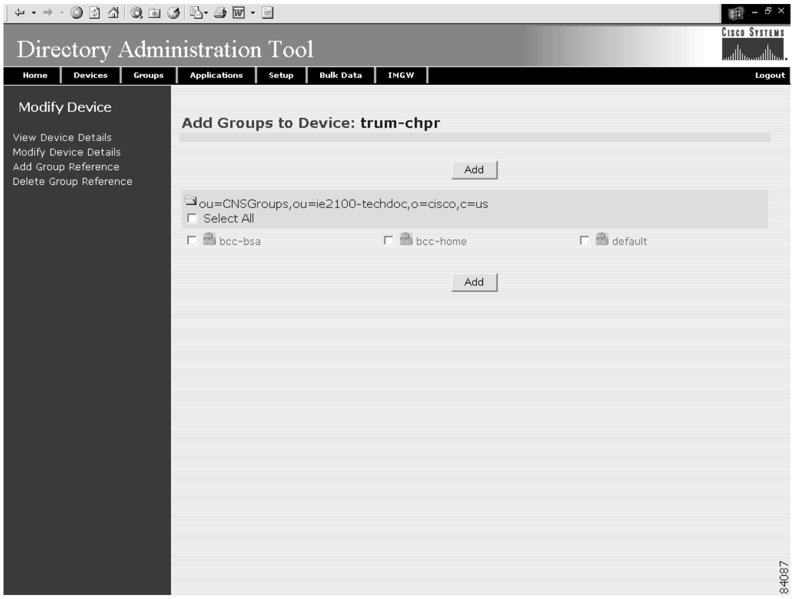
How to Add Device Group References to a Device

To add groups in which this device is referenced as a member, follow these steps:

Step 1 From the Modify Device page left side-bar menu, click **Add Group Reference**.

The Group Reference page appears (see Figure 4-11).

Figure 4-11 Add Groups to Device



Add Groups to Device: trum-chpr

ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

□ Select All

□ bcc-bsa □ bcc-home □ default

Step 2 Check the groups in which you want this device to appear.

Step 3 To apply these changes to this device, click **Add**.

Step 4 To return to the main menu, click the **Home** tab.

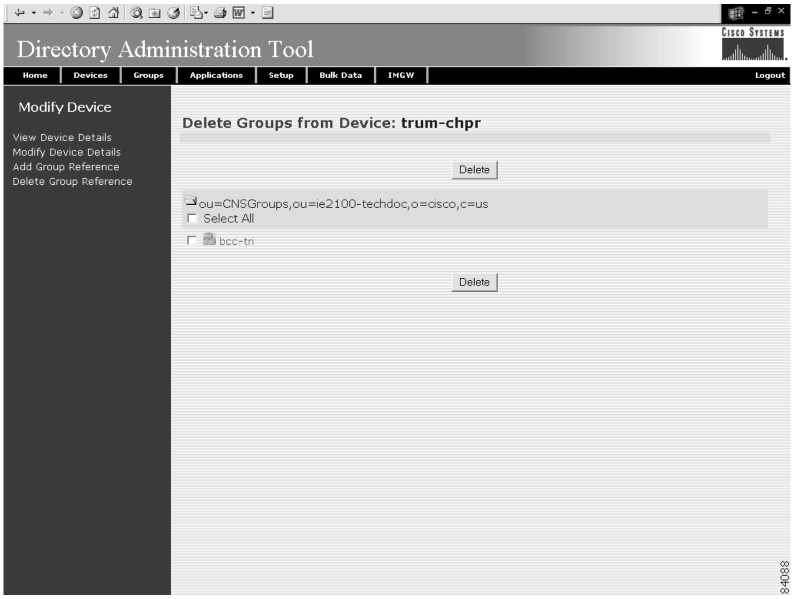
How to Delete Device Group References to a Device

To delete groups in which this device is referenced as a member, follow these steps:

Step 1 From the Modify Device page left side-bar menu, click **Delete Group Reference**.

The Delete Devices from Group page appears (see Figure 4-12).

Figure 4-12 Delete Devices from Group



Delete Groups from Device: trum-chpr

ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

□ Select All

□ bcc-tri

Step 2 Check those group references you want to delete.

Step 3 To these group references, click **Delete**.

Step 4 To return to the main menu, click the **Home** tab.

How to Delete Devices

The delete device function relative to groups is different for each type of directory.

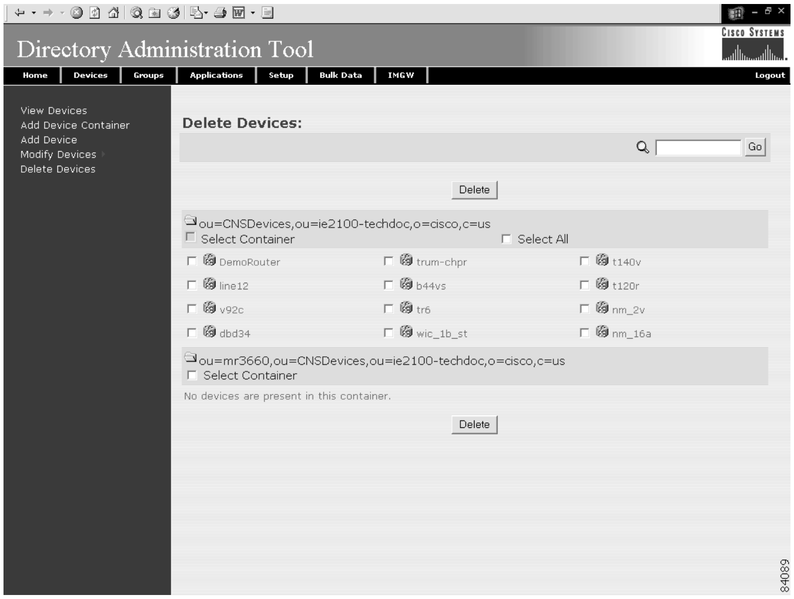
For Critical Path, NDS, and iPlanet, if the device is the only member of a group when you delete the device, the group remains in an empty state. However, the device reference is deleted from the group.

To delete devices from the system using DAT, follow these steps:

Step 1 From the Device Management page, click Delete Devices.

The Delete Devices page appears (see Figure 4-13)

Figure 4-13 Delete Devices



Delete Devices:

ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

□ Select Container □ Select All

□ DemoRouter	□ trum-chpr	□ t140v
□ line12	□ b44vs	□ t120r
□ v92c	□ tr6	□ nm_2v
□ dbd34	□ wic_1b_st	□ nm_16a

ou=mr3660,ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

□ Select Container

No devices are present in this container.

Note Devices with no parent attributes are shown with a dully-shaded icon, so you can easily identify the devices with no groups associated.

Step 2 Select the devices you want to delete from the system.

Step 3 To delete this device, click **Delete**.

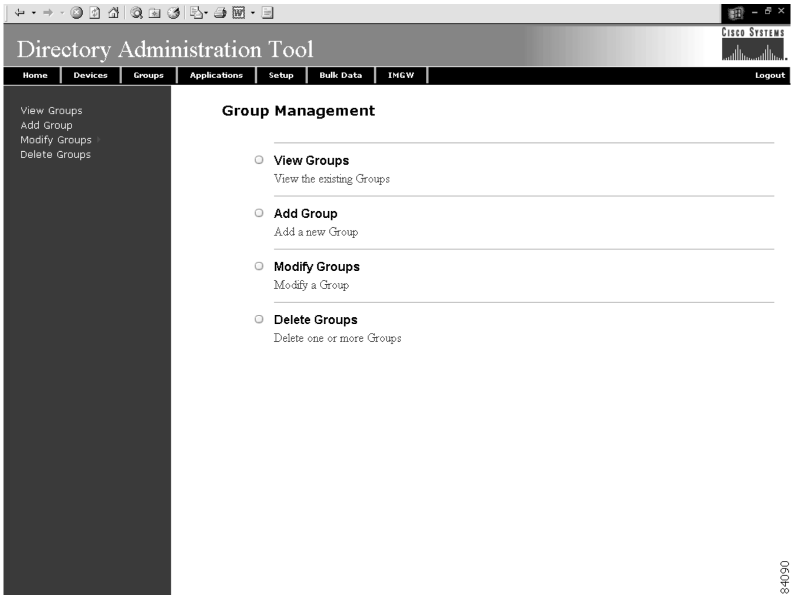
Step 4 To return to the main menu, click the **Home** tab.

How to Manage Groups

To manage groups in the system, from the main menu, click the **Groups** tab.

The Group Management page appears (see Figure 4-14).

Figure 4-14 Group Management



Group Management

- ○ **View Groups**
  View the existing Groups
- ○ **Add Group**
  Add a new Group
- ○ **Modify Groups**
  Modify a Group
- ○ **Delete Groups**
  Delete one or more Groups

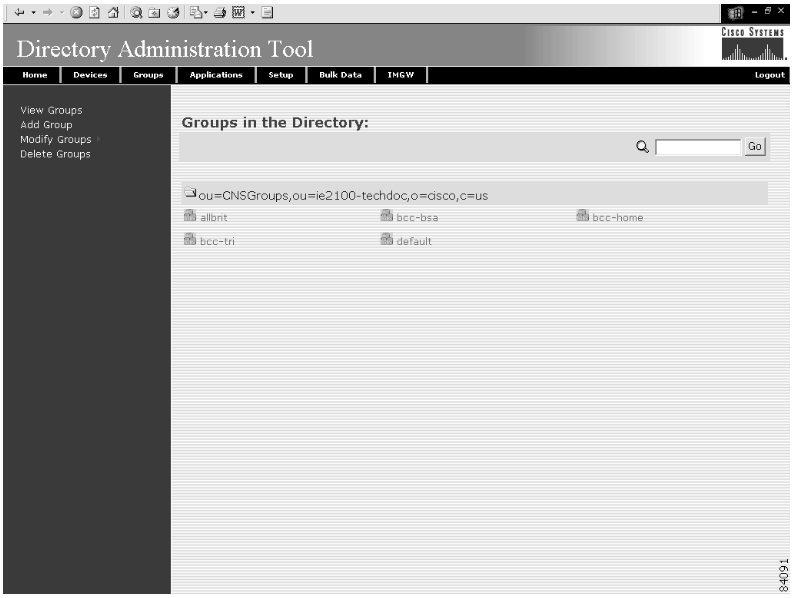
How to View Groups in the System

To view all the groups in the system, follow these steps:

Step 1 From the Group Management page, click **View Groups**.

The group listing appears (see Figure 4-15).

Figure 4-15 Groups in the System



Groups in the Directory:

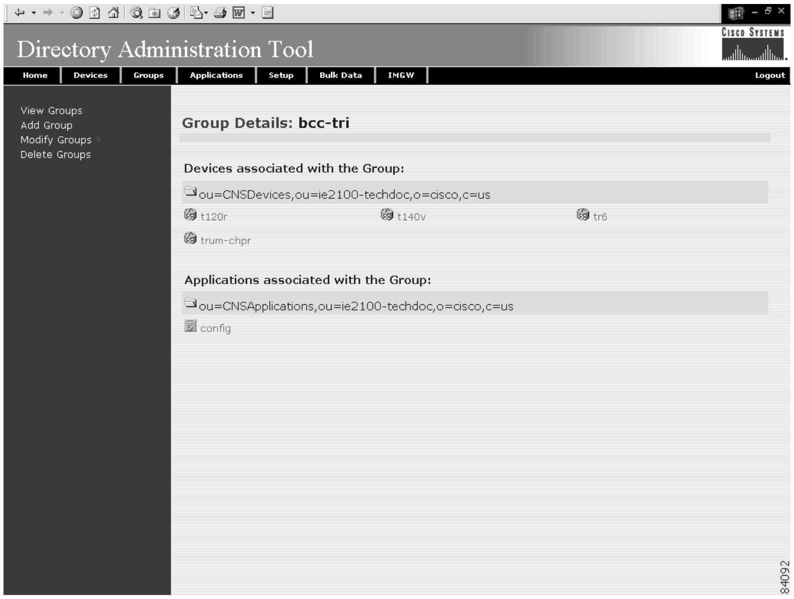
ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

allbrit	bcc-bsa	bcc-home
bcc-tri	default	

Step 2 To view the details of a particular group, click on the icon associated with the group you want to view.

The Groups Detail page appears (see Figure 4-16).

Figure 4-16 Groups Details



Group Details: bcc-tri

Devices associated with the Group:

ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

t120r t140v tr6

trum-chpr

Applications associated with the Group:

ou=CNSApplications,ou=ie2100-techdoc,o=cisco,c=us

config

Step 3 To return to the main menu, click the **Home** tab.

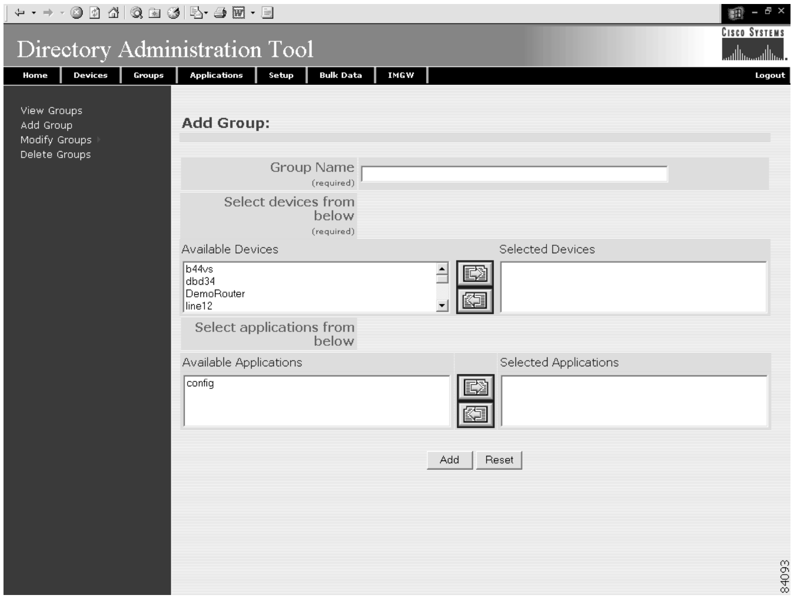
How to Add a Group

To add a group, follow these steps:

Step 1 From the Group Management page, click **Add Group**.

The Add Group page appears (see Figure 4-17).

Figure 4-17 Add Group



Step 2 Enter a value for the group name in the **Group Name** field.

Table 4-4 lists valid values for this field.

Table 4-4 Valid Values for Add Group

Attribute	Description	Valid Values
Group Name	The name used as **cn** (common name) of the Group.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 From the list of available devices, select the devices you want associated with this group.

Step 4 From the list of available applications, select the applications you want associated with this group.

Step 5 Modify all appropriate fields.

Step 6 To clear all field and enter new values, click **Reset**.

Step 7 To add this group, click **Add**.

Step 8 To return to the main menu, click the **Home** tab.

Modifying Groups

To modify a group, follow these steps:

Step 1 From the Group Management page, click **Modify Group**.

The Group list appears (see Figure 4-15).

Step 2 Click on the icon associated with the group you want to modify.

The group details appear (see Figure 4-16).

Step 3 From the left side-bar menu, choose which aspect of the group you want to modify.

Modifying Group Details

Using the user interface to modify group details (attributes) is possible only if you have extended the group objectclass in the directory with extra attributes.

How to Populate a Group Attribute

Before you can populate a group attribute, you must extend the directory schema manually. The Cisco CNS Configuration Engine 1.4 cannot add new attributes to the group objectclass in the directory.

Once you have extended the schema, you can populate the new object class using DAT by following these steps:

Step 1 In the DAT user interface, under **Group Setup**, click on **Add More Attributes to the UI**.

(See "How to View and Modify Group Setup" section on page 4-38.)

Step 2 Enter the new attributes.

Step 3 Click **Save**.

Now, when you go to **Modify Groups**, you can modify these new attributes under **Modify Group Details**.

How to Modify Group Details

To modify group details, follow these steps:

Step 1 From the Group Management page, click **Modify Groups**.

The group list appears (see Figure 4-15).

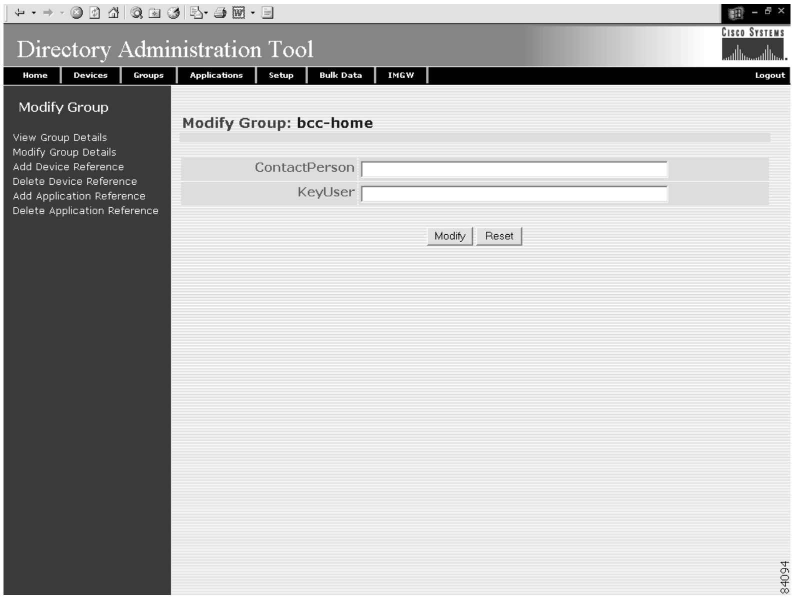
Step 2 Click on the icon associated with the group you want to modify.

The Group Details page appears (see Figure 4-16).

Step 3 To modify the group attributes, from the left side-bar menu, click on **Modify Group Details**.

The modify attributes task page appears (see Figure 4-18).

Figure 4-18 Modify Group Details



Modify Group: bcc-home

ContactPerson

KeyUser

Step 4 Modify all appropriate attributes.

Table 4-5 lists valid values for these fields.

Table 4-5 Valid Values for Modify Group Details

Attribute	Description	Valid Values
ContactPerson	Name of the primary contact person.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
KeyUser	Name of the primary contact person.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 5 To clear all field and enter new values, click **Reset**.

Step 6 To modify this group, click **Modify**.

Step 7 To return to the main menu, click the **Home** tab.

How to Add Device References to a Group

To add devices to a group, follow these steps:

Step 1 From the Group Management page, click **Modify Groups**.

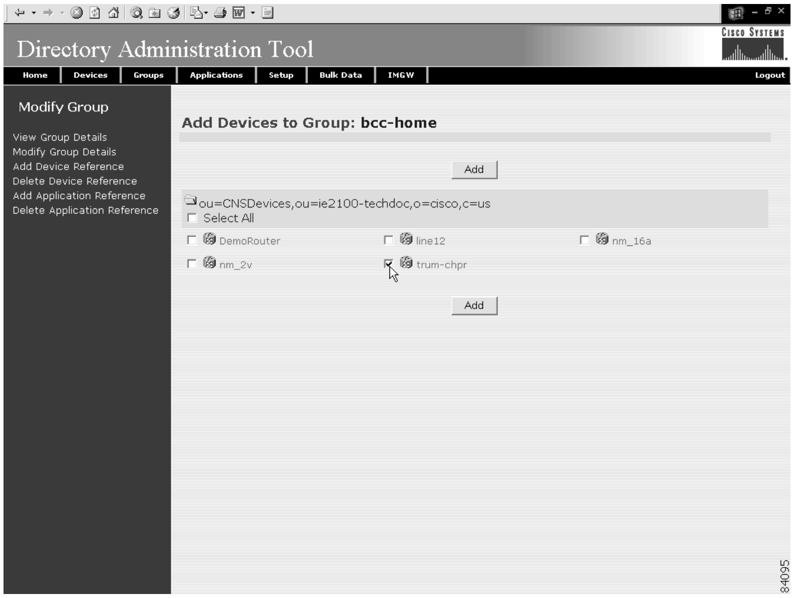
The group list appears (see Figure 4-15).

Step 2 Select the group you want to modify by clicking on its icon.

Step 3 To add devices to this group, from the left side-bar menu, click on **Add Device Reference**.

The device list appears (see Figure 4-19).

Figure 4-19 Add Devices to Group



Add Devices to Group: bcc-home

ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

□ Select All

□ DemoRouter	□ line12	□ nm_16a
□ nm_2v	☑ trum-chpr	

Step 4 Check all devices you want to appear in this group.

Step 5 To modify the group with these devices, click **Add**.

Step 6 To return to the main menu, click the **Home** tab.

How to Delete Devices from a Group

To delete devices to a group, follow these steps:

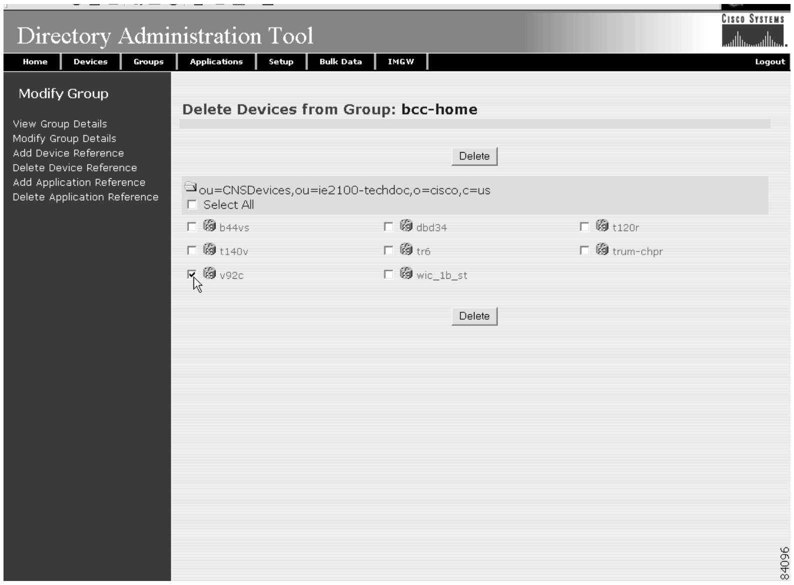
Step 1 From the Group Management page, click **Modify Groups**.

The group list appears (see Figure 4-15).

Step 2 Select the group you want to modify by clicking on its icon.

The list of devices currently associated with this group appears (see Figure 4-20).

Figure 4-20 Delete Devices from Group



Delete Devices from Group: bcc-home

ou=CNSDevices,ou=ie2100-techdoc,o=cisco,c=us

☐ Select All

☐ b44vs	☐ dbd34	☐ t120r
☐ t140v	☐ tr6	☐ trum-chpr
☑ v92c	☐ wic_1b_st	

Step 3 Check all devices you want to delete from this group.

Step 4 To delete these devices from this group, click **Delete**.

Step 5 To return to the main menu, click the **Home** tab.

How to Add Applications to a Group

To add applications to a group, follow these steps:

Step 1 From the Group Management page, click **Modify Groups**.

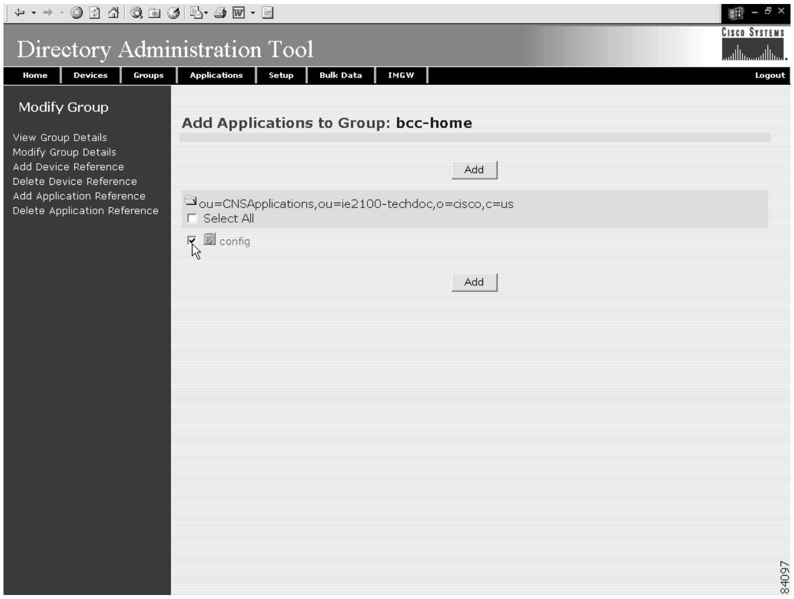
The group list appears (see Figure 4-15).

Step 2 Select the group you want to modify by clicking on its icon.

Step 3 To add applications to this group, from the left side-bar menu, click on **Add Application Reference**.

A list of applications appears (see Figure 4-21).

Figure 4-21 Add Applications to Group



Add Applications to Group: bcc-home

ou=CNSApplications,ou=ie2100-techdoc,o=cisco,c=us

□ Select All

☑ config

Step 4 Check the applications you want to add to this group.

Step 5 To modify the group with these applications, click **Add**.

Step 6 To return to the main menu, click the **Home** tab.

How to Delete Applications from a Group

To delete applications to a group, follow these steps:

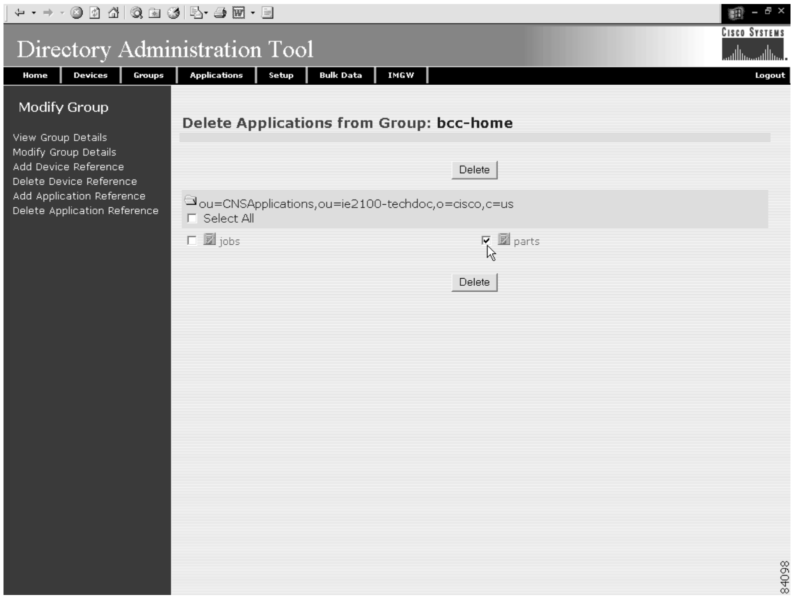
Step 1 From the Group Management page, click **Modify Groups**.

The group list appears (see Figure 4-15).

Step 2 Select the group you want to modify by clicking on its icon.

The list of applications currently associated with this group appears (see Figure 4-22).

Figure 4-22 Delete Applications from Group



Delete Applications from Group: bcc-home

ou=CNSApplications,ou=ie2100-techdoc,o=cisco,c=us

□ Select All

□ jobs ☑ parts

Step 3 Check the applications you want to delete from this group.

Step 4 To delete these applications from this group, click **Delete**.

Step 5 To return to the main menu, click the **Home** tab.

How to Delete Groups

To delete group(s) from the system using DAT, follow these steps:

Step 1 From the Device Management page, click Delete Groups.

The Delete Groups page appears

Step 2 Select the group(s) you want to delete from the system.

Step 3 To delete this group(s), click **Delete**.

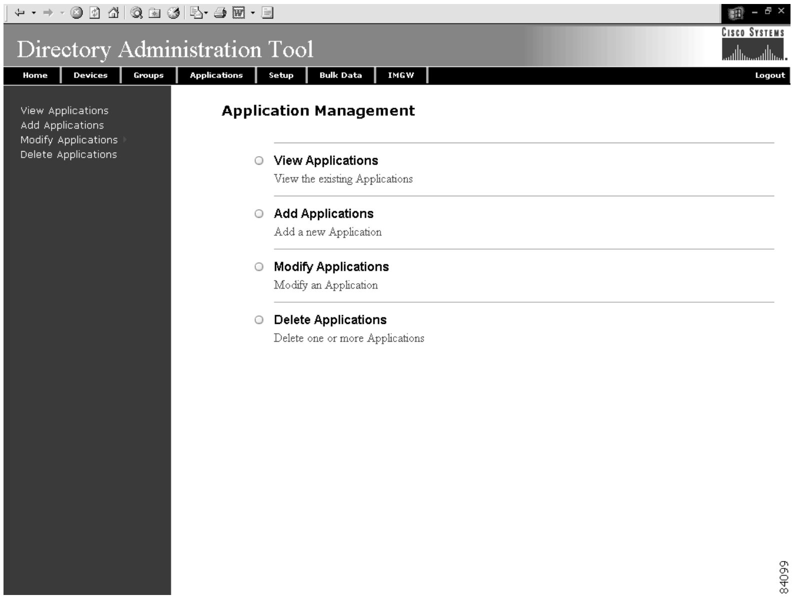
Step 4 To return to the main menu, click the **Home** tab.

How to Manage Applications

To view and modify applications, from the main menu, click the **Applications** tab.

The Application Management page appears (see Figure 4-23).

Figure 4-23 Application Management



Application Management

○ **View Applications**
View the existing Applications

○ **Add Applications**
Add a new Application

○ **Modify Applications**
Modify an Application

○ **Delete Applications**
Delete one or more Applications

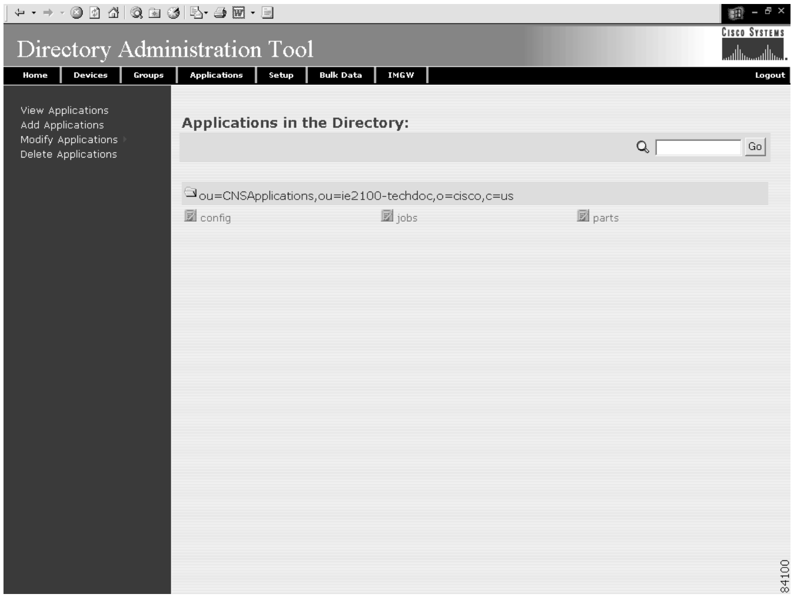
How to View Applications on the System

To view the current list of applications running on the system, follow these steps:

Step 1 From the Application Management page, click **View Applications**.

The application list appears (see Figure 4-24).

Figure 4-24 Applications List



Applications in the Directory:

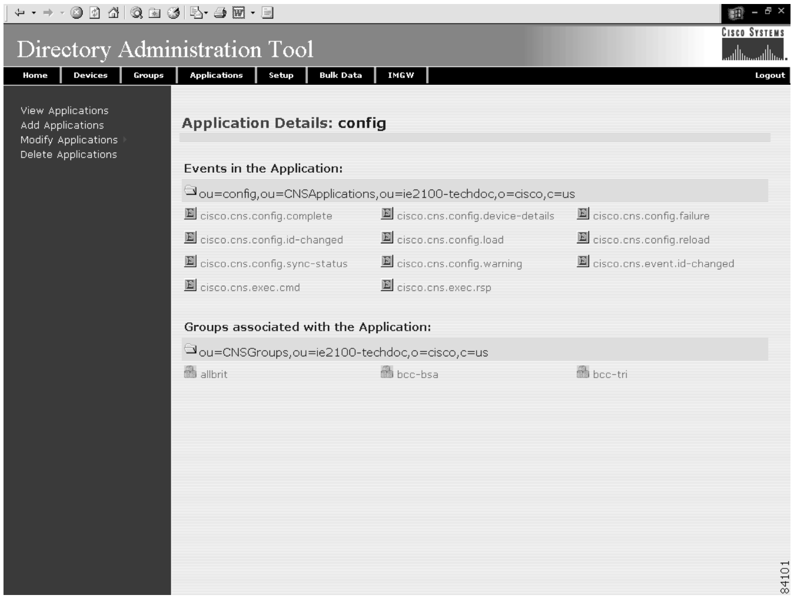
ou=CNSApplications,ou=ie2100-techdoc,o=cisco,c=us

config jobs parts

Step 2 To view the details of an application, click on the icon associated with application you want to view.

The application details appear (seeFigure 4-25) listing the events in the application and group currently associated with this application.

Figure 4-25 Application Details



Application Details: config

Events in the Application:

ou=config,ou=CNSApplications,ou=ie2100-techdoc,o=cisco,c=us

cisco.cns.config.complete	cisco.cns.config.device-details	cisco.cns.config.failure
cisco.cns.config.id-changed	cisco.cns.config.load	cisco.cns.config.reload
cisco.cns.config.sync-status	cisco.cns.config.warning	cisco.cns.event.id-changed
cisco.cns.exec.cmd	cisco.cns.exec.rsp	

Groups associated with the Application:

ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

allbrit	bcc-bsa	bcc-tri

Step 3 To return to the main menu, click the **Home** tab.

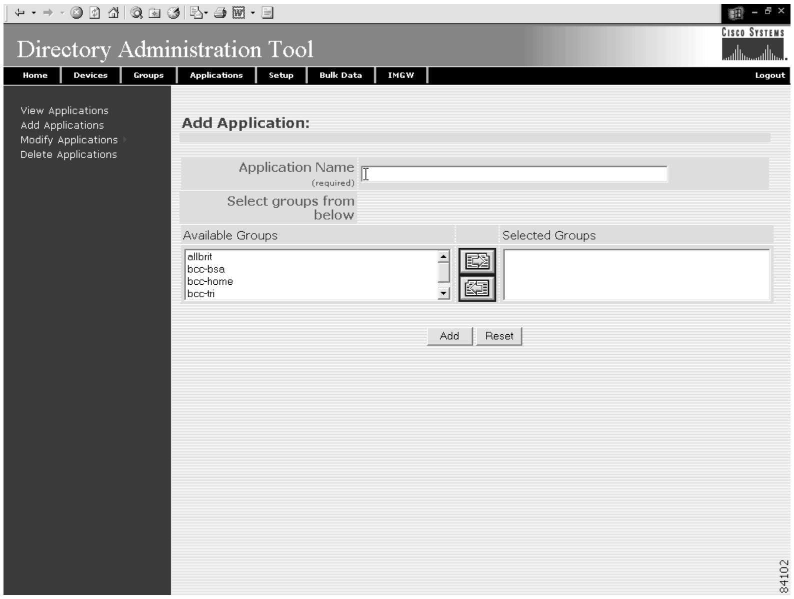
How to Add Applications

To add an application to the system, follow these steps:

Step 1 From the Application Management page, click **Add Application**.

The Add Application page appears (see Figure 4-26).

Figure 4-26 Add Applications



Step 2 Enter a value in the **Application Name** field.

Table 4-6 list the valid values for this field.

Table 4-6 Valid Values for Add Application

Attribute	Description	Valid Values
Application Name	The name used as **cn** (common name) of the Application.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 From the list of Available Groups, choose the groups with which you want this application associated.

Step 4 To clear your entries and start over, click **Reset**.

Step 5 To add this application to the system, click **Add**.

After adding an application, you get a success message with a link to add events to that application. Clicking the link takes you to the add events screen (see "How to Add Events to an Application" section on page 4-27).

Step 6 To return to the main menu, click the **Home** tab.

Modifying Applications

To modify an application, follow these steps:

Step 1 From the Application Management page, click **Modify Application**.

The Application list appears (see Figure 4-24).

Step 2 Click on the icon associated with the application you want to modify.

The application details appear (see Figure 4-25).

Step 3 From the left side-bar menu, choose which aspect of the application you want to modify.

Modifying Application Details

Using the user interface to modify application details (attributes) is possible only if you have extended the application objectclass in the directory with extra attributes.

How to Populate an Application Attribute

Before you can populate a application attribute, you must extend the directory schema manually. The Cisco CNS Configuration Engine 1.4 cannot add new attributes to the application objectclass in the directory.

Once you have extended the schema, you can populate the new object class using DAT by following these steps:

Step 1 In the DAT user interface, under **Application Setup**, click on **Add More Attributes to the UI**.

(See "How to View and Modify Application Setup" section on page 4-39.)

Step 2 Enter the new attributes.

Step 3 Click **Save**.

Now, when you go to **Modify Application**, you can modify these new attributes under **Modify Application Details**.

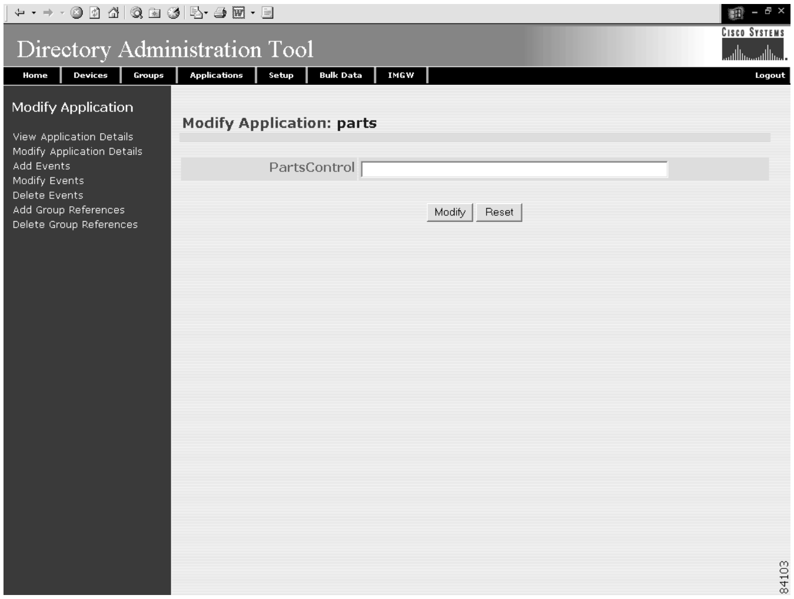
How to Modify Application Details

To modify application details (attributes), follow these steps:

Step 1 From the left side-bar menu, click **Modify Applications Details**.

The modify attributes task page appears.

Figure 4-27 Modify Application Details



Modify Application: parts

PartsControl

Step 2 Modify the application UI attribute as required.

Note The valid values could be anything that is supported by the schema of the directory.

Step 3 To clear all field and enter new values, click **Reset**.

Step 4 To modify this application, click **Modify**.

Step 5 To return to the main menu, click the **Home** tab.

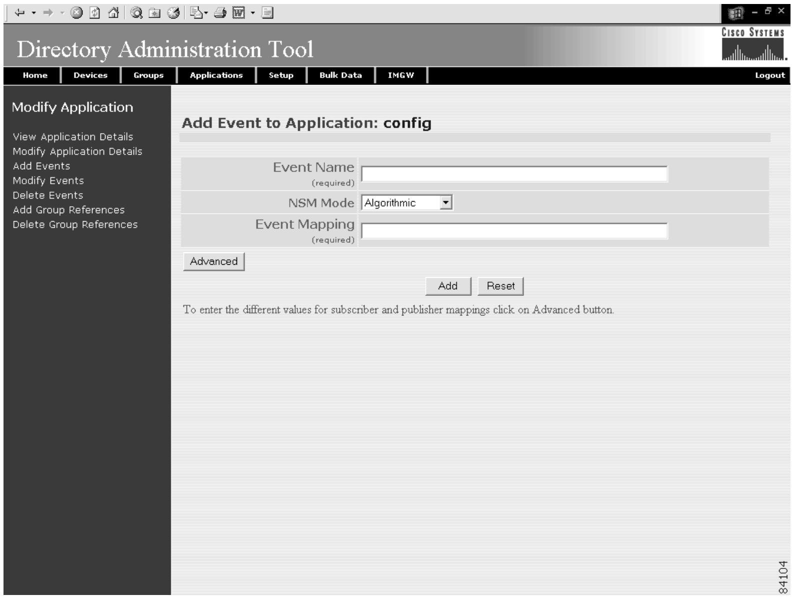
How to Add Events to an Application

To add events to this application, follow these steps:

Step 1 From the left side-bar menu, click **Add Events**.

The Add Events page appears (see Figure 4-28).

Figure 4-28 Add Events to an Application



Add Event to Application: config

Event Name (required)

NSM Mode Algorithmic

Event Mapping (required)

To enter the different values for subscriber and publisher mappings click on Advanced button.

Step 2 Enter a value in the **Event Name** field.

Table 4-7 lists valid values for these fields.

All the events that are added in the internal directory for **config** application are as follows:

cisco.mgmt.cns.config.complete

cisco.mgmt.cns.config.failure

cisco.mgmt.cns.config.warning

cisco.mgmt.cns.config.sync-status

cisco.mgmt.cns.config.reboot – deprecated. Use cisco.mgmt.cns.exec.reload instead.

cisco.mgmt.cns.config.load

cisco.mgmt.cns.config.id-changed

cisco.mgmt.cns-config-changed

cisco.mgmt.cns.config-changed.lost

Table 4-7 Valid Values for Event Add

Attribute	Description	Valid Values
Event Name	Name of the event that will be controlled by the selected application.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Table 4-7 Valid Values for Event Add

Attribute	Description	Valid Values
NSM Mode	If Algorithmic, specialize the mapping algorithmically, else, the field mapping gives the complete mapping list for a subscriber/publisher.	From drop-down list
Event Mapping	Mapping of the given event to be returned to a subscriber or publisher application.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 From the NSM Mode pull down menu, choose a mode.

- Algorithmic — NSM server uses a mapping algorithm
- Non-algorithmic — NSM server mapping algorithm is overridden by the application

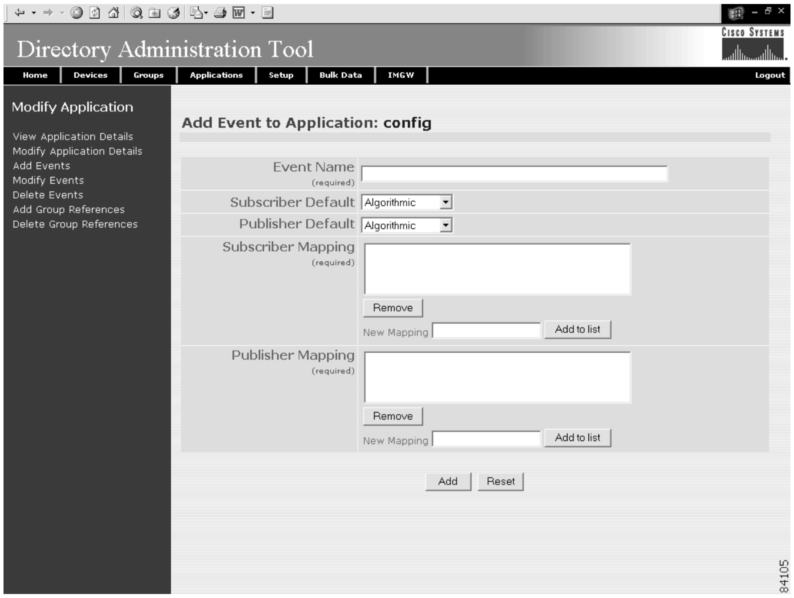
Step 4 Enter the event mapping in the **Event Mapping** field.

For more information about naming events, see “NameSpace Mapper” section on page 1-7.

Step 5 To change Subscriber and Publisher parameters from default, click **Advanced**.

The Advanced Event page appears (see Figure 4-29).

Figure 4-29 Advanced Event Add



Add Event to Application: config

Event Name (required)

Subscriber Default: Algorithmic

Publisher Default: Algorithmic

Subscriber Mapping (required)

New Mapping

Publisher Mapping (required)

New Mapping

Step 6 Enter a value in the **Event Name** field.

Table 4-8 lists valid values for these fields.

Table 4-8 Valid Values for Advanced Event Add

Attribute	Description	Valid Values
Event Name	Name of the event that will be controlled by the selected application.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Subscriber Default	If Algorithmic, specialize the mapping algorithmically, else, the field mapping gives the complete mapping list for a subscriber/publisher.	From drop-down list
Publisher Default	If Algorithmic, specialize the mapping algorithmically, else, the field mapping gives the complete mapping list for a subscriber/publisher.	From drop-down list
Subscriber Mapping (New Mapping)	Mapping list for subscriber	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Publisher Mapping (New Mapping)	Mapping list for publisher	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 7 Select the Subscriber Default mode from the pull down menu.

Step 8 Select the Publisher Default mode from the pull down menu.

Step 9 To add a new subscriber mapping, enter the subscriber mapping in the **New Mapping** field, the click **Add to list**.

Step 10 To remove a subscriber mapping, in the **Subscriber Mapping** list, select the desired mapping, then click **Remove**.

Step 11 To add a new publisher mapping, enter the publisher mapping in the **New Mapping** field, the click **Add to list**.

Step 12 To remove a publisher mapping, in the **Publisher Mapping** list, select the desired mapping, then click **Remove**.

Step 13 To add this event to the system, click **Add**.

Step 14 To clear your entries and start over, click **Reset**.

Step 15 To return to the main menu, click the **Home** tab.

How to Modify Events in an Application

To modify events to this application, follow these steps:

Step 1 From the Application Management page, click **Modify Application**.

The application list appears (see Figure 4-24).

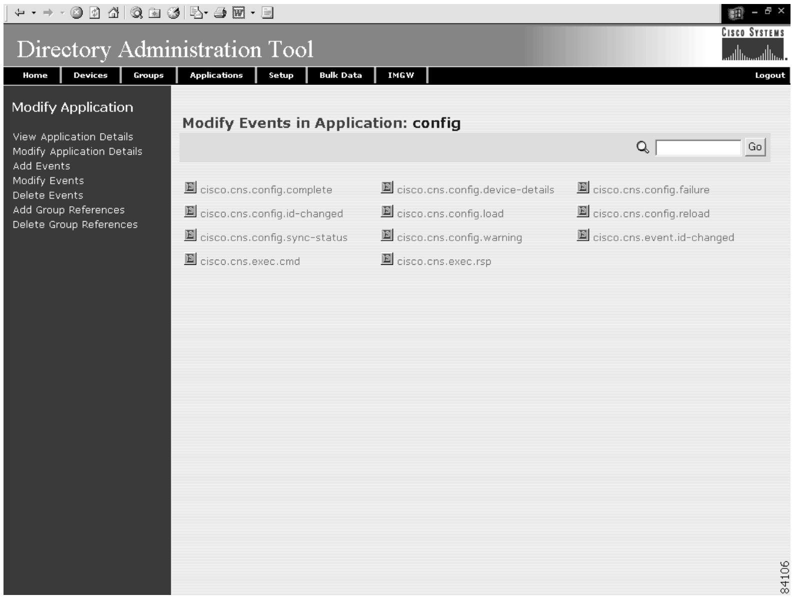
Step 2 Click on the icon associated with the application for which you want to modify events.

The Application Details page appears (see Figure 4-25).

Step 3 From the left side-bar menu, click **Modify Events**.

The events list for this application appears (see Figure 4-30).

Figure 4-30 Modify Events in Application



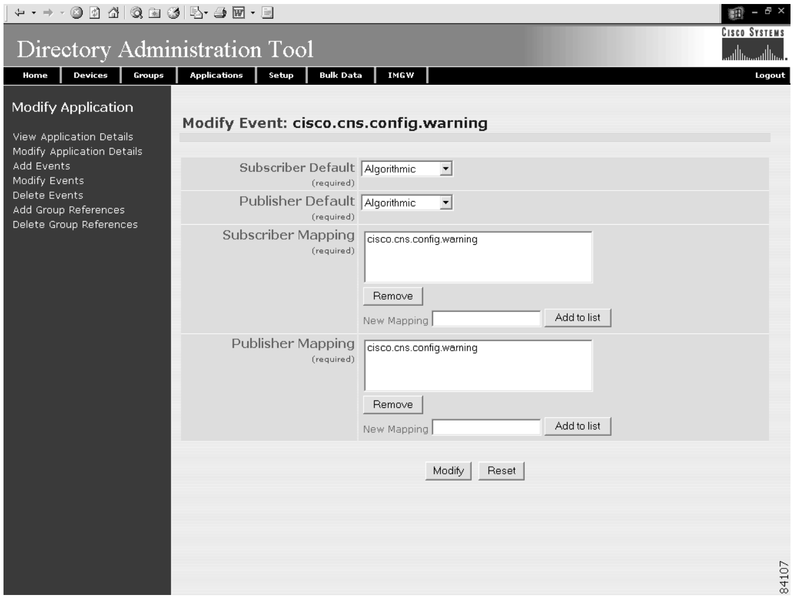
Modify Events in Application: config

cisco.cns.config.complete	cisco.cns.config.device-details	cisco.cns.config.failure
cisco.cns.config.id-changed	cisco.cns.config.load	cisco.cns.config.reload
cisco.cns.config.sync-status	cisco.cns.config.warning	cisco.cns.event.id-changed
cisco.cns.exec.cmd	cisco.cns.exec.rsp	

Step 4 Click on the icon associated with the event you want to modify.

The Modify Event page appears (see Figure 4-31).

Figure 4-31 Modify Event



Modify Event: cisco.cns.config.warning

Subscriber Default (required): Algorithmic

Publisher Default (required): Algorithmic

Subscriber Mapping (required): cisco.cns.config.warning

New Mapping

Publisher Mapping (required): cisco.cns.config.warning

New Mapping

Step 5 Modify all appropriate fields.

Table 4-9 lists valid values for these fields.

Table 4-9 Valid Values for Modify Event

Attribute	Description	Valid Values
Subscriber Default	If Algorithmic, specialize the mapping algorithmically, else, the field mapping gives the complete mapping list for a subscriber/publisher.	From drop-down list
Publisher Default	If Algorithmic, specialize the mapping algorithmically, else, the field mapping gives the complete mapping list for a subscriber/publisher.	From drop-down list
Subscriber Mapping (New Mapping)	Mapping list for subscriber	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Publisher Mapping (New Mapping)	Mapping list for publisher	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 6 To clear your entries and start over, click **Reset**.

Step 7 To Modify this event, click **Modify**.

Step 8 To return to the main menu, click the **Home** tab.

How to Delete Events in a Application

To delete events from an application, follow these steps:

Step 1 From the Application Management page, click **Modify Application**.

The application list appears (see Figure 4-24).

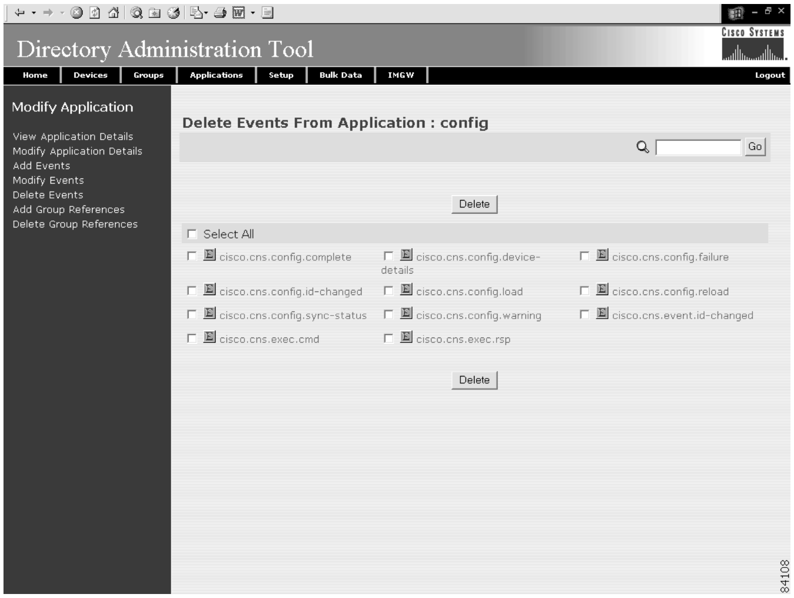
Step 2 Click on the icon associated with the application from which you want to delete events.

The Application Details page appears (see Figure 4-25).

Step 3 From the left side-bar menu, click **Delete Events**.

The delete events list for this application appears (see Figure 4-32).

Figure 4-32 Delete Events from Application



Delete Events From Application : config

☐ Select All

☐ cisco.cns.config.complete ☐ cisco.cns.config.device-details ☐ cisco.cns.config.failure
☐ cisco.cns.config.id-changed ☐ cisco.cns.config.load ☐ cisco.cns.config.reload
☐ cisco.cns.config.sync-status ☐ cisco.cns.config.warning ☐ cisco.cns.event.id-changed
☐ cisco.cns.exec.cmd ☐ cisco.cns.exec.rsp

Step 4 Check all events you want to delete from this application.

Step 5 To delete these events, click **Delete**.

Step 6 To return to the main menu, click the **Home** tab.

How to Add Group References to an Application

To add group references to an application, follow these steps:

Step 1 From the Application Management page, click **Modify Application**.

The application list appears (see Figure 4-24).

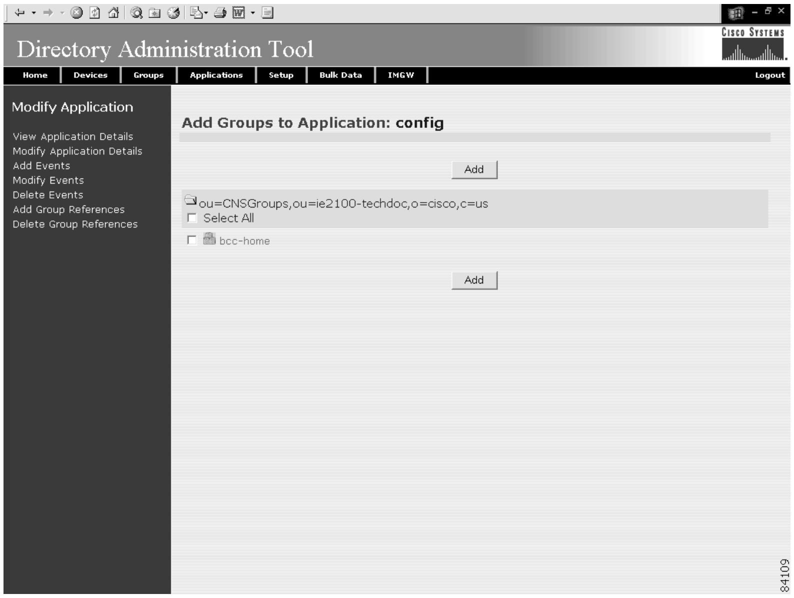
Step 2 Click on the icon associated with the application from which you want to add groups.

The Application Details page appears (see Figure 4-25).

Step 3 From the left side-bar menu, click **Add Group References**.

A list of available groups to add to this application appears (see Figure 4-33).

Figure 4-33 Add Groups to an Application



Add Groups to Application: config

ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

□ Select All

□ bcc-home

Step 4 Check all groups you want associated with this application.

Step 5 To add these group references to this application, click **Add**.

Step 6 To return to the main menu, click the **Home** tab.

How to Delete Group References from an Application

To delete group references from an application, follow these steps:

Step 1 From the Application Management page, click **Modify Application**.

The application list appears (see Figure 4-24).

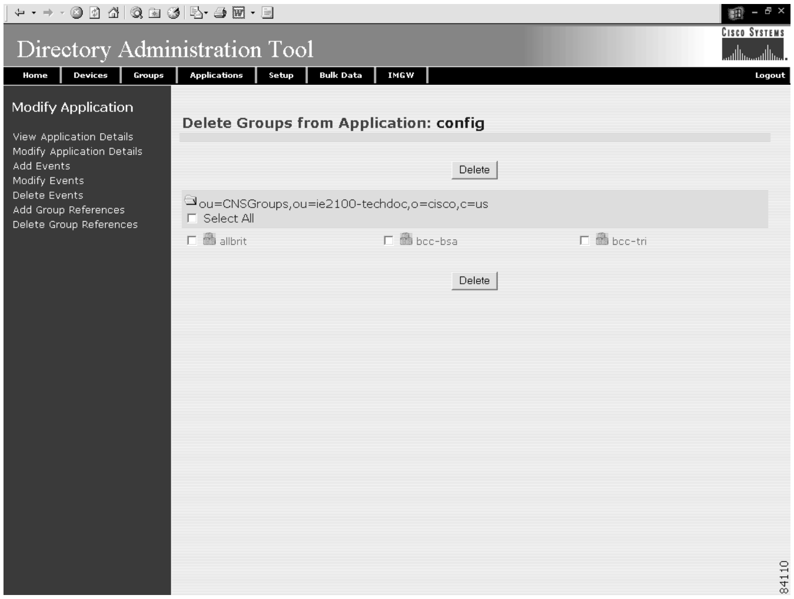
Step 2 Click on the icon associated with the application from which you want to delete groups.

The Application Details page appears (see Figure 4-25).

Step 3 From the left side-bar menu, click **Delete Group References**.

A list of groups currently associated with this application appears (see Figure 4-34).

Figure 4-34 Delete Groups from an Application



Delete Groups from Application: config

ou=CNSGroups,ou=ie2100-techdoc,o=cisco,c=us

☐ Select All

☐ allbrit ☐ bcc-bsa ☐ bcc-tri

Step 4 Check all groups you want to delete from this application.

Step 5 To delete these groups to this application, click **Delete**.

Step 6 To return to the main menu, click the **Home** tab.

How to Delete Applications

To delete an application, follow these steps:

Step 1 From the Application Management page, click **Delete Application**.

The Application list appears (see Figure 4-24).

Step 2 Click the icon(s) associated with the application you want to delete.

Step 3 To delete these applications, click **Delete**.

Step 4 To return to the main menu, click the **Home** tab.

Managing Directory Setup

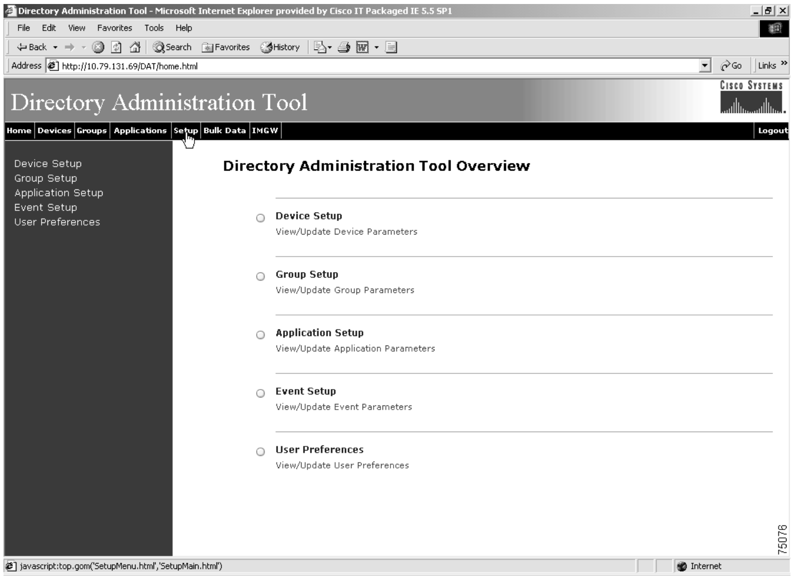
When the Cisco CNS Configuration Engine 1.4 is setup, DAT also gets configured with the values as entered by the user during setup. If you have extended the schema, then you have to provide the information about the new attributes (name of the attribute, whether the attribute is mandatory or not, and whether the attribute is single-valued or multi-valued).

Note Adding attributes in setup does not add these attributes to the directory. These attributes are written only to the DAT property files.

There are some attributes related to directories that get default values during initial setup of the system. You may need to change some of these attributes to match your specific values.

From the DAT main menu, click the Setup tag. The Setup page appears (see Figure 4-35).

Figure 4-35 Setup Page


Directory Administration Tool - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.79.131.69/DAT/home.html
Go Links
Directory Administration Tool
Cisco Systems
Home Devices Groups Applications Setup Bulk Data IMGW
Logout
Device Setup
Group Setup
Application Setup
Event Setup
User Preferences
Directory Administration Tool Overview
Device Setup
View/Update Device Parameters
Group Setup
View/Update Group Parameters
Application Setup
View/Update Application Parameters
Event Setup
View/Update Event Parameters
User Preferences
View/Update User Preferences
75076
javascript:top.gom('SetupMenu.html','SetupMain.html')
Internet

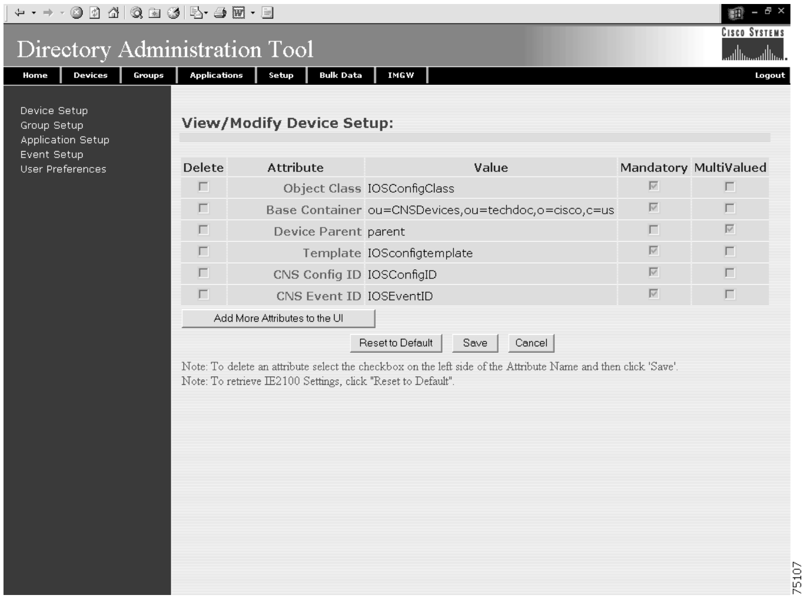
How to View and Modify Device Setup

To view and modify device setup, follow these steps:

Step 1 From the Setup main menu, choose, **Device Setup**.

The Device Setup page appears (see Figure 4-36).

Figure 4-36 View and Modify Device Setup



View/Modify Device Setup:

Delete	Attribute	Value	Mandatory	MultiValued
☐	Object Class	IOSConfigClass	☑	☐
☐	Base Container	ou=CNSDevices,ou=techdoc,o=cisco,c=us	☑	☐
☐	Device Parent	parent	☐	☑
☐	Template	IOSconfigtemplate	☑	☐
☐	CNS Config ID	IOSConfigID	☑	☐
☐	CNS Event ID	IOSEventID	☑	☐

Note: To delete an attribute select the checkbox on the left side of the Attribute Name and then click 'Save'.
Note: To retrieve IE2100 Settings, click "Reset to Default".

Step 2 To modify device setup, change all appropriate fields.

With this page, you can add new attributes that you intend to populate through DAT. The names of the other attributes; template, uniqueconfigid, uniquedeviceid, Parent (device-group association) are also listed in this page.These values are the same as entered during the Cisco CNS Configuration Engine 1.4 setup. These attributes are made mandatory. To change any of these values, the Cisco CNS Configuration Engine 1.4 setup has to be run again. These are the attributes that DAT recognizes initially.If you want more attributes to be managed by DAT, you can add those attribute details on this page.

Step 3 To add more attributes, click **Add More Attributes to the UI**.

Here you can add more attributes to the Device objectClass. You can add new attributes to a Device by giving the attribute name and whether it is mandatory, multi valued.

Note Adding attributes in setup does not add these attributes to the directory. These attributes are written only to the DAT property files. Before you can use the DAT UI to populate a newly added attribute, directory schema must have been extended with that new attribute.

Step 4 To reset this device setup to default values, click **Reset to Default**.

This restores the Cisco CNS Configuration Engine 1.4 settings for only device setup.

Step 5 To save your changes, click **Save**.

Step 6 To cancel this task, click **Cancel**.

Step 7 To return to the main menu, click the **Home** tab.

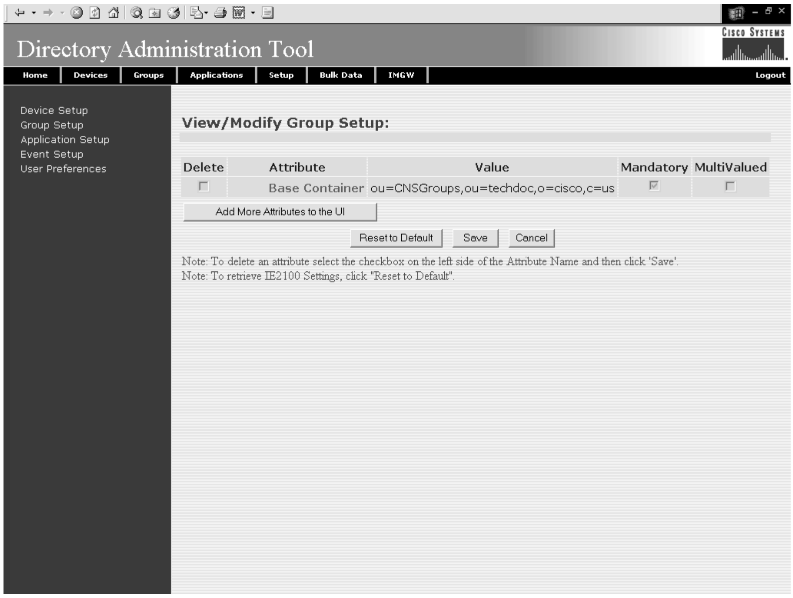
How to View and Modify Group Setup

To view and modify group setup, follow these steps:

Step 1 From the Setup main menu, choose, **Group Setup**.

The Group Setup page appears (see Figure 4-37).

Figure 4-37 View and Modify Group Setup



View/Modify Group Setup:

Delete	Attribute	Value	Mandatory	MultiValued
□	Base Container	ou=CNSGroups,ou=techdoc,o=cisco,c=us	☑	□

Note: To delete an attribute select the checkbox on the left side of the Attribute Name and then click 'Save'.
Note: To retrieve IE2100 Settings, click "Reset to Default".

Step 2 To add more attributes, click **Add More Attributes to the UI**.

Here you can add new attributes to the group objectClass; for example, you might be interested in designating a contact person for each of the groups. This can be done by adding an attribute to the group object class in the directory. You can add new attributes to a group by giving the attribute name and whether it is mandatory, or multi valued.

Note Adding attributes in setup does not add these attributes to the directory. These attributes are written only to the DAT property files. Before you can use the DAT UI to populate a newly added attribute, directory schema must have been extended with that new attribute.

Step 3 To reset this group setup to default values, click **Reset to Default**.

This restores the Cisco CNS Configuration Engine 1.4 settings for only group setup.

Step 4 To save your changes, click **Save**.

Step 5 To cancel this task, click **Cancel**.

Step 6 To return to the main menu, click the **Home** tab.

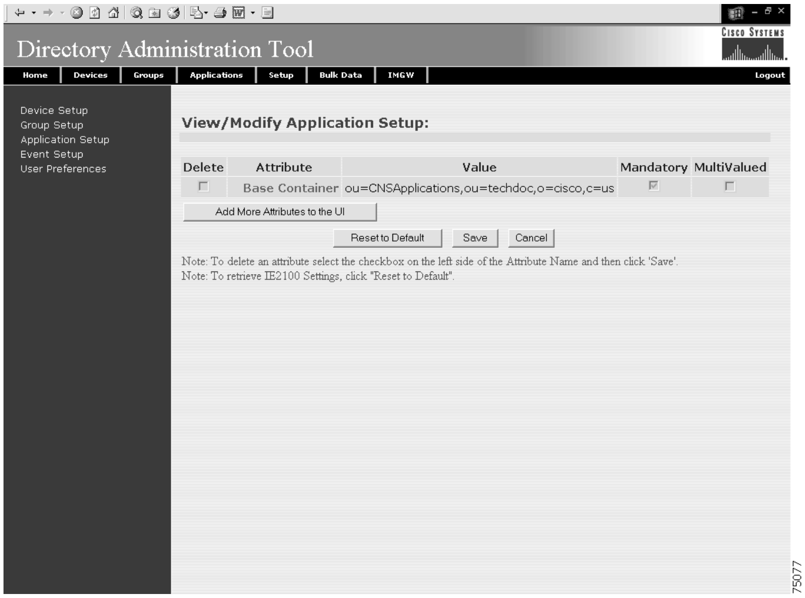
How to View and Modify Application Setup

To view and modify application setup, follow these steps:

Step 1 From the Setup main menu, choose, **Application Setup**.

The Application Setup page appears (see Figure 4-38).

Figure 4-38 View and Modify Application Setup



View/Modify Application Setup:

Delete	Attribute	Value	Mandatory	MultiValued
□	Base Container	ou=CNSApplications,ou=techdoc,o=cisco,c=us	☑	□

Note: To delete an attribute select the checkbox on the left side of the Attribute Name and then click 'Save'.
Note: To retrieve IE2100 Settings, click "Reset to Default".

Step 2 Click **Save**.

Step 3 To add more attributes, click **Add More Attributes to the UI**.

Here you can add more attributes to the application objectClass; for example, you might be interested in designating a contact person for each of the applications. This can be done by adding an attribute to the application object class in the directory. You can add new attributes to applications by giving the attribute name and whether it is mandatory, or multi valued.

Note Adding attributes in setup does not add these attributes to the directory. These attributes are written only to the DAT property files. Before you can use the DAT UI to populate a newly added attribute, directory schema must have been extended with that new attribute.

Step 4 To reset this application setup to default values, click **Reset to Default**.

This restores theCisco CNS Configuration Engine 1.4 settings for only application setup.

Step 5 To save your changes, click **Save**.

Step 6 To cancel this task, click **Cancel**.

Step 7 To return to the main menu, click the **Home** tab.

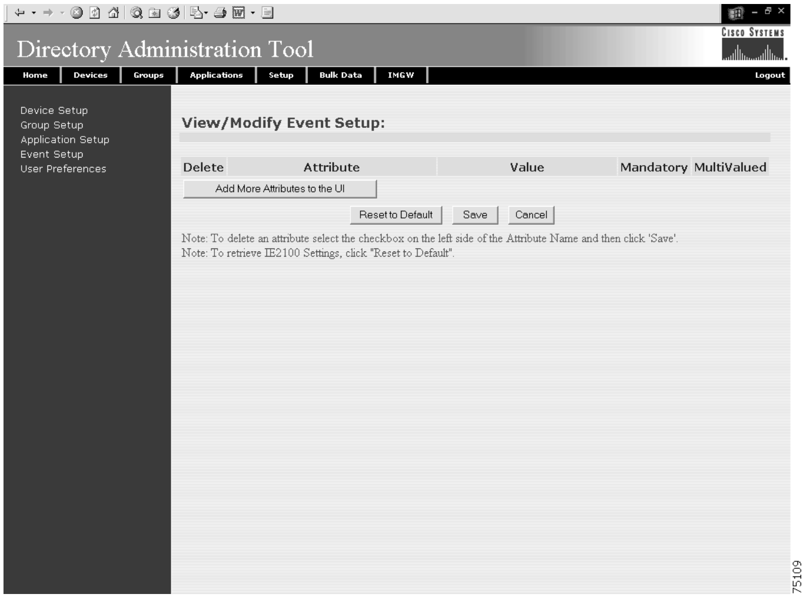
How to View and Modify Event Setup

To view and modify Event setup, follow these steps:

Step 1 From the Setup main menu, choose, **Event Setup**.

The Event Setup page appears (see Figure 4-39).

Figure 4-39 View and Modify Event Setup



View/Modify Event Setup:

Delete	Attribute	Value	Mandatory	MultiValued

Note: To delete an attribute select the checkbox on the left side of the Attribute Name and then click 'Save'.
Note: To retrieve IE2100 Settings, click "Reset to Default".

Step 2 To modify event setup, change all appropriate fields.

If you use the default NSM schema, you will notice that there are no fields to be modified here. This is because there are no attributes required for the event object class. However if you have extended the schema and added some extra attributes to the event object class then you can modify those attributes by changing the name of the attribute in the **Value** text box and updating the Mandatory and MultiValued check boxes.

Step 3 To add more attributes, click **Add More Attributes to the UI**.

Here you can add more attributes to the event objectClass; for example, you might be interested in adding an extra event to the object class. This can be done by adding an attribute to the event object class in the directory. You can add new attributes to events by giving the attribute name and whether it is mandatory, or multi valued.

Note Adding attributes in setup does not add these attributes to the directory. These attributes are written only to the DAT property files. Before you can use the DAT UI to populate a newly added attribute, directory schema must have been extended with that new attribute.

Step 4 To save your changes, click **Save**.

Step 5 To cancel this task, click **Cancel**.

Step 6 To return to the main menu, click the **Home** tab.

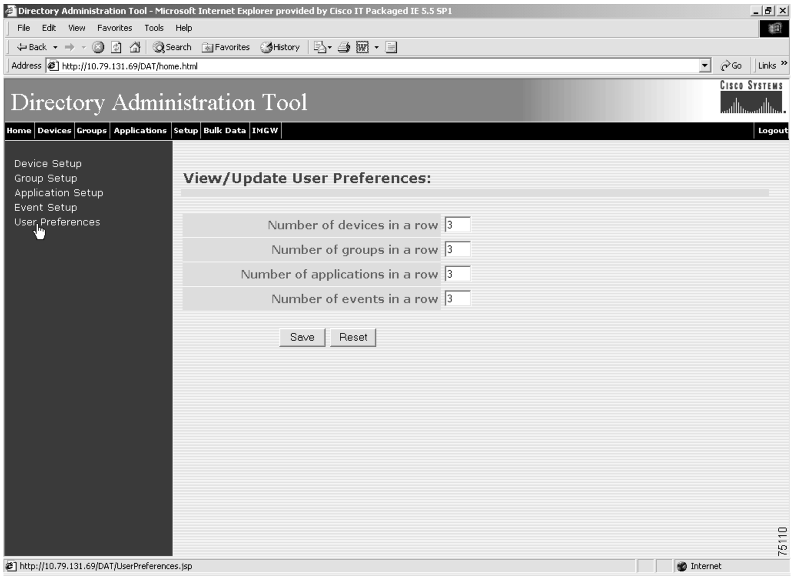
How to View and Modify User Preferences

To view and modify user preferences, follow these steps:

Step 1 From the Setup main menu, choose, **User Preferences**.

The User Preferences page appears (see Figure 4-40).

Figure 4-40 View and Modify User Preferences


Directory Administration Tool - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.79.131.69/DAT/home.html
Go Links
Directory Administration Tool
Cisco Systems
Home Devices Groups Applications Setup Bulk Data IMGW Logout
Device Setup
Group Setup
Application Setup
Event Setup
User Preferences
Save Reset
75110
http://10.79.131.69/DAT/UserPreferences.jsp
Internet

View/Update User Preferences:

Number of devices in a row 3
Number of groups in a row 3
Number of applications in a row 3
Number of events in a row 3

Step 2 To modify user preferences, change all appropriate fields.

This consists of the following options:

- Number of devices in a row
- Number of groups in a row
- Number of applications in a row
- Number of events in a row.

These options can be changed by changing the value in the text box.

Step 3 To save your changes, click **Save**.

Step 4 To cancel this task, click **Cancel**.

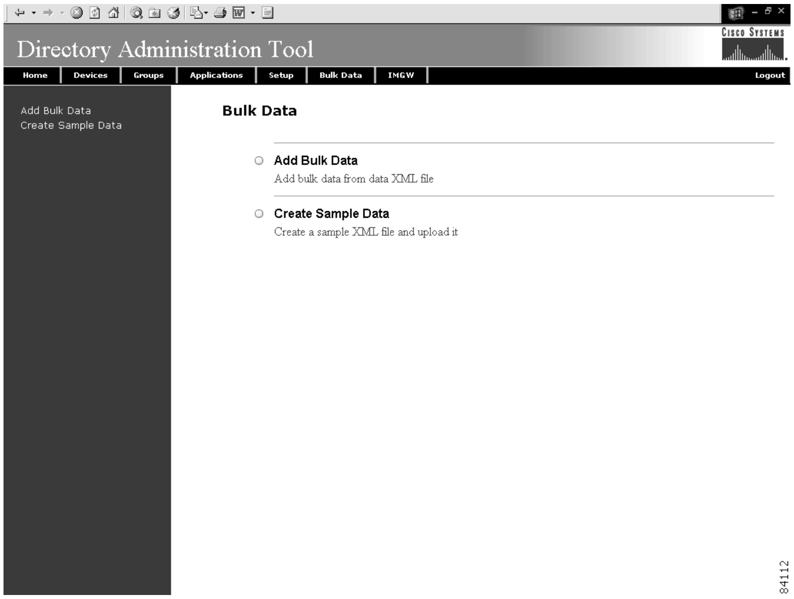
Step 5 To return to the main menu, click the **Home** tab.

How to Manage Bulk Data

To manage bulk data loads, from the main menu, click the **Bulk Data** tab.

The Bulk Data main menu appears (see Figure 4-41).

Figure 4-41 Bulk Data



XML DTD

The following example shows the Document Type Definition (DTD) for the XML bulk upload:

```
<?xml version="1.0" encoding="utf-8"?>
<!ELEMENT cns-bulk-upload (cns-element-data)>
<!ATTLIST cns-bulk-upload
    stop-on-error (true | false) "false"
>
<!ELEMENT cns-element-data ( NSM-DATA | IMGW-DATA | IMAGE-DATA)>
<!ELEMENT IMGW-DATA (imgw-device*)>
<!ATTLIST IMGW-DATA
    op-type (add) #REQUIRED
>
<!ELEMENT imgw-device (device-id, gateway-id?, device-type, hop-information*)>
<!ELEMENT device-id (#PCDATA)>
<!ELEMENT gateway-id (#PCDATA)>
<!ELEMENT device-type (#PCDATA)>
<!ELEMENT hop-information (hop-type, ip-address?, port?, username?, password?)>
<!ELEMENT hop-type (#PCDATA)>
<!ELEMENT ip-address (#PCDATA)>
<!ELEMENT port (#PCDATA)>
<!ELEMENT username (#PCDATA)>
<!ELEMENT password (#PCDATA)>
<!ELEMENT NSM-DATA (cns-device-container*, cns-device-info*, cns-application-info*,
cns-group-info*)>
<!ATTLIST NSM-DATA
    op-type (add) #REQUIRED
    validate-data (true | false) #REQUIRED
>
<!ELEMENT cns-device-container (device-container-name+, parent-container?)>
<!-- This tag is to add the sub containers for devices-->
<!ELEMENT device-container-name (#PCDATA)>
<!ELEMENT parent-container (#PCDATA)>
<!-- This is an optional tag that specifies which container the dev. container object is 
to be added-->
<!ELEMENT cns-device-info (cns-device-name, cns-extended-attr*, device-container?, 
dev-image-information?)>
<!ELEMENT device-container (#PCDATA)>
<!-- This is an optional tag that specifies which container this object is to be added-->
<!ELEMENT cns-device-name (#PCDATA)>
<!ELEMENT cns-extended-attr (#PCDATA)>
<!ELEMENT dev-image-information (image-id, activation-template?, dev-image-info+)>
<!ELEMENT image-id (#PCDATA)>
<!ELEMENT activation-template (#PCDATA)>
<!ELEMENT dev-image-info (image-name, distribution)>
<!ELEMENT image-name (#PCDATA)>
<!ELEMENT distribution ( destination?, location)>
<!ATTLIST distribution
    overwrite  (yes | no) "no"
    erase-flash (yes | no) "no"
    activate (true | false) "false"
>
<!ELEMENT destination (#PCDATA)>
<!ELEMENT location (#PCDATA)>
<!ELEMENT cns-application-info (cns-application-name, cns-subject-mapping*, 
application-container?)>
<!ELEMENT application-container (#PCDATA)>
<!-- This is an optional tag that specifies which container this object is to be added-->
<!ELEMENT cns-application-name (#PCDATA)>
<!ELEMENT cns-subject-mapping (cns-original-subject, cns-pub-mapping*, cns-sub-mapping*, 
cns-pub-default, cns-sub-default, cns-extended-attr*)>
<!ELEMENT cns-original-subject (#PCDATA)>
<!ELEMENT cns-pub-mapping (#PCDATA)>
<!ELEMENT cns-sub-mapping (#PCDATA)>
<!ELEMENT cns-pub-default (#PCDATA)>
<!ELEMENT cns-sub-default (#PCDATA)>
<!ELEMENT cns-group-info (cns-group-name, cns-group-application-name*, cns-group-member*, 
cns-extended-attr*, group-container?)>
<!ELEMENT group-container (#PCDATA)>
<!-- This is an optional tag that specifies which container this object is to be added-->
<!ELEMENT cns-group-name (#PCDATA)>
<!ELEMENT cns-group-application-name (#PCDATA)>
<!ELEMENT cns-group-member (#PCDATA)>
<!ATTLIST cns-group-application-name
    application-container CDATA #IMPLIED
>
<!ATTLIST cns-group-member
    device-container CDATA #IMPLIED
>
<!ATTLIST cns-extended-attr
    name CDATA #REQUIRED
>
<!-- Here starts the definition for Image-data-->
<!ELEMENT IMAGE-DATA (image+)>
<!ATTLIST IMAGE-DATA
    op-type (add) #REQUIRED
>
<!ELEMENT image (name, image-info)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT image-info (img-name, img-chksum?, hdr-chksum?, software-version?, 
system-description?, file-byte-size?, platform-family-name?, img-location*)>
```

```
<!ATTLIST image-info
        image-type (IOS | pix-image | pdm | other) "IOS"
>
<!ELEMENT img-name (#PCDATA)>
<!ELEMENT img-chksum (#PCDATA)>
<!ELEMENT hdr-chksum (#PCDATA)>
<!ELEMENT file-byte-size (#PCDATA)>
<!ELEMENT system-description (#PCDATA)>
<!ELEMENT platform-family-name (#PCDATA)>
<!ELEMENT software-version (#PCDATA)>
<!ELEMENT img-location (#PCDATA)>
```

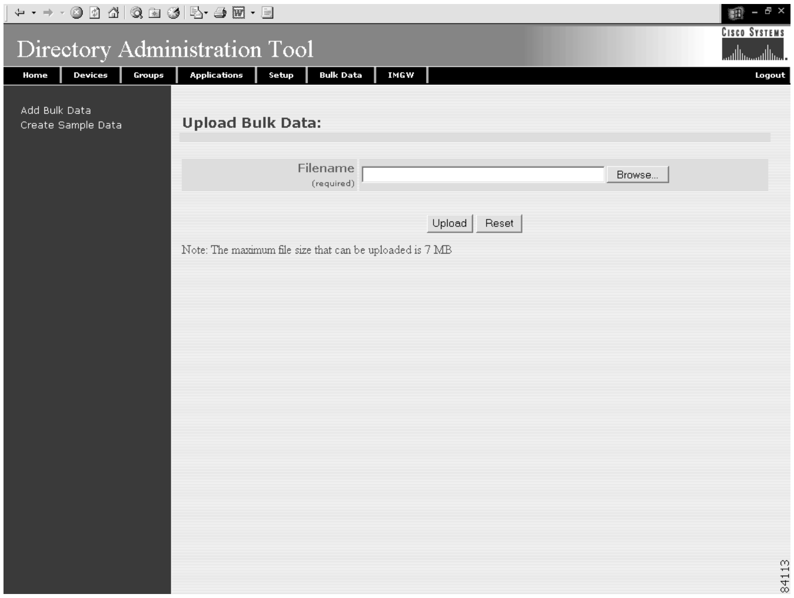
How to Upload Bulk Data

To upload bulk data to your system, follow these steps:

Step 1 From the Bulk Data main menu, click **Add Bulk Data**.

The Upload Bulk Data page appears (see Figure 4-42).

Figure 4-42 Upload Bulk Data



Upload Bulk Data:

Filename (required)

Note: The maximum file size that can be uploaded is 7 MB

Step 2 If you know the filename of the data file you want to load, enter it in the **Filename** field, otherwise use the browse function.

Table 4-10lists the valid values for this field.

Table 4-10 Valid Values for Upload Bulk Data

Attribute	Description	Valid Values
Filename	Name of the file containing the data to be uploaded.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)

Step 3 To use the browser to locate the filename of the data file you want to upload, click **Browse**.

Step 4 To clear your entry and start over, click **Reset**.

Step 5 To initiate the upload, click **Upload**.

Step 6 To return to the main menu, click the **Home** tab.

Command-Line Upload of Bulk Data

You can also upload the XML file to the directory using a command line utility as follows:

Step 1 FTP the bulk upload XML file to the */opt/CSCOdat/scripts/* directory on the CNS 2100 Series system.

Step 2 Login to the box using Telnet

Step 3 Go to: **/opt/CSCOdat/scripts/**

Step 4 Run the following command to invoke the bulk upload command line utility:

./upload.sh <*xml filename***>**

For example: **./upload.sh my_bulk_data.xml**

This uploads the data to the LDAP directory.

Creating Sample Data for Bulk Upload

Even though the DTD (see "XML DTD" section on page 4-42) outlines the structure of the input XML file, it does not convey the information about what values should be given for each tag. By looking at the sample data files (NSM and IMGW) in this section, you can get an idea of how the data should be arranged in the Bulk Upload XML file.

You can create sample data files for both NSM and IMGW devices.

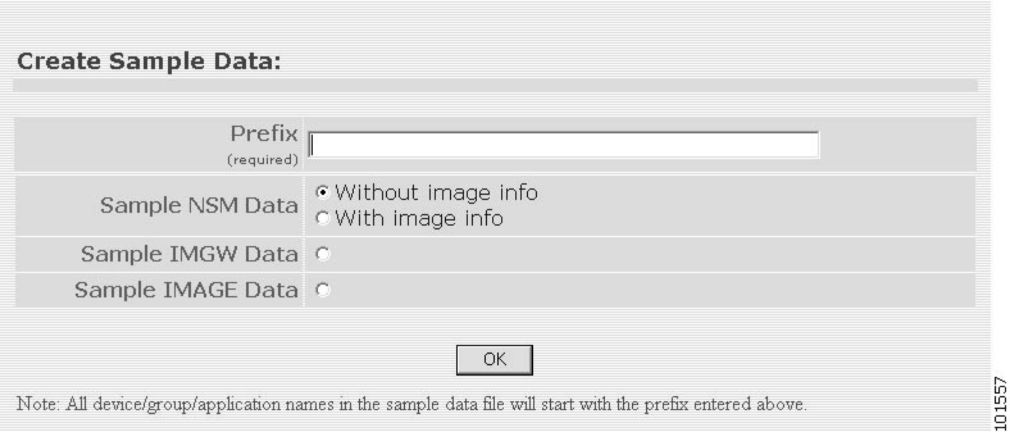
How to Create Sample Data for Bulk Upload

To create sample data on your system, follow these steps:

Step 1 From the Bulk Data main menu, click **Add Bulk Data**.

The Upload Bulk Data page appears (see Figure 4-43).

Figure 4-43 Create Sample Data



Create Sample Data:

Prefix (required) [ ]

Sample NSM Data ● Without image info ○ With image info

Sample IMGW Data ○

Sample IMAGE Data ○

Note: All device/group/application names in the sample data file will start with the prefix entered above.

Step 2 Enter the prefix name for this sample in the **Prefix** field.

Table 4-11 lists valid values for these fields.

Table 4-11 Valid Values for Create Sample Data

Attribute	Description	Valid Values
Prefix	Prefix that is used to create the device/application/group objects.	a-z A-Z 0-9 -(hyphen) _ (under-score) . (period)
Sample NSM Data Without image info	Creates application, group, CNS device data without the image information for CNS device.	Radio button
Sample NSM Data With image info	Creates application, group, CNS device data without the image information for CNS device. Also creates IMAGE object data.	Radio button
Sample IMGW Data	Creates IMGW device object data	Radio button
Sample IMAGE Data	Creates IMAGE object data	Radio button

Step 3 Select whether this is for NSM, IMGW, or IMAGE data.

Step 4 To create this sample, click **OK**.

Step 5 To return to the main menu, click the **Home** tab.

NSM Data Sample

The following example shows an NSM data sample for bulk upload:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE cns-bulk-upload SYSTEM "BulkUpload.dtd">
<cns-bulk-upload stop-on-error="false">
    <cns-element-data>
        <NSM-DATA op-type="add" validate-data="false">
            <cns-device-container>
                <device-container-name>SampleSubDevices</device-container-name>
            </cns-device-container>
            <cns-device-container>
                <device-container-name>SubSubDevices</device-container-name>

<parent-container>ou=SampleSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=infy,c=in</parent-co
ntainer>
            </cns-device-container>
            <cns-device-info>
                <cns-device-name>SampleDevice1</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">SampleDevice1</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">SampleDevice1</cns-extended-attr>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>SampleDevice2</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">SampleDevice2</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">SampleDevice2</cns-extended-attr>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>SampleDevice3</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">SampleDevice3</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">SampleDevice3</cns-extended-attr>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>SampleDevice4</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">SampleDevice4</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">SampleDevice4</cns-extended-attr>

<device-container>ou=SampleSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=infy,c=in</device-co
ntainer>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>SampleDevice5</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">SampleDevice5</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">SampleDevice5</cns-extended-attr>

<device-container>ou=SubSubDevices,ou=SampleSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=inf
y,c=in</device-container>
```

```
            </cns-device-info>
            <cns-application-info>
                <cns-application-name>SampleTestApp</cns-application-name>
                <cns-subject-mapping>
                    <cns-original-subject>SampleTestApp.Event1</cns-original-subject>

<cns-pub-mapping>SampleTestApp.Event1.cns-pub-mapping</cns-pub-mapping>

<cns-sub-mapping>SampleTestApp.Event1.cns-sub-mapping</cns-sub-mapping>
                    <cns-pub-default>0</cns-pub-default>
                    <cns-sub-default>0</cns-sub-default>
                </cns-subject-mapping>
                <cns-subject-mapping>
                    <cns-original-subject>SampleTestApp.Event2</cns-original-subject>

<cns-pub-mapping>SampleTestApp.Event2.cns-pub-mapping</cns-pub-mapping>

<cns-sub-mapping>SampleTestApp.Event2.cns-sub-mapping</cns-sub-mapping>
                    <cns-pub-default>0</cns-pub-default>
                    <cns-sub-default>0</cns-sub-default>
                </cns-subject-mapping>
            </cns-application-info>
            <cns-group-info>
                <cns-group-name>SampleGroup1</cns-group-name>
                <cns-group-application-name>SampleTestApp</cns-group-application-name>
                <cns-group-member>SampleDevice1</cns-group-member>
                <cns-group-member>SampleDevice2</cns-group-member>
                <cns-group-member>SampleDevice3</cns-group-member>
            </cns-group-info>
            <cns-group-info>
                <cns-group-name>SampleGroup2</cns-group-name>
                <cns-group-application-name>SampleTestApp</cns-group-application-name>
                <cns-group-member>SampleDevice1</cns-group-member>
                <cns-group-member>SampleDevice2</cns-group-member>
                <cns-group-member>SampleDevice3</cns-group-member>
                <cns-group-member
device-container="ou=SampleSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=infy,c=in">SampleDev
ice4</cns-group-member>
                <cns-group-member
device-container="ou=SubSubDevices,ou=SampleSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=inf
y,c=in">SampleDevice5</cns-group-member>
            </cns-group-info>
        </NSM-DATA>
    </cns-element-data>
</cns-bulk-upload>
```

NSM Data Sample With Image Information

The following example shows an NSM data sample with image information:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE cns-bulk-upload SYSTEM "BulkUpload.dtd">
<cns-bulk-upload stop-on-error="false">
    <cns-element-data>
        <NSM-DATA op-type="add" validate-data="false">
            <cns-device-container>
                <device-container-name>xyzSubDevices</device-container-name>
            </cns-device-container>
            <cns-device-container>
                <device-container-name>SubSubDevices</device-container-name>

<parent-container>ou=xyzSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=cisco,c=us</parent-cont
ainer>
```

```
            </cns-device-container>
            <cns-device-info>
                <cns-device-name>xyzDevice1</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">xyzDevice1</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">xyzDevice1</cns-extended-attr>
                <dev-image-information>
                    <image-id>xyzDevice1</image-id>
                    <activation-template>DemoRouter.cfgtpl</activation-template>
                    <dev-image-info>
                        <image-name>xyzIMAGEObj1</image-name>
                        <distribution overwrite="yes" erase-flash="no" activate="false">
                            <destination>flash</destination>
                            <location>tftp://test.com/c7200-js-mz1</location>
                        </distribution>
                    </dev-image-info>
                </dev-image-information>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>xyzDevice2</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">xyzDevice2</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">xyzDevice2</cns-extended-attr>
                <dev-image-information>
                    <image-id>xyzDevice2</image-id>
                    <activation-template>DemoRouter.cfgtpl</activation-template>
                    <dev-image-info>
                        <image-name>xyzIMAGEObj2</image-name>
                        <distribution overwrite="yes" erase-flash="no" activate="false">
                            <destination>flash</destination>
                            <location>tftp://test.com/c7200-js-mz2</location>
                        </distribution>
                    </dev-image-info>
                </dev-image-information>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>xyzDevice3</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">xyzDevice3</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">xyzDevice3</cns-extended-attr>
                <dev-image-information>
                    <image-id>xyzDevice3</image-id>
                    <activation-template>DemoRouter.cfgtpl</activation-template>
                    <dev-image-info>
                        <image-name>xyzIMAGEObj3</image-name>
                        <distribution overwrite="yes" erase-flash="no" activate="false">
                            <destination>flash</destination>
                            <location>tftp://test.com/c7200-js-mz3</location>
                        </distribution>
                    </dev-image-info>
                </dev-image-information>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>xyzDevice4</cns-device-name>
                <cns-extended-attr
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">xyzDevice4</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">xyzDevice4</cns-extended-attr>

<device-container>ou=xyzSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=cisco,c=us</device-cont
ainer>
```

```
                <dev-image-information>
                    <image-id>xyzDevice4</image-id>
                    <activation-template>DemoRouter.cfgtpl</activation-template>
                    <dev-image-info>
                        <image-name>xyzIMAGEObj4</image-name>
                        <distribution overwrite="yes" erase-flash="no" activate="false">
                            <destination>flash</destination>
                            <location>tftp://test.com/c7200-js-mz4</location>
                        </distribution>
                    </dev-image-info>
                </dev-image-information>
            </cns-device-info>
            <cns-device-info>
                <cns-device-name>xyzDevice5</cns-device-name>
                <cns-extended-attr 
name="IOSconfigtemplate">DemoRouter.cfgtpl</cns-extended-attr>
                <cns-extended-attr name="IOSConfigID">xyzDevice5</cns-extended-attr>
                <cns-extended-attr name="IOSEventID">xyzDevice5</cns-extended-attr>

<device-container>ou=SubSubDevices,ou=xyzSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=cisco,
c=us</device-container>
                <dev-image-information>
                    <image-id>xyzDevice5</image-id>
                    <activation-template>DemoRouter.cfgtpl</activation-template>
                    <dev-image-info>
                        <image-name>xyzIMAGEObj5</image-name>
                        <distribution overwrite="yes" erase-flash="no" activate="false">
                            <destination>flash</destination>
                            <location>tftp://test.com/c7200-js-mz5</location>
                        </distribution>
                    </dev-image-info>
                </dev-image-information>
            </cns-device-info>
            <cns-application-info>
                <cns-application-name>xyzTestApp</cns-application-name>
                <cns-subject-mapping>
                    <cns-original-subject>xyzTestApp.Event1</cns-original-subject>
                    <cns-pub-mapping>xyzTestApp.Event1.cns-pub-mapping</cns-pub-mapping>
                    <cns-sub-mapping>xyzTestApp.Event1.cns-sub-mapping</cns-sub-mapping>
                    <cns-pub-default>1</cns-pub-default>
                    <cns-sub-default>1</cns-sub-default>
                </cns-subject-mapping>
                <cns-subject-mapping>
                    <cns-original-subject>xyzTestApp.Event2</cns-original-subject>
                    <cns-pub-mapping>xyzTestApp.Event2.cns-pub-mapping</cns-pub-mapping>
                    <cns-sub-mapping>xyzTestApp.Event2.cns-sub-mapping</cns-sub-mapping>
                    <cns-pub-default>1</cns-pub-default>
                    <cns-sub-default>1</cns-sub-default>
                </cns-subject-mapping>
            </cns-application-info>
            <cns-group-info>
                <cns-group-name>xyzGroup1</cns-group-name>
                <cns-group-application-name>xyzTestApp</cns-group-application-name>
                <cns-group-member>xyzDevice1</cns-group-member>
                <cns-group-member>xyzDevice2</cns-group-member>
                <cns-group-member>xyzDevice3</cns-group-member>
            </cns-group-info>
            <cns-group-info>
                <cns-group-name>xyzGroup2</cns-group-name>
                <cns-group-application-name>xyzTestApp</cns-group-application-name>
                <cns-group-member>xyzDevice1</cns-group-member>
                <cns-group-member>xyzDevice2</cns-group-member>
                <cns-group-member>xyzDevice3</cns-group-member>
                <cns-group-member 
device-container="ou=xyzSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=cisco,c=us">xyzDevice4<
/cns-group-member>
                <cns-group-member 
device-container="ou=SubSubDevices,ou=xyzSubDevices,ou=CNSDevices,ou=cns-pokhran4,o=cisco,
c=us">xyzDevice5</cns-group-member>
            </cns-group-info>
        </NSM-DATA>
    </cns-element-data>
</cns-bulk-upload>
```

NOTES

- For Bulk Upload of NSM devices with Image Info, make sure that the image objects referenced in the **dev-image-info** element tag already exist.
- The location given should be one of the multiple image locations specified with the image object.
- If there are errors while adding the devices, please check the error file provided as a result of the Upload operation. There can be an exception given as CISException, which points to the CISDevice creation failed, which could have occurred if you had ignored the checklist. In this case, just recheck the information provided in the **dev-image-information** element tag. Correct the file and upload it again.

Image Sample Data

The following example shows image data sample:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE cns-bulk-upload SYSTEM "BulkUpload.dtd">
<cns-bulk-upload stop-on-error="false">
    <cns-element-data>
        <IMAGE-DATA op-type="add">
            <image>
                <name>xyzIMAGEObj1</name>
                <image-info image-type="IOS">
                    <img-name>c7200-js-mz1</img-name>
                    <img-chksum>0x1256faf245</img-chksum>
                    <software-version>12.2(8)T6</software-version>
                    <system-description>Cisco Network Operating 
System</system-description>
                    <file-byte-size>1040</file-byte-size>
                    <platform-family-name>7200</platform-family-name>
                    <img-location>tftp://test.com/c7200-js-mz1</img-location>
                </image-info>
            </image>
            <image>
                <name>xyzIMAGEObj2</name>
                <image-info image-type="IOS">
                    <img-name>c7200-js-mz2</img-name>
                    <img-chksum>0x1256faf245</img-chksum>
                    <software-version>12.2(8)T6</software-version>
                    <system-description>Cisco Network Operating 
System</system-description>
                    <file-byte-size>1040</file-byte-size>
                    <platform-family-name>7200</platform-family-name>
                    <img-location>tftp://test.com/c7200-js-mz2</img-location>
                </image-info>
            </image>
            <image>
                <name>xyzIMAGEObj3</name>
                <image-info image-type="IOS">
                    <img-name>c7200-js-mz3</img-name>
                    <img-chksum>0x1256faf245</img-chksum>
                    <software-version>12.2(8)T6</software-version>
                    <system-description>Cisco Network Operating 
System</system-description>
                    <file-byte-size>1040</file-byte-size>
                    <platform-family-name>7200</platform-family-name>
                    <img-location>tftp://test.com/c7200-js-mz3</img-location>
                </image-info>
            </image>
            <image>
                <name>xyzIMAGEObj4</name>
                <image-info image-type="IOS">
                    <img-name>c7200-js-mz4</img-name>
                    <img-chksum>0x1256faf245</img-chksum>
                    <software-version>12.2(8)T6</software-version>
                    <system-description>Cisco Network Operating 
System</system-description>
                    <file-byte-size>1040</file-byte-size>
                    <platform-family-name>7200</platform-family-name>
                    <img-location>tftp://test.com/c7200-js-mz4</img-location>
                </image-info>
            </image>
            <image>
                <name>xyzIMAGEObj5</name>
                <image-info image-type="IOS">
                    <img-name>c7200-js-mz5</img-name>
                    <img-chksum>0x1256faf245</img-chksum>
                    <software-version>12.2(8)T6</software-version>
                    <system-description>Cisco Network Operating 
System</system-description>
                    <file-byte-size>1040</file-byte-size>
                    <platform-family-name>7200</platform-family-name>
                    <img-location>tftp://test.com/c7200-js-mz5</img-location>
                </image-info>
            </image>
        </IMAGE-DATA>
    </cns-element-data>
</cns-bulk-upload>
```

IMGW Sample Data

The following example shows an IMGW data sample for bulk upload:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE cns-bulk-upload SYSTEM "BulkUpload.dtd">
<cns-bulk-upload stop-on-error="false">
    <cns-element-data>
        <IMGW-DATA op-type="add">
            <imgw-device>
                <device-id>xyzIMGWDevice1</device-id>
                <gateway-id>xyzIMGWGatewayID1</gateway-id>
                <device-type>IOS</device-type>
            </imgw-device>
            <imgw-device>
                <device-id>xyzIMGWDevice2</device-id>
                <gateway-id>xyzIMGWGatewayID2</gateway-id>
                <device-type>IOS</device-type>
                <hop-information>
                    <hop-type>IOS_LOGIN</hop-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>xyzusr2</username>
                    <password>xyzpwd2</password>
                </hop-information>
            </imgw-device>
            <imgw-device>
                <device-id>xyzIMGWDevice3</device-id>
                <gateway-id>xyzIMGWGatewayID3</gateway-id>
                <device-type>IOS</device-type>
                <hop-information>
                    <hop-type>IOS_LOGIN</hop-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>xyzusr3</username>
                    <password>xyzpwd3</password>
                </hop-information>
                <hop-information>
                    <hop-type>IOS_LOGIN</hop-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>xyzuser3</username>
                    <password>xyzpasswd3</password>
                </hop-information>
            </imgw-device>
            <imgw-device>
                <device-id>xyzIMGWDevice4</device-id>
                <gateway-id>xyzIMGWGatewayID4</gateway-id>
                <device-type>IOS</device-type>
                <hop-information>
                    <hop-type>IOS_LOGIN</hop-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>xyzusr4</username>
                    <password>xyzpwd4</password>
                </hop-information>
                <hop-information>
                    <hop-type>IOS_LOGIN</hop-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>xyzuser4</username>
                    <password>xyzpasswd4</password>
                </hop-information>
            </imgw-device>
            <imgw-device>
                <device-id>xyzIMGWDevice5</device-id>
                <gateway-id>xyzIMGWGatewayID5</gateway-id>
                <device-type>IOS</device-type>
                <hop-information>
                    <hop-type>IOS_LOGIN</hop-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>xyzusr5</username>
                    <password>xyzpwd5</password>
                </hop-information>
                <hop-information>
                    <hop-type>IOS_LOGIN</hop-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>xyzuser5</username>
                    <password>xyzpasswd5</password>
                </hop-information>
            </imgw-device>
        </IMGW-DATA>
    </cns-element-data>
</cns-bulk-upload>
```

Updating Configurations for IMGW Devices

In order to modify configurations for IMGW devices, corresponding CNS devices with the same device names must be created in the Configure Registrar.

The steps for updating configurations for IMGW devices in the Configure Registrar are outlined as follows:

Step 1 Create a CNS device, making sure its device name is the same as that of its corresponding IMGW device (see "How to Add a Device" section on page 2-9).

Provide ConfigID, EventID, and a template file as the ConfigTemplate.

Note ConfigID must be the same as the device name.

Step 2 Create template file if it does not exist (see "Templates and Template Management" section on page 2-57).

Step 3 Edit template parameters for the device (see "How to Edit Device Templates" section on page 2-17).

Step 4 Preview the configuration for the device (see "How to View Device Configuration" section on page 2-8).

Step 5 Update the device configuration (see "How to Update Device Configuration and Image" section on page 2-19).

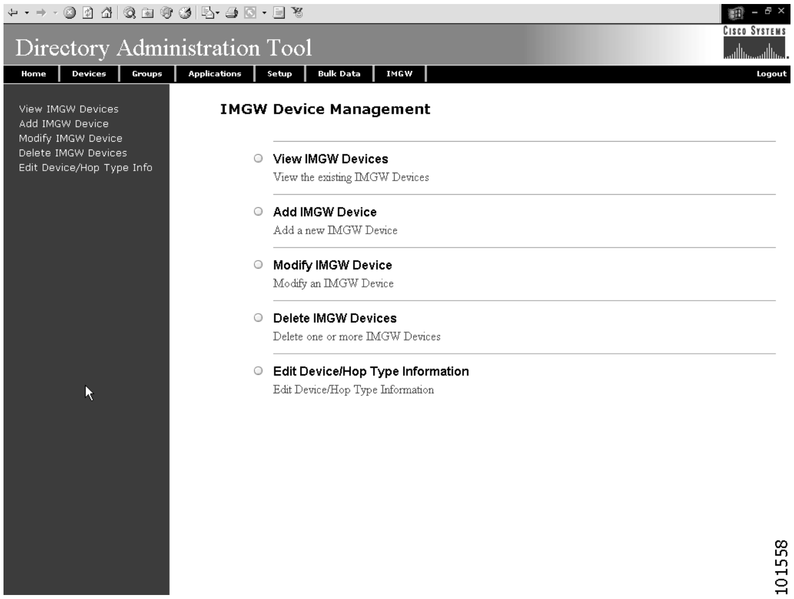
Check the response message returned by IMGW (see "How to View Log Files" section on page 2-71).

Managing IMGW Parameters

To manage IMGW parameters, from the main menu, click the **IMGW** tab.

The IMGW main menu appears (see Figure 4-44).

Figure 4-44 IMGW Device Management



IMGW Device Management

○ View IMGW Devices
View the existing IMGW Devices

○ Add IMGW Device
Add a new IMGW Device

○ Modify IMGW Device
Modify an IMGW Device

○ Delete IMGW Devices
Delete one or more IMGW Devices

○ Edit Device/Hop Type Information
Edit Device/Hop Type Information

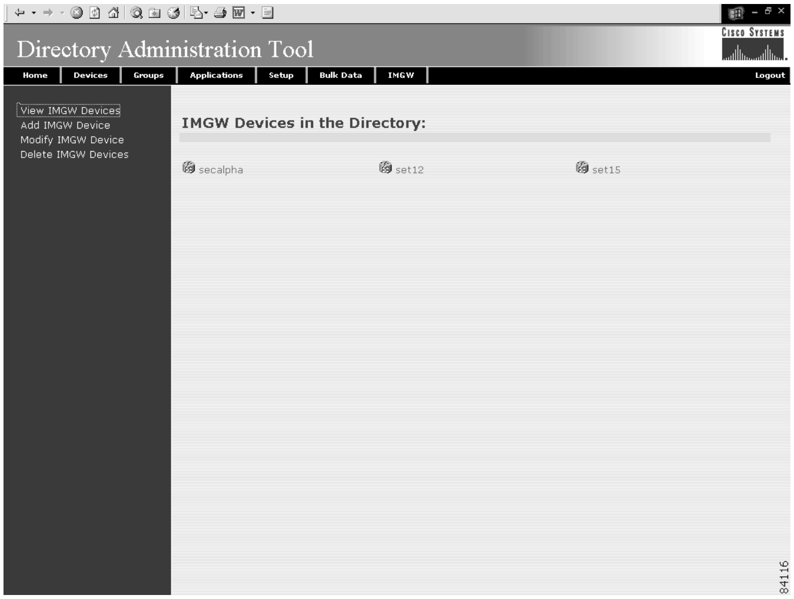
How to View IMGW Devices

To view IMGW devices in the system, click **View IMGW Devices**.

The IMGW Devices page appears (see Figure 4-45).

You can see the details of a particular device by clicking on the device icon.

Figure 4-45 IMGW Devices in the System



IMGW Devices in the Directory:

secalpha set12 set15

Adding IMGW Devices to the System

This section describes how to add IMGW devices to the system. However, before adding a device to IMGW, you should be familiar with hop tables.

Hop Tables

To access devices by means of Telnet, it is necessary to construct hop tables (see "HopInfo Examples" section on page 4-58). These are tables that indicate what network path exists to the device, as well as all the authentication information necessary at each stage, or hop.

What You Should Know About Device Hop Information

The Hop Information (HopInfo) structure describes one portion of the path between source and destination. HopInfo can be chained together to specify how to login to a device. Examples of uses of this structure include:

- Devices with basic authentication mode requiring IP address, username, and password
- Devices with additional authentication modes such as Cisco IOS enable mode
- Embedded-within-embedded applications such as linecards on a Catalyst switch

The latter two examples require a login, but not a hop to a different device. Therefore, they are referred to as *virtual* hops.

Table 4-12 shows the fields in the HopInfo structure:

Table 4-12 HopInfo Structure

Field	Purpose
hop_type	String indicating type of hop.
ip_address	IP address of device (string)
port	TCP port on which to access device (integer)
username	Username with which to login to device (string)
password	Password with which to login to device (string)

Currently Supported Device Types

Table 4-13 through Table 4-20 on page 4-58 provide the HopInfo list for devices that are directly accessible on the network by IMGW. For accessing devices by way of Commserver, see Table 4-21 on page 4-58.

All the rows in these tables are mandatory. Also, the hop_type fields cannot be NULL or empty. The fields marked with **X** are mandatory in IMGW unless they are not required on the device-side.

Table 4-13 Cisco IOS Device Directly Connected

hop_type	ip_address	port	username	password
IOS_LOGIN	X		X	X
IOS_EN			X	X

Table 4-14 Cisco IOS Device Directly Connected Supporting SSH

hop_type	ip_address	port	username	password
IOS_LOGIN:SSH	X		X	X
IOS_EN			X	X

Table 4-15 Catalyst Device Directly Connected

hop_type	ip_address	port	username	password
CATALYST_LOGIN	X		X	X
CATALYST_EN			X	X

Table 4-16 Catalyst IOS MSFC Blade Directly Connected

hop_type	ip_address	port	username	password
CATALYST_LOGIN	X		X	X
IOS_CAT_BLADE		X	X	X
IOS_EN			X	X

Table 4-17 Catalyst IOS Device Directly Connected

hop_type	ip_address	port	username	password
CATIOS_LOGIN	X		X	X
CATIOS_EN			X	X

Table 4-18 CSS Device Directly Connected

hop_type	ip_address	port	username	password
CSS_LOGIN	X		X	X
CSS_EN			X	X

Table 4-19 CE Device Directly Connected

hop_type	ip_address	port	username	password
CE_LOGIN	X		X	X
CE_EN			X	X

Table 4-20 PIX Device Directly Connected

hop_type	ip_address	port	username	password
PIX_LOGIN	X		X	X
PIX_EN			X	X

When any of the above devices is accessed by way of a Commserver (such as a Cisco 2511 Access Server), the resultant HopInfo list has the following two rows prepended to the respective HopInfo list for that device:

Table 4-21 Partial HopInfo List For Commserver Access

hop_type	ip_address	port	username	password
COMMSERVER_LOGIN	X		X	X
COMMSERVER		X	///////////////	X

Note Because the current release does not support port username, the username field of HopInfo structure for COMMSERVER is always ignored by IMGW. Do not set up the port username on the Commserver.

HopInfo Examples

Table 4-22 Cisco IOS Device Directly Connected

hop_type	ip_address	port	username	password
IOS_LOGIN	172.28.6.90		Johndoe	Passnow
IOS_EN			dummy	compass

Table 4-23 Cisco IOS Device Directly Connected Supporting SSH

hop_type	ip_address	port	username	password
IOS_LOGIN:SSH	172.28.6.90		Johndoe	Passnow
IOS_EN			dummy	compass

Table 4-24 Cisco IOS Device Connected With Commserver

hop_type	ip_address	port	username	password
COMMSERVER_LOGIN	172.28.6.226		Sandra	Me1100
COMMSERVER		2005	//////////////////	Lab123
IOS_LOGIN			Johndoe	Passnow
IOS_EN			dummy	compass

Table 4-25 Catalyst IOS MFSC Blade Directly Connected

hop_type	ip_address	port	username	password
CATALYST_LOGIN	172.29.132.32		Admin	Raining
IOS_CAT_BLADE		15	Admin	winding
IOS_EN			dummy	moonlight

Table 4-26 Catalyst IOS MFSC Blade Accessed With Commserver

hop_type	ip_address	port	username	password
COMMSERVER_LOGIN	172.28.22.229		Kldfg	Dsdsfg
COMMSERVER		2010	/////////////////	Dadada
CATALYST_LOGIN			Admin	Raining
IOS_CAT_BLADE		15	Admin	winding
IOS_EN			dummy	moonlight

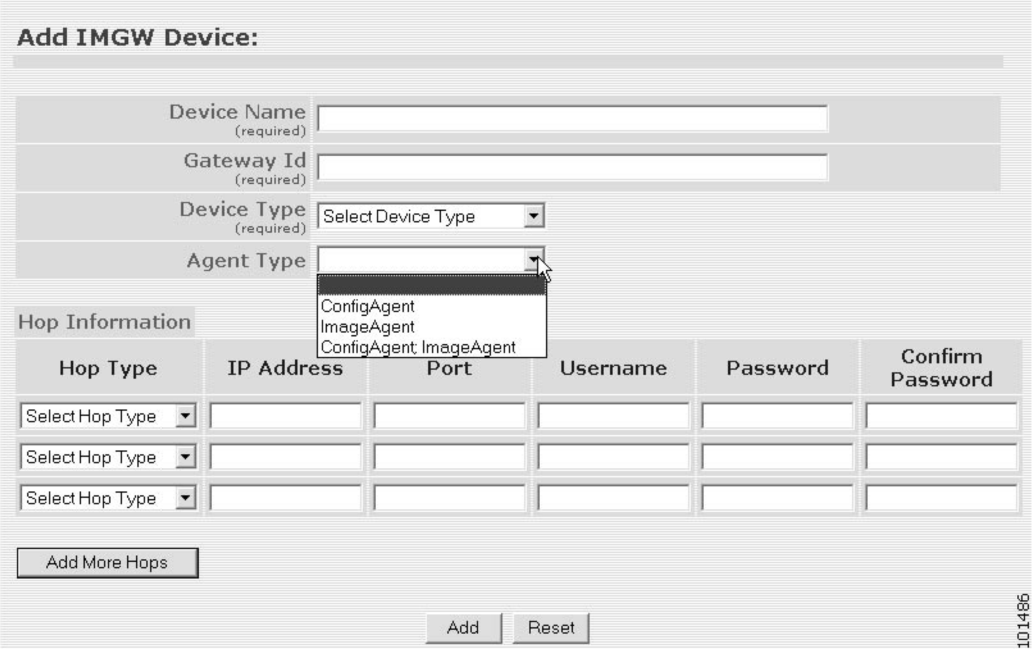
How to Add an IMGW Device

To add an IMGW device to the system, follow these steps:

Step 1 From the IMGW main menu, click **Add IMGW Device**.

The Add IMGW Device page appears (see Figure 4-46).

Figure 4-46 Add IMGW Devices



Step 2 Enter the name of the device in the **Device Name** field.

Table 4-27 lists valid values for these fields.

Table 4-27 Valid Values for Add IMGW Device

Attribute	Description	Valid Values
Device Name	The name used as **cn** (common name) of the IMGW device.	Non-empty string excluding the special characters: !, “, #, $, %, &, ', (,), *, /, <, >, ?, @, \, ^, `, ~
Gateway ID	Gateway identifier for this device.	Non-empty string excluding the special characters: !, “, #, $, %, &, ', (,), *, /, <, >, ?, @, \, ^, `, ~
Device Type	Type of IMGW device.	From drop-down list
Agent Type	Type of agent you want IMGW to simulate.	From drop-down list
Hop Type	Nature of the particular connection hop.	From drop-down list
IP Address	IP address of the connecting node in the hop	Valid IP address of the following format: 10.1.14.216
Port	Port number of the node.	Integer values
Username	Username to login to the hop node.	String excluding the special characters: !, “, #, $, %, &, ', (,), *, /, <, >, ?, @, \, ^, `, ~
Password	Password to login to the hop node.	Non-null string

Step 3 Enter the gateway ID in the **Gateway Id** field.

Note The gateway ID for IMGW devices must be the same as that entered during **Setup** (see “Re-configure IMGW Parameters” section on page 2-9). By convention, hostname is used as the gateway ID.

Step 4 Select the device type from the drop-down list.

Step 5 Select the agent type from the drop-down list.

Step 6 Enter parameters about each hop in the **Hop Information** fields.

For more information, see “Hop Tables” section on page 4-56.

Step 7 To add more hops, click **Add More Hops**.

Step 8 To clear your entries and start over, click **Reset**.

Step 9 To add this IMGW device to the system, click **Add**.

Step 10 To return to the main menu, click the **Home** tab.

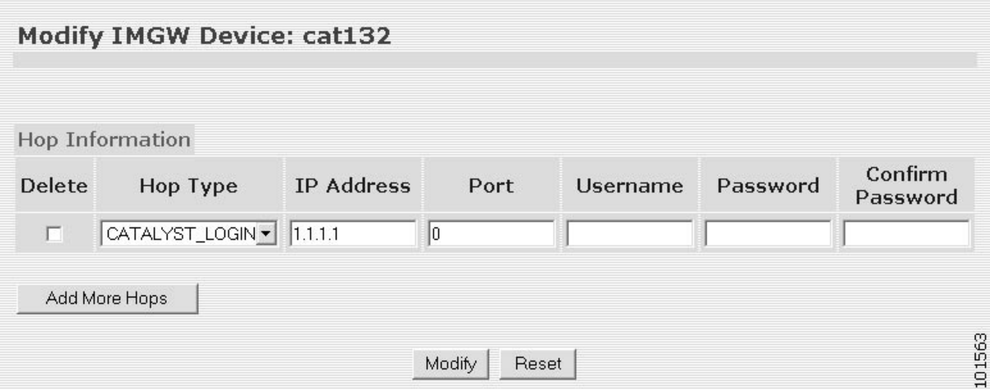
How to Modify IMGW Devices

To modify an IMGW device to the system, follow these steps:

Step 1 From the IMGW main menu, click **Modify IMGW Device**.

The Modify IMGW Device page appears (see Figure 4-47).

Figure 4-47 Modify IMGW Devices



Modify IMGW Device: cat132

Hop Information

Delete	Hop Type	IP Address	Port	Username	Password	Confirm Password
□	CATALYST_LOGIN	1.1.1.1	0			

Step 2 Modify all required fields.

Table 4-28 lists valid values for these fields.

Table 4-28 Valid Values for Modify IMGW Device

Attribute	Description	Valid Values
Hop Type	Type of IMGW hop.	From drop-down list
IP Address	IP address of the connecting node in the hop	Valid IP address of the following format: 10.1.14.216
Port	Port number of the node.	Integer values
Username	Username to login to the hop node.	String excluding the special characters: !, “, #, $, %, &, ', (,), *, /, <, >, ?, @, \, ^, `, ~
Password	Password to login to the hop node.	Non-null string

Step 3 To add more hops, click **Add More Hops**.

Step 4 To delete a hop, select the **Delete** check-box.

Step 5 To clear your entries and start over, click **Reset**.

Step 6 To apply these changes, click **Modify**.

Step 7 To return to the main menu, click the **Home** tab.

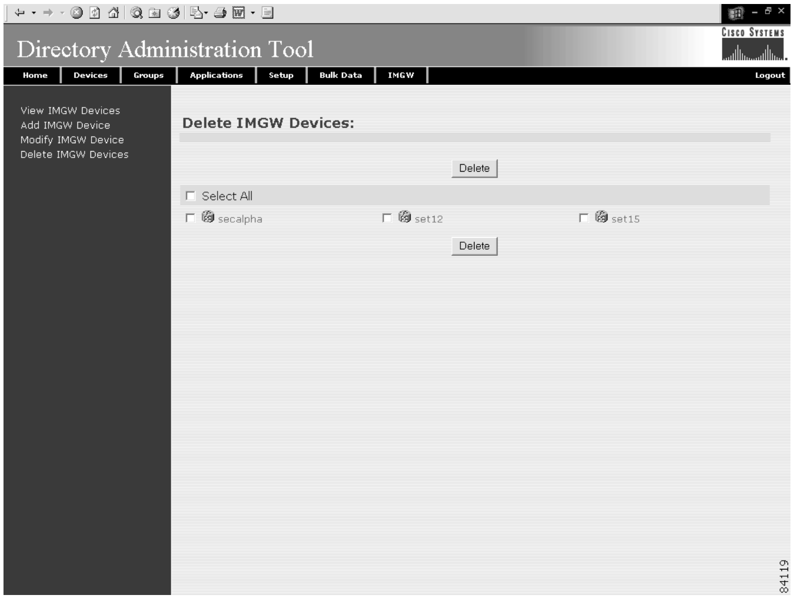
How to Delete IMGW Devices

To delete IMGW devices from the system, follow these steps:

Step 1 From the IMGW main menu, click **Delete IMGW Devices**.

The delete IMGW devices page appears (see Figure 4-48).

Figure 4-48 Delete IMGW Devices



Delete IMGW Devices:

□ Select All

□ secalpha □ set12 □ set15

Step 2 Check all IMGW devices you want to delete from the system.

Step 3 To delete these IMGW devices, click **Delete**.

To return to the main menu, click the **Home** tab.

How to Edit Device/Hop Type Information

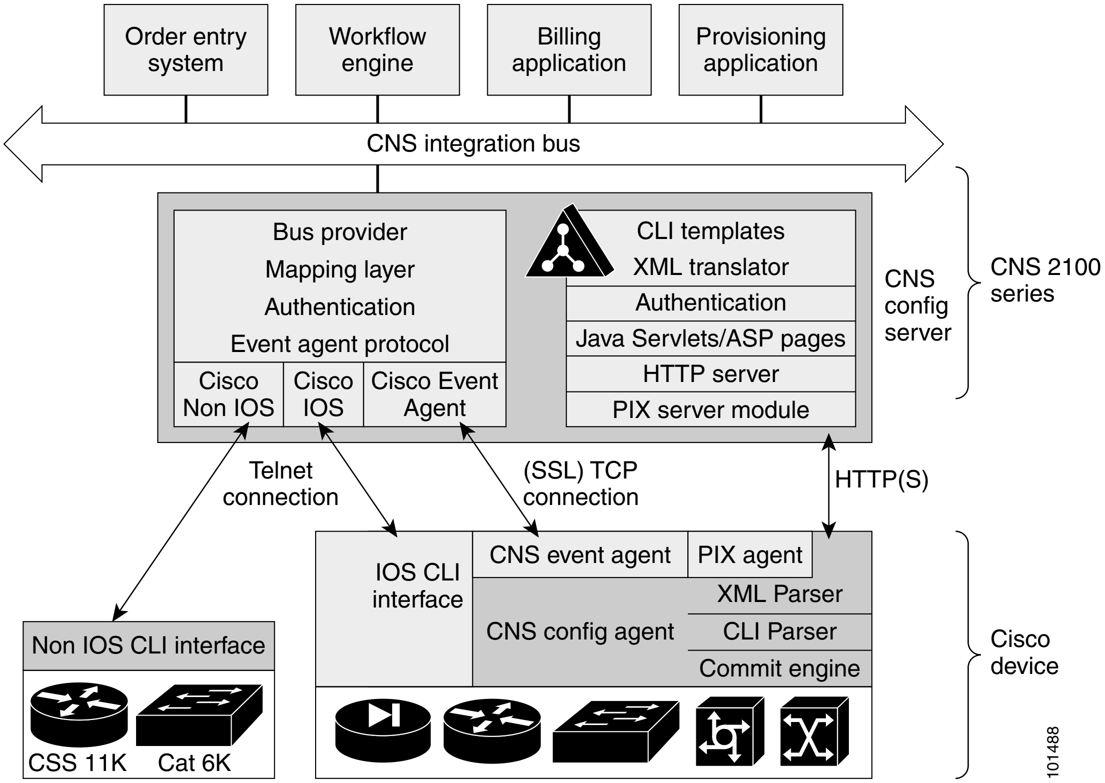
To complete information about how to edit device and hop type information using the IMGW Device Module Toolkit, see Appendix B, “How to Use the IMGW Device Module Development Toolkit.”

CHAPTER 5

Cisco PIX Firewall Device Support

Cisco CNS Configuration Engine 1.4 provides configuration management and image service to Cisco PIX firewall devices (PIX device). Figure 5-1 shows a functional block diagram of CNS Configuration Engine 1.4 including the PIX device interface module.

Figure 5-1 PIX-Compatible CNS Configuration Engine Module Interaction



PIX Device Polls for Updates

The PIX device contacts the PIX module in the CNS Configuration Engine 1.4 to report information about itself. This occurs when the PIX starts, when any of the reported information changes and whenever the PIX wants to check for updates. PIX sends the **DeviceDetails** message to the server.

DeviceDetails gives the CNS Configuration Engine 1.4 an update of the versions of software the device is currently running. The information received in **DeviceDetails** is logged into the log file (*pix.log*) for reference.

The server responds with the **UpdateInfo** message. This message contains (optionally)

- Checksum and URL for the configuration file the PIX should be running
- Checksum and URL for the PIX image
- Checksum and URL for the PIX Device Manager (PDM) image
- URL for reporting any errors

The PIX compares the checksum in the message with the current checksum of the component concerned. In the case of configuration, it also calculates the cryptochecksum of the running configuration and compare that with the one calculated the last time the configuration was updated from the CNS Configuration Engine 1.4. An update is required if the checksum (or cryptochecksum) differs.

If a software/configuration update is required, the PIX sends requests on the respective URLs.

Configuration Processing

For any configuration update that is required, the PIX sends an HTTPS GET request to the returned URL. The configuration file is completely read into a local buffer before being applied. This is to prevent a connection error from leaving the PIX in a partially configured state. If there are no errors (or the *errors* attribute of the **config-data** message is *continue*) while applying the configuration commands, then the running configuration is copied to flash with the **write memory** command. All configuration files work in the *replace* mode.

Completion of configuration download by a PIX device results in a log file entry indicating the same in *pix.log*.

Note The log entry does not mean that the configuration has been successfully applied on a PIX device. It only means that the PIX device has downloaded the configuration file.

Image Processing

The **DeviceDetails** XML sent along with the initial HTTPS POST optionally has information regarding the PIX image, its version and checksum. The CNS Configuration Engine 1.4 returns with the UpdateInfo XML containing image URLs and checksums based on the entries in the directory. The PIX downloads and applies images one after the other (and reload itself if required). Any error is processed as mentioned below.

Note There is no notification of successful image download because image distribution might be external to CNS Configuration Engine 1.4 and hence the PIX server cannot keep track of the same. Also, PIX device does not provide any image upgrade successful indication.

Error Processing

All errors are reported by way of HTTPS POST to the error URL using the **ErrorList** message.

Each configuration error report (type=error, warning or info) is logged by the CNS Configuration Engine 1.4 into *pix.log*. The log file is cyclic to limit disk space usage. The content of error-message is the error XML from the PIX device itself.

Note An error occurring during configuration does not mean that the downloaded configuration has not been applied on the PIX entirely. It only means that the error mentioned in the log file has happened with respect to this particular device.

Any error or notification (type= warning, notification, informational, debugging, emergency, alert, critical and error) that occurs while retrieving the data at one of the URLs received from the CNS Configuration Engine 1.4 results in log file entries.

If a failure is encountered during the processing of any of the URLs in the UpdateInfo response from the server, the error is reported to the Error URL. Also, processing of all URLs received in the current call home is discontinued. Any further processing is deferred till the PIX calls home again.

After all updates are successfully completed, another **DeviceDetails** message is sent to the CNS Configuration Engine 1.4 by the PIX device. The CNS Configuration Engine 1.4 again sends the **UpdateInfo** and checksum. The PIX device compares the checksums and finds that no further updates are required.

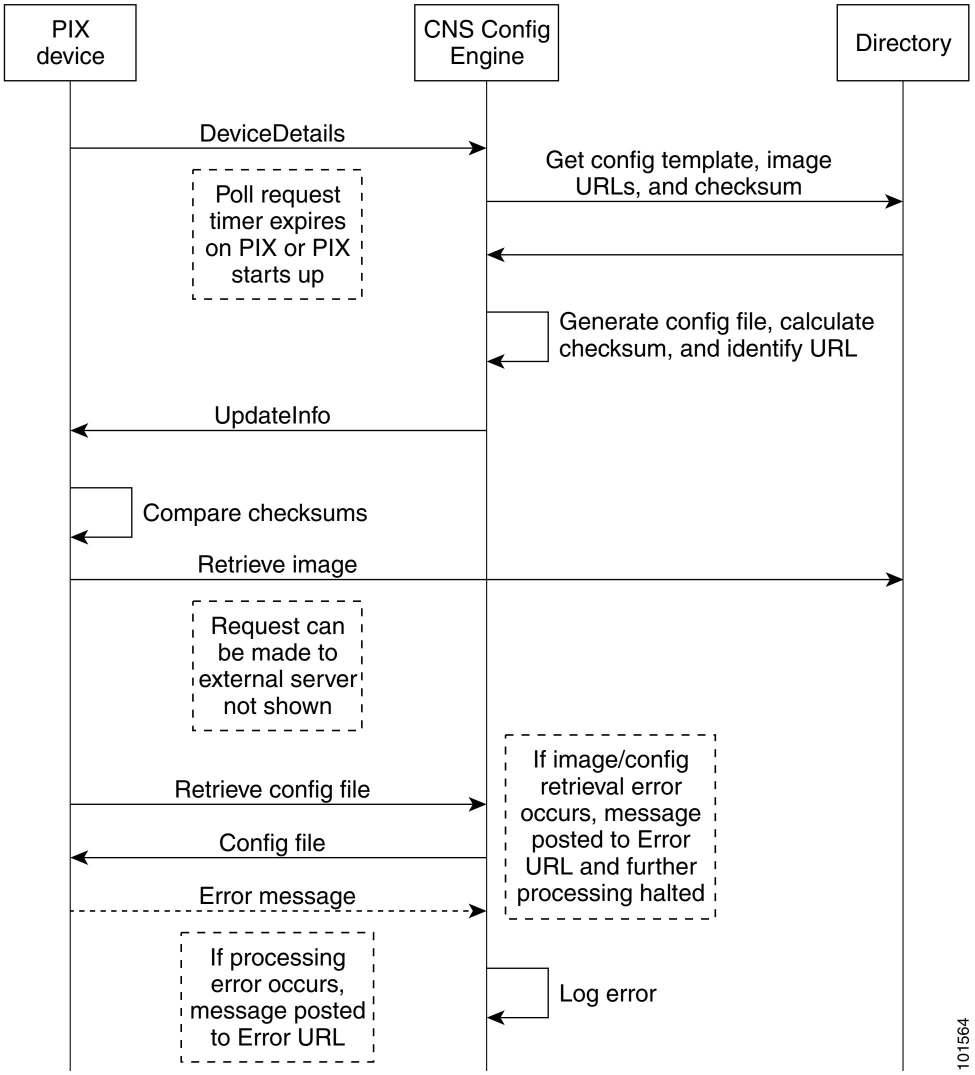
Processing a DeviceDetails Request from PIX Device

The sequence of processing a DeviceDetails request from a PIX device is as follows:

1. PIX device contacts the CNS Configuration Engine 1.4 with **DeviceDetails** as XML payload by means of an HTTPS post request.
2. New PIX Configuration servlet receives request, parses XML and retrieves DeviceID.
3. The device is authenticated.
4. The template associated with this DeviceID is processed to generate a configuration file.
5. The configuration file is converted into XML format as per the PIX DTD and the file is saved (over-written in case a file is already present for this DeviceID).
6. The checksum of XML configuration file is calculated and URL noted.
7. URLs and checksums for pix image and PDM images are retrieved from image object attached with the PIX device.
8. Checksums and URLs for configuration file and various images (if the corresponding checksum differs) and the Error URL are sent to the PIX device as an HTTP response with an XML payload (UpdateInfo)
9. Device now requests for configuration/image based on the content of the UpdateInfo response
10. If errors are encountered, information is posted to error URL.
11. The error servlet logs the errors to *pix.log*.

Figure 5-2 shows the pull model process flow.

Figure 5-2 Sequence Diagram for Pull Model of Device Update


PIX device
CNS Config Engine
Directory
DeviceDetails
Poll request timer expires on PIX or PIX starts up
Get config template, image URLs, and checksum
Generate config file, calculate checksum, and identify URL
UpdateInfo
Compare checksums
Retrieve image
Request can be made to external server not shown
If image/config retrieval error occurs, message posted to Error URL and further processing halted
Retrieve config file
Config file
Error message
If processing error occurs, message posted to Error URL
Log error
101564

PIX DeviceID

The following PIX CLI decides the value of DeviceID sent by PIX in the DeviceDetails request:

[no] auto-update device-id hardware-serial | hostname | ipaddress [*if-name***] | mac-address [***if-name***] | string text**

- **auto-update device-id** command specifies the device ID to send when polling the Management server.
- **no auto-update device-id** command resets the device ID to the default of hostname.
- **hardware-serial** option uses the PIX serial number.
- **hostname** option uses the PIX host name.
- **ipaddress** option uses the IP address of the interface with the name **if-name**.

  If the interface name is not specified, it uses the IP address of the interface used to communicate with the remote management server.

- **mac-address** option uses the MAC address of the interface with the name *if-name*.

  If the interface name is not specified, it uses the MAC address of the interface used to communicate with the remote management server.
- **string** option uses the specified *text*.

  The text can not contain white space or the characters ‘, “, <, >, & and ?.

Note Since DeviceID provided by PIX is internally mapped to ConfigID and EventID in the CNS Configuration Engine 1.4, it only supports hyphen (-), underscore (_), period (.) and alphanumeric characters.

Security Considerations

Since PIX devices are firewall devices and configuration information is vital, transport of this information is made secure by the use of SSL.

HTTPS has been enforced as the transport protocol between PIX devices and CNS Configuration Engine 1.4 under all circumstances. **DeviceDetails**, **Update Info**, **ErrorInfo** and configuration files are transported only using HTTPS. The authorization mechanism used in Configuration Service has been leveraged in the PIX server module. The URLs supplied by you towards PDM/pix-image can use HTTP or HTTPS.

PIX Device Polling Setup

PIX devices can be configured to poll the CNS Configuration Engine 1.4 at regular intervals for configuration or image updates. This entry has to be made by you on the PIX device itself. Details are available from PIX device documentation. CLI format for the same is as follows:

Usage: auto-update device-id hardware-serial | hostname |

ipaddress [<if_name>] | mac-address [<if_name>] | string <text>

no auto-update device-id

auto-update poll-period <poll-period> [<retry-count>

[<retry-period>]]

no auto-update poll-period

auto-update server <url> [verify-certificate]

no auto-update server

auto-update timeout <period>

no auto-update timeout

Example:

```
auto-update device-id string myPIXDevice
auto-update poll-period 120
auto-update server https://********@cns-ie2100/cns/PIXConfig
```

The URI to be polled on the CNS Configuration Engine 1.4 is:

/cns/PIXConfig

The **auto-update poll-period** command specifies how often to poll the Management server for configuration or image updates. The *poll-period* parameter specifies how often (in minutes) to check for an update. The default is 720 (12 hours). The *retry-count* option specifies how many times to try re-connecting to the server if the first attempt fails. The default is 0. The *retry-period* option specifies how long to wait (in minutes) between retries. The default is 5.

The **no auto-update poll-period** command resets the poll period to the default.

Also, you need to map the hostname of the server on the PIX device with its IP address. You can do this by using the *name* command as follows:

pixfirewall# **conf t**

pixfirewall(config)# **name <ip_address of the server> <hostname of the server>**

Configuration and Restrictions

PIX compatibility module is setup along with Configuration Service during the initial setup of the system in **internal directory default mode**. You need not do anything specifically to enable PIX compatibility.

PIX devices with **software versions of 6.2.1 and higher** are supported by CNS Configuration Engine 1.4 (auto-update from PIX device side was introduced in this version). All PIX hardware platforms that run software version 6.2.1 or higher will be supported.

The configuration files will be generated with options config-action= **replace** and errors=**revert**. No other options are supported.

CHAPTER 6

IMGW Device Module Development Toolkit

The IMGW device module development toolkit clearly defines the southbound interface of IMGW and provides a registration utility to allow you to register plug-in device modules into IMGW after the device module is installed onto the CNS Configuration Engine 1.4.

This chapter analyzes the requirements of the IMGW device module development toolkit and describes the functionality that is offered by this toolkit.

Note You can also implement the device module in either shell scripts or Linux/Solaris executables as long as the device module conforms to IMGW southbound interface.

User Types

This toolkit is oriented to three types of users:

- *Plug-in Developer*—responsible for developing the device module that complies with the IMGW southbound interface defined in this toolkit
- *System Administrator*—responsible for the following:
  - Plug the device module into and out of the CNS Configuration Engine 1.4
  - Register and de-register the plug-in device module
  - Update the device module on the CNS Configuration Engine 1.4
- *Network Operator*—configures the device through the plug-in device module

Toolkit Usage

There are three common usages of this toolkit:

- Plug a device module into CNS Configuration Engine 1.4 and configure devices using the device module.
- Update a device module on the CNS Configuration Engine 1.4 and configure devices through the modified device module.
- Unplug a device module from the CNS Configuration Engine 1.4.

Plug Device Module Into CNS Configuration Engine 1.4

To plug a device module into the CNS Configuration Engine 1.4 and configure devices using the device module, follow these general steps:

Step 1 The *Plug-in Developer* develops a device module conforming to the IMGW southbound interface defined in this toolkit to handle the given device type.

For information about the device module syntax, see "IMGW Southbound Interface" section on page 6-3.

Step 2 The *System Administrator* installs the device module onto CNS Configuration Engine 1.4.

Step 3 The *System Administrator* runs the registration utility to register the device module into IMGW.

Step 4 The *Network Operator* configures devices through the device module.

Update Device Module on CNS Configuration Engine 1.4

To update a device module on the CNS Configuration Engine 1.4 and configure devices using the modified device module, follow these general steps:

Step 1 The *Plug-in Developer* provides a new version of the device module.

Step 2 The *System Administrator* runs the registration utility to de-register the device module from IMGW.

If the device module you want to update is not registered, skip this step

Step 3 The *System Administrator* updates the device module with the new version on CNS Configuration Engine 1.4.

Step 4 The *System Administrator* runs registration utility to register the updated device module into IMGW.

Step 5 The *Network Operator* configures devices through modified device module.

Unplug Device Module from CNS Configuration Engine 1.4

To unplug a device module from the CNS Configuration Engine 1.4 and, follow these general steps:

Step 1 The *System Administrator* runs the registration utility to de-register the plug-in device module from IMGW.

Step 2 The *System Administrator* uninstalls the plug-in device module from the CNS Configuration Engine 1.4.

IMGW Southbound Interface

When a command execution or a configuration update event is received by IMGW runtime, it will first retrieve device type information from the device information database. If the device module corresponding to device type and operation type (**CONFIG_UPLOAD** or **CONFIG_DOWNLOAD**) is registered, IMGW runtime forks a process to execute the proper plug-in program and pass the parameter list to the plug-in program.

The initial mapping information from the <*device type, operation type*> pair to the plug-in program is read from a configuration file into memory upon start up. When IMGW is running, the system administrator can still add, remove, or update the entries of mapping information by way of the toolkit registration utility.

The *System Administrator* can modify only the entries for non-legacy device modules. This restriction is enforced by IMGW runtime.

User Designed Device Module Specifications

A user-defined device module must conform to the IMGW southbound interface as specified in this section.

Config Event

<***plug-in program***> <*temp_logfile_name*> <*logging_level*> <*device_id*> <*action_type*> <*warning_logfile_name*> <*error_logfile_name*> <*hop_information_string*> <*configuration_file_name*> <*persistence*> <*operation_timeout_value*> <*prompt_timeout_value*>.

Exec Event

<***plug-in program***> <*temp_logfile_name*> <*logging_level*> <*device_id*> <*action_type*> <*hop_information_string*> <*command_to_be_executed*> <*command_arguments*> <*exec_response_logfile_name*> <*operation_timeout_value*> <*prompt_timeout_value*>.

Hop Test

<***plug-in program***> <*temp_logfile_name*> <*logging_level*> <*device_id*> <*action_type*> <*hop_information_string*> <*operation_timeout_value*> <*prompt_timeout_value*>.

Note All files specified for the IMGW southbound interface are managed by IMGW runtime and their file names are absolute path names.

Parameter Descriptions

Plug-in Program: The plug-in program that is executed in the child process forked by IMGW runtime. The system administrator gives this information to IMGW runtime during registration.

temp_logfile_name: The full path to the device module temporary log file, which should be used by the device module to log the processing history of one instance of operation (configuration download, command execution or hop test). This file is by default located at */tmp* directory on the CNS

Configuration Engine 1.4. After the plug-in program exits, IMGW runtime puts the content of this file into a centralized log file named */opt/CSCOimgw/bin/IMGW-DEVMOD_LOG* for debugging purpose, then unlinks this file.

logging_level: It could be verbose, error, or silent. This flag can be set up by running setup command on the CNS 2100 Series system. It is recommended that the device module log information into the file <*temp_logfile_name*> based on the specified logging level.

device_id: The identification of the device that is processed by the device module. It is passed in by the *cisco.mgmt.cns.config.load* or *cisco.mgmt.cns exec.cmd* event.

action_type: It could be **config**, **exec** or **hoptest**. Action type **config** notifies the device module to update the device configuration. Action type **exec** notifies the device module to execute a command on the device. Action type **hoptest** notifies the device module to test if the device is reachable by way of the hop information provided in <*hop_information_string*>. The device module should do the proper operation in response to this flag.

warning_logfile_name: The full path to the file that is used by the device module to log all warning messages and its corresponding configuration commands line numbers. This parameter is supplied by IMGW runtime only when the action type is **config** because the information in this file is only used to generate the response message to the *cisco.mgmt.cns.config.load* event if the configure succeeds with warnings. In order for the IMGW runtime to generate the proper response message, each warning message should begin a new line and be prefixed with the string of **LINE <***line number of the configuration command that causes the warning message***>:**. An example of the warning file is as follows:

```
LINE 3: The interface has already been removed
.
.
.
LINE 7: The interface already exists.
```

The location of this file is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime puts the content of this file into the response event payload, then immediately unlinks this file.

error_logfile_name: The full path to the file that is used by the device module to log the occurrences of the error messages and their corresponding configuration command line numbers. This parameter is supplied by IMGW runtime only when the action type is **config** because the information in this file is only used to generate the response message to the *cisco.mgmt.cns.config.load* event if the configure fails. In order for the IMGW runtime to generate the proper response message, each error message should begin a new line and be prefixed with the string of **LINE <***line number of the configuration command that causes the error message***>**.

An example of the error file is as follows:

```
LINE 3: % Invalid input detected at
LINE 7: % Incomplete command
.
.
.
LINE 12: % The interface already exists
```

The location of this file is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime puts the content of this file into the response event payload, then immediately unlinks this file.

exec_response_logfile_name: The full path to the file that is used to log the output of command execution on the device. It is supplied by IMGW runtime only when the action type is **exec** and its location is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime puts the content of this file into the response event payload, then immediately unlinks this file.

hop_information_string: The string used to store the access information of the device. It is the string concatenation of all individual hop information of the device in order. An example the hop information and its <*hop_information_string*> are as follows:

Hop type	IP address	Port	Username	Password
IOS_LOGIN	172.29.145.45		Admin	Cisco
IOS_EN			Lab	Lab

The corresponding <*hop_information_string*> should be as follows:

```
“IOS_LOGIN” “172.29.145.45” “ ” “Admin” “Cisco” “IOS_EN” “ ” “ ” “Lab” “Lab”
```

Note For those fields of hop information with null value, IMGW runtime automatically adds a space before passing it to the child process.

command_to_be_executed: The command to be executed on the device. It is supplied by IMGW runtime only when the action type is **exec**.

command_arguments: The arguments of the command to be executed on the device. It is supplied by IMGW runtime only when the action type is **exec**.

configuration_file_name: The full path to the configuration file which will be downloaded onto the device. It is supplied by IMGW runtime only when the action type is **config** and its location is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime immediately unlinks this file.

persistence: y or **n**. The value **y** means the configuration needs to be written into non-volatile storage. It is supplied by IMGW runtime only when the action type is **config**. This option is dependent on the device type. This means the device module can ignore it if the device type does not support it.

operation_timeout_value: The maximum time period allowed to execute a command on the device. This parameter is now used by Expect scripts in IMGW legacy device module for IOS, CatOS, CatIOS, PIX, CSS and CE devices. A user-defined device module can ignore this parameter if it does not use it.

prompt_timeout_value: The maximum time period allowed to wait for the next prompt during login session to the device. This parameter is now used by Expect scripts in IMGW legacy device module for IOS, CatOS, CatIOS, PIX, CSS and CE devices. A user-defined device module can ignore this parameter if it does not use it.

Exit Codes

When the forked process (in which the plug-in program is executed) exits, the following exit codes are expected by IMGW runtime from the forked process:

config event:

0 – Download succeeds

1 – Download fails

2 – Download succeeds but with warning messages

Exec Event:

0 – Command execution succeeds

1 – Command execution fails

Hop Test:

0 – Hop test succeeds

1 – Hop test fails

How to Develop Plug-in Device Module

This toolkit allows the *Plug-in Developer* to use any implementation to realize the plug-in device module as long as the device module complies with IMGW southbound interface specified in “IMGW Southbound Interface” section on page 6-3.

This toolkit also provides sample code (see Appendix B, “How to Use the IMGW Device Module Development Toolkit”) in Perl plus Expect scripts as well as inline comments to help beginners to understand the workflow of the plug-in device module.

The plug-in device module should render three basic functions:

- Device configuration update
- Command execution
- Hop test

The first two functions are in response to the *cisco.mgmt.cns.config.load* and *cisco.mgmt.cns.exec.cmd* events respectively. The last one is an internal routine operation required by IMGW runtime and is transparent to network operators.

After IMGW runtime spawns a child process to execute the plug-in program, the corresponding device module should read the action type from the parameter list. If the action type is:

- **config** – device module should do device a configuration update.
- **exec** – device module should do a command execution.
- **hoptest –** device module should do hop test.

Development Guidelines

The following subsections describe the processes associated with each function.

Note The subject of actions in the subsections below is the plug-in device module.

Device Configuration Update

1. Access the device by way of the <*hop_information_string*>.
2. Download the configuration file named after <*configuration_file_name* > onto the device.
3. If above download operation succeeds, the <*persistence*> is set to **y** and the device supports this option, then write the configuration to non-volatile storage.

4. Write all warning messages prompted by the device and their corresponding configuration commands line numbers into the file named after <*warning_logfile_name*> in the specified format (see "Parameter Descriptions" section on page 6-3). The content of this file will be part of the payload of the response event if the download succeeds but with warning messages.
5. Write all error messages prompted by the device and their corresponding configuration commands' line numbers into the file named after <*error_logfile_name*> in the specified format (see "Parameter Descriptions" section on page 6-3). The first error message and its corresponding configuration command line number will be part of the payload of the response event if the download fails.
6. Based on the <*logging_level*>, selectively redirect the processing history into the file named after <*temp_logfile_name*> for debugging purpose during the whole procedure.
7. Exit with proper exit code to return control to IMGW runtime. See"Exit Codes" section on page 6-5 to get the definition of exit codes.

Command Execution

1. Access the device by way of the <*hop_information_string*>.
2. Execute on the device the <*command_to_be_executed*> with the <*command_arguments*>.
3. Capture all output from the command execution into the file named after <*exec_response_logfile_name*>. The content of this file will be part of the payload of the response event.
4. Based on the <*logging_level*>, selectively redirect the processing history into the file named after <*temp_logfile_name*> for debugging purpose during the whole procedure.
5. Exit with proper exit code to return control to IMGW runtime. See"Exit Codes" section on page 6-5 to get the definition of exit codes.

Hop Test

1. Access the device by way of the <*hop_information_string*>.
2. Based on the <*logging_level*>, selectively redirect the processing history into the file named after <*temp_logfile_name*> for debugging purpose during the whole procedure.
3. Exit with proper exit code to return control to IMGW runtime. See"Exit Codes" section on page 6-5 to get the definition of exit codes.

Installing Plug-in Device Module

The *System Administrator* is required to take charge of the install/uninstall. He/She should make sure the installation is successful before calling the registration utility.

The *System Administrator* should install all plug-in device modules into the reserved file directory of */opt/CSCOimgw/plugin-modules* with one subdirectory per device module. For example, install the device module for MGX into /opt/CSCOimgw/plugin-modules/MGX while install the one for NT into /opt/CSCOimgw/plugin-modules/NT.

The *System Administrator* should only operate within the device module installation directory to set/remove the running environment of the module. The installation activities should not affect the running environment of other components on the CNS Configuration Engine 1.4.

Registering Plug-in Device Module

The *System Administrator* must provide the device type and the full path to the plug-in program when registering a device module. IMGW runtime does not check the integrity of this information. It is responsibility of the *System Administrator* to make sure the information is correct.

This toolkit provides a dynamic registration utility to the system administrator, which allows the *System Administrator* to plug the device module into and out of IMGW seamlessly without tearing down IMGW runtime. Therefore, the services irrelevant to the device module that is being registered/de-registered will not be affected. However, this may not be the case for other services.

For example, at the time you issue the de-register command on device module *x*, the events related to *x* that are still queued in CNS event bus may get failure responses from IMGW.

Caution It is HIGHLY RECOMMENDED that the *System Administrator* notify all *Network Operators* of the upcoming registration activities so that *Network Operators* have a chance to stop beforehand any relevant operation.

End User Interface

The end user interface of IMGW device module development toolkit consists of IMGW southbound interface as well as the command line registration utility.

Configuration and Restrictions

This toolkit does not put a restriction on the maximum number of plug-in device modules that can be put into IMGW.

Device Module Restrictions

- The device module must be able to run on the Linux and/or Solaris platform.
- If the executable of the device module is a C++ binary file, it must utilize the glib that exists on CNS Configuration Engine 1.4 where applicable.
- If the executable of the device module is a java class, it must run in the existing JVM of CNS Configuration Engine 1.4.
- If the device module includes Perl and/or Expect scripts, the scripts should use the Perl and/or Expect interpreters that exist on CNS Configuration Engine 1.4.

Registration Utility Restriction

The *System Administrator* is not allowed to register/de-register IMGW legacy device module. Sometimes users may want to modify one of the legacy device modules to do upload/download operation on CatOS, CatIOS, PIX, CSS, CE or IOS devices in order to meet their specific needs. In this case, they can only modify their own copy of the legacy device module, associate a different device type name to the modified device module and register the device module into IMGW.

APPENDIX A

Troubleshooting

This appendix provides troubleshooting information. It contains information about:

- Contacting Cisco TAC
- Cannot Log In to the System
- System Cannot Connect to the Network
- Cannot Connect to the System Using a Web Browser
- System Cannot Start from the Disk
- Cannot Connect to System with SSH or SSH Interaction is Slow
- Backup and Restore not Working Properly
- How to Use the showversion Command
- How to Use the cns-send and cns-listen Commands

Contacting Cisco TAC

In some of the following sections, you might be advised to contact the Cisco Technical Assistance Center (TAC) for assistance. You can obtain TAC assistance online at http://www.cisco.com/tac.

For more information, refer to the "Obtaining Technical Assistance" section on page xiii.

Cannot Log In to the System

Problem: You cannot log in to the system.

Probable causes:

- You did not run the setup program to create an initial system configuration.
- You lost all of the user account passwords.

Resolution:

Step 1 Did you run the setup program after starting the system for the first time?

If no, run the setup program as described in the "Running the Setup Program" section on page 2-1.

If yes, continue.

Step 2 Do you know the password for any system user accounts?

If no, reconfigure the system to create a new user account. Refer to the "How to Manage User Accounts" section on page 2-31 for more information.

If yes, continue.

Step 3 If you are certain you entered a valid username and password, contact the TAC for assistance.

System Cannot Connect to the Network

Problem: The system cannot connect to the network.

Probable causes:

- The network cable is not connected to the Ethernet 0 port.
- The Ethernet 0 interface is disabled or misconfigured.
- The system is configured correctly, but the network is down or misconfigured.
- The system is not configured correctly.

Resolution:

Step 1 Verify that the network cable is connected to the Ethernet 0 port and the Link light is on.

- If the network cable is not connected, connect it.
- If the network cable is connected but the Link light is not on, these are the probable causes:
  - The network cable is faulty.
  - The network cable is the wrong type (for example, a cross-over type, rather than the required straight-through type).
  - The port on the default gateway to which the system connects is down.

If the network cable is connected and the Link light is on but the system cannot connect to the network, continue.

Step 2 Use the **ping** command to perform the following tests:

a. Try to connect to a well-known host on the network. A DNS server is a good target host.

   If the ping command can reach another host, the system is connected to the network. If it cannot connect to a particular host, the problem is with the network configuration or that host. Contact your network administrator for assistance.

   If the ping command cannot reach another host, continue.

b. Attempt to reach another host on the same subnet as the system.

   If the ping command can reach a host on the same subnet, but cannot reach a host on a different subnet, the default gateway is probably down or misconfigured.

If the ping command cannot reach any hosts, continue.

Step 3 Use the **ifconfig** command to determine if the Ethernet 0 interface is disabled or misconfigured.

If the Ethernet 0 interface is disabled, enable it. If it is misconfigured, configure it correctly. For more information, refer to "Running the Setup Program" section on page 2-1.

If the interface is enabled and correctly configured, continue.

Step 4 To ensure all network setting are configured correctly, run the **Setup** program again by entering the **setup** command in the shell prompt.

Note You cannot run **Setup** a second time by logging in as **setup** because that account is disabled for security reasons after it is used once successfully.

Step 5 Contact your network administrator to verify that there are no conditions on the network that prevent the system from connecting to the network.

If conditions prevent the system from connecting to the network, have your network administrator correct them.

Step 6 If no conditions are preventing the system from connecting to the network, contact the Cisco TAC.

Cannot Connect to the System Using a Web Browser

Problem: You cannot connect to the system by entering its IP address in a web browser.

Probable causes:

- The system cannot connect to the network.
- Encryption is enabled (plaintext disabled).
- The HTTP service is not running.

Resolution:

Step 1 Make sure that the system can connect to the network by following the procedure in the "System Cannot Connect to the Network" section on page A-2.

Step 2 When you are sure that the system is connected to the network, attempt to connect the system using a web browser.

If encryption is enabled:

- Use **https://**… to connect.
- Ensure the certificate is correct.

If you still cannot connect, continue

Step 3 To stop and start the web server only, enter the following commands:

```
/etc.rc.d/init.d/httpd stop
/etc.rc.d/init.d/httpd start
```

If the LDAP directory contains thousands of devices, restart and wait 20 minutes.

Step 4 Attempt to connect the system using a web browser.

If you cannot connect, continue.

Step 5 Restart the system.

If the LDAP directory contains thousands of devices, restart and wait 20 minutes.

Step 6 If you still cannot connect to the system using a web browser, contact the Cisco TAC for assistance.

System Cannot Start from the Disk

Problem: The system cannot start from the disk during a restart.

Probable causes:

- The disk has a physical error.
- The disk image is corrupted.

Resolution:

Step 1 If the system does not start automatically from the maintenance image and the start process fails, power the system off and then on.

Step 2 Contact the Cisco TAC if the system still cannot start from the disk.

Note If you require a replacement system, refer to the "Installing a Replacement CNS 2100 Series System" section on page 2-25 for information about installing a replacement system.

Cannot Connect to System with SSH or SSH Interaction is Slow

Problem: You cannot connect to the system using SSH or SSH interaction with the system is extremely slow, even though the system is connected to the network.

Probable cause: The system cannot get DNS services from the network. The system will not function correctly without DNS. SSH problems are the most visible symptom, but the system will have more serious problems. In most cases, it will not correctly process requests from management applications that use it.

Resolution: Perform the following steps. Connect to the console if you cannot connect using SSH.

Step 1 To set up the name servers properly, edit the */etc/resolv.conf* file.

Or, you can re-execute **Setup** (see "How to Re-execute Setup" section on page 2-2).

Step 2 Verify that the system can get DNS services from the network by entering the following command:

```
# host <dns-name>
```

where <*dns-name*> is the DNS name of a host on the network that is registered in DNS. The command returns the IP address of the host.

Step 3 If the system cannot resolve DNS names to IP addresses, the DNS server it is using is not working properly.

Resolve the network DNS problem, then continue.

Step 4 If the system can resolve DNS names to IP addresses but you still cannot connect to the system using SSH or SSH interaction with the system is extremely slow, contact the Cisco TAC.

Cannot Connect to System Using Telnet

Problem: You cannot connect to the system using Telnet even though the system is connected to the network.

Probable cause: Telnet service is disabled on the system.

Resolution: Connect to the system with SSH.

Backup and Restore not Working Properly

Problem: Your backup and restore is not working properly.

Probable causes:

- The time base for the CNS 2100 Series system is not set to the UTC time zone.
- The time has changed.
- The cron job is not started.

Resolution: Perform the following steps:

Step 1 Connect to the console if you cannot connect using SSH.

Step 2 Log into the CNS 2100 Series system as root.

Example:

```
Kernel 2.2.16-11bipsec.uid32 on an i586
login: admin
Password:
Copyright (c) 2000 Cisco Systems, Inc.
Appliance 1.0 Wed Feb 21 22:20:29 UTC 2001
Build Version (152) Wed Nov 15 12:00:13 PST 2000
bash$ su
Password:
```

Step 3 To determine if the time is correct, enter the command:

```
# date
```

Step 4 To determine the state of the cron job, enter the command:

# **/etc/rc.d/init.d/crond restart**

Example:

```
# /etc/rc.d/init.d/crond restart
Stopping cron daemon:                                       [  OK  ]
Starting cron daemon:                                       [  OK  ]
#
```

How to Use the showversion Command

Use the **showversion** command to list all the current RPMs (package managers) loaded on your CNS 2100 Series system. This command is located in the */opt/CSCOcnsie/bin* directory.

Use the **showversion** command to get the following listing:

```
Internal directory mode.

anaconda-images  Version:7.3 Release:6
compat-libs  Version:6.2 Release:3
glibc-profile  Version:2.2.5 Release:43
indexhtml  Version:7.3 Release:3
libmng-static  Version:1.0.3 Release:2
man-pages  Version:1.48 Release:2
rmt  Version:0.4b27 Release:3
ACE  Version:5.2.4 Release:0
basesystem  Version:7.0 Release:2
bdflush  Version:1.5 Release:17
chkconfig  Version:1.3.5 Release:3
cracklib  Version:2.7 Release:15
db2  Version:2.4.14 Release:10
e2fsprogs  Version:1.27 Release:3
expat  Version:1.95.2 Release:2
glib  Version:1.2.10 Release:5
glib2  Version:2.0.1 Release:2
hdparm  Version:4.6 Release:1
IBMJava2-SDK  Version:1.4 Release:0.0
krbafs  Version:1.1.1 Release:1
libaio  Version:0.3.12 Release:1
libdbi  Version:0.6.4 Release:2
libjpeg  Version:6b Release:19
libole2  Version:0.2.4 Release:1
libtool-libs  Version:1.4.2 Release:7
libungif  Version:4.1.0 Release:10
libusb  Version:0.1.5 Release:3
mailx  Version:8.1.1 Release:22
mktemp  Version:1.5 Release:14
ncurses4  Version:5.0 Release:5
open  Version:1.4 Release:14
parted  Version:1.4.24 Release:3
pcre  Version:3.9 Release:2
popt  Version:1.6.4 Release:7x.18
reiserfs-utils  Version:3.x.0j Release:3
setserial  Version:2.17 Release:5
slang  Version:1.4.5 Release:2
netconfig  Version:0.8.11 Release:7
setuptool  Version:1.8 Release:2
syslinux  Version:1.52 Release:2
expect  Version:5.32.2 Release:67
termcap  Version:11.0.1 Release:10
bash  Version:2.05a Release:13
crontabs  Version:1.10 Release:1
CSCOcnsimgs  Version:1.4 Release:0
iproute  Version:2.4.7 Release:1
groff  Version:1.17.2 Release:12
lockdev  Version:1.0.0 Release:16
MAKEDEV  Version:3.3 Release:4
info  Version:4.1 Release:1
cpio  Version:2.4.2 Release:26
diffutils  Version:2.7.2 Release:5
fileutils  Version:4.1 Release:10.1
CSCOcnspki  Version:1.3 Release:0
```

```
findutils  Version:4.1.7 Release:4
grep  Version:2.5.1 Release:1
less  Version:358 Release:24
libgtop  Version:1.0.12 Release:8
libxml10  Version:1.0.0 Release:8
mgetty  Version:1.1.30 Release:0.7
bind-utils  Version:9.2.1 Release:1.7x.2
openssl-perl  Version:0.9.6b Release:32.7
pdksh  Version:5.2.14 Release:16
procmail  Version:3.22 Release:5
psmisc  Version:20.2 Release:3.73
raidtools  Version:1.00.2 Release:1.3
ftp  Version:0.17 Release:13
readline2.2.1  Version:2.2.1 Release:4
redhat-release  Version:7.3 Release:1
routed  Version:0.17 Release:8
console-tools  Version:19990829 Release:40
ntp  Version:4.1.1 Release:1
slocate  Version:2.6 Release:1
tar  Version:1.13.25 Release:4.7.1
tcsh  Version:6.10 Release:6
telnet  Version:0.17 Release:20
dev  Version:3.3 Release:4
mouseconfig  Version:4.25 Release:1
time  Version:1.7 Release:16
tmpwatch  Version:2.8.3 Release:1
CSCOcnscommon  Version:1.3 Release:0
unzip  Version:5.50 Release:11
hotplug  Version:2002_04_01 Release:3
vim-common  Version:6.1 Release:18.7x.2
wget  Version:1.8.2 Release:4.73
words  Version:2 Release:18
pam  Version:0.75 Release:46.7.3
cyrus-sasl  Version:1.5.24 Release:25
cyrus-sasl-plain  Version:1.5.24 Release:25
openldap  Version:2.0.27 Release:2.7.3
passwd  Version:0.67 Release:1
krb5-libs  Version:1.2.4 Release:11
krb5-workstation  Version:1.2.4 Release:11
modutils  Version:2.4.18 Release:3.7x
mkinitrd  Version:3.3.10 Release:1
mkbootdisk  Version:1.4.3 Release:1
pam_krb5  Version:1.55 Release:1
SysVinit  Version:2.84 Release:2
vim-enhanced  Version:6.1 Release:18.7x.2
zip  Version:2.3 Release:12
file  Version:3.39 Release:8.7x
dhcpcd  Version:1.3.22pl1 Release:7
libgcj  Version:2.96 Release:29
libpng  Version:1.0.14 Release:0.7x.4
libtiff  Version:3.5.7 Release:2
libglade  Version:0.17 Release:5
librsvg  Version:1.0.2 Release:1
libglade2  Version:1.99.9 Release:2
mod_auth_any  Version:1.2.2 Release:2
mod_dav  Version:1.0.3 Release:5
mod_put  Version:1.3 Release:4
mod_roaming  Version:1.0.2 Release:4
mod_throttle  Version:3.1.2 Release:5
apacheconf  Version:0.8.2 Release:2
libxslt-python  Version:1.0.15 Release:1
ibm_directory  Version:5.1.1 Release:0
rpm-perl  Version:4.0.4 Release:7x.18
anaconda  Version:7.3 Release:7
```

```
rpmfind  Version:1.7 Release:7
Tibco  Version:7.1 Release:0
CSCOImgwDeviceServer  Version:1.4 Release:0.0
CSCOdat  Version:1.3 Release:0
CSCOTools  Version:1.2 Release:0
initscripts  Version:6.67 Release:1
hwcrypto  Version:1.0 Release:3
kernel  Version:2.4.20 Release:19.7
kernel-smp  Version:2.4.20 Release:19.7
lokkit  Version:0.50 Release:8
openssh-askpass  Version:3.5p1 Release:1
openssh-server  Version:3.5p1 Release:1
portmap  Version:4.0 Release:41
quota  Version:3.03 Release:1
vixie-cron  Version:3.0.1 Release:64
xinetd  Version:2.3.11 Release:1.7x
tftp-server  Version:0.28 Release:2
ypbind  Version:1.10 Release:7
ypserv  Version:2.5 Release:2.7x
IBM_db2msen81  Version:8.1.0 Release:16
IBM_db2cucs81  Version:8.1.0 Release:16
IBM_db2icuc81  Version:8.1.0 Release:16
IBM_db2jhen81  Version:8.1.0 Release:16
IBM_db2sp81  Version:8.1.0 Release:16
IBM_db2cj81  Version:8.1.0 Release:16
IBM_db2ca81  Version:8.1.0 Release:16
IBM_db2crte81  Version:8.1.0 Release:16
IBM_db2engn81  Version:8.1.0 Release:16
IBM_db2wssg81  Version:8.1.0 Release:16
ldap-clientd  Version:5.1 Release:1
ldap-msg_en_US  Version:5.1 Release:1
lincimom  Version:1.0 Release:1
mpcim  Version:1.0 Release:01
asmlxag  Version:3.1.1 Release:0
SysAvailAgent  Version:3.11 Release:1
anaconda-help  Version:7.3 Release:2
anaconda-runtime  Version:7.3 Release:7
glibc-common  Version:2.2.5 Release:43
hwdata  Version:0.14.1 Release:1
libelf  Version:0.7.0 Release:2
mailcap  Version:2.1.9 Release:2
redhat-logos  Version:1.1.3 Release:1
setup  Version:2.5.12 Release:1
filesystem  Version:2.1.6 Release:2
glibc  Version:2.2.5 Release:43
bzip2-libs  Version:1.0.2 Release:2
compat-libstdc++  Version:6.2 Release:2.9.0.16
db1  Version:1.85 Release:8
db3  Version:3.3.11 Release:6
eject  Version:2.0.12 Release:4
gdbm  Version:1.8.0 Release:14
glib10  Version:1.0.6 Release:10
gmp  Version:4.0.1 Release:3
hesiod  Version:3.0.2 Release:18
iputils  Version:20020124 Release:3
ksymoops  Version:2.4.4 Release:1
libcap  Version:1.10 Release:8
libghttp  Version:1.0.9 Release:2
libjpeg6a  Version:6a Release:8
libsigc++  Version:1.0.3 Release:5
libtool-libs13  Version:1.3.5 Release:2
libunicode  Version:0.4 Release:6
losetup  Version:2.11n Release:12.7.3
mingetty  Version:1.00 Release:1
```

```
mm  Version:1.1.3 Release:11
net-tools  Version:1.60 Release:4
pam_smb  Version:1.1.6 Release:2
patch  Version:2.5.4 Release:12
perl  Version:5.6.1 Release:34.99.6
pwdb  Version:0.61.2 Release:2
rsh  Version:0.17 Release:5
shadow-utils  Version:20000902 Release:9.7
newt  Version:0.50.35 Release:1
ntsysv  Version:1.3.5 Release:3
specspo  Version:7.3 Release:4
tcl  Version:8.3.3 Release:67
tcllib  Version:1.0 Release:67
libtermcap  Version:2.0.8 Release:28
bzip2  Version:1.0.2 Release:2
CSCOcnscfgs  Version:1.4 Release:0
dhcp  Version:2.0pl5 Release:8
libstdc++  Version:2.96 Release:113
libungif-progs  Version:4.1.0 Release:10
logrotate  Version:3.6.4 Release:1
ncurses  Version:5.2 Release:26
binutils  Version:2.11.93.0.2 Release:11
cpp  Version:2.96 Release:113
ed  Version:0.2 Release:25
at  Version:3.1.8 Release:23
CSCOImgwConfig  Version:1.4 Release:0.0
gawk  Version:3.1.0 Release:4
grub  Version:0.91 Release:4
gzip  Version:1.3.3 Release:1
libtool  Version:1.4.2 Release:7
man  Version:1.5j Release:7.7x.0
openssl  Version:0.9.6b Release:32.7
libesmtp  Version:0.8.12 Release:0.7.x
patchutils  Version:0.2.11 Release:2
perladdon  Version:1.0 Release:1
procps  Version:2.0.7 Release:12
pxe  Version:0.1 Release:31.99.7.3
readline  Version:4.2a Release:4
librep  Version:0.15.1 Release:3
readline41  Version:4.1 Release:10
rootfiles  Version:7.2 Release:1
sed  Version:3.02 Release:11
kbdconfig  Version:1.9.15 Release:2
sharutils  Version:4.2.1 Release:9
sysklogd  Version:1.4.1 Release:8
tclx  Version:8.3 Release:67
metamail  Version:2.7 Release:28
textutils  Version:2.0.21 Release:1
mount  Version:2.11n Release:12.7.3
tftp  Version:0.28 Release:2
Tivoli  Version:93 Release:1
tomcat  Version:4.1.18 Release:0
CSCOcnsnsm  Version:1.5 Release:0
usbutils  Version:0.9 Release:5
utempter  Version:0.5.2 Release:6
vim-minimal  Version:6.1 Release:18.7x.2
which  Version:2.13 Release:3
cracklib-dicts  Version:2.7 Release:15
authconfig  Version:4.2.8 Release:4
cyrus-sasl-md5  Version:1.5.24 Release:25
gpm  Version:1.19.3 Release:21
libuser  Version:0.50.2 Release:1
sh-utils  Version:2.0.11 Release:14
krb5-server  Version:1.2.4 Release:11
```

```
krbafs-utils  Version:1.1.1 Release:1
kudzu  Version:0.99.52 Release:1
lilo  Version:21.4.4 Release:14
nscd  Version:2.2.5 Release:43
sendmail  Version:8.11.6 Release:25.73
usermode  Version:1.53 Release:2
xerces  Version:1.5 Release:0
zlib  Version:1.1.4 Release:8.7x
apache  Version:1.3.27 Release:2
gnupg  Version:1.0.6 Release:5
libmng  Version:1.0.3 Release:2
glibc-utils  Version:2.2.5 Release:43
libxml  Version:1.8.17 Release:3
libgtkhtml9  Version:0.9.2 Release:10
libxml2  Version:2.4.19 Release:4
libxslt  Version:1.0.15 Release:1
mod_bandwidth  Version:2.0.3 Release:3
mod_perl  Version:1.26 Release:5
mod_python  Version:2.7.8 Release:1
mod_ssl  Version:2.8.12 Release:2
python  Version:1.5.2 Release:43.73
libxml2-python  Version:2.4.19 Release:4
rpm  Version:4.0.4 Release:7x.18
rpm-build  Version:4.0.4 Release:7x.18
rpm-python  Version:4.0.4 Release:7x.18
rpm2html  Version:1.7 Release:6
rpmlint  Version:0.38 Release:5
CSCOcnses  Version:1.9 Release:0
CSCOimgw  Version:1.4 Release:0.0
CSCOencryption  Version:1.4 Release:1
util-linux  Version:2.11n Release:12.7.3
bind  Version:9.2.1 Release:1.7x.2
ipchains  Version:1.3.10 Release:13
iptables  Version:1.2.5 Release:3
kernel-utils  Version:2.4 Release:7.4
iptables  Version:1.2.5 Release:3
kernel-utils  Version:2.4 Release:7.4
libpcap  Version:0.6.2 Release:17.7.3.2
openssh  Version:3.5p1 Release:1
openssh-clients  Version:3.5p1 Release:1
pciutils  Version:2.1.9 Release:2
nfs-utils  Version:0.3.3 Release:5
timeconfig  Version:3.2.7 Release:1
anacron  Version:2.3 Release:17
telnet-server  Version:0.17 Release:20
wu-ftpd  Version:2.6.2 Release:11.73.1
yp-tools  Version:2.6 Release:4
zCSCOcnssetup  Version:1.5 Release:0
IBM_db2cliv81  Version:8.1.0 Release:16
IBM_db2conv81  Version:8.1.0 Release:16
IBM_db2icut81  Version:8.1.0 Release:16
IBM_db2repl81  Version:8.1.0 Release:16
IBM_db2chen81  Version:8.1.0 Release:16
IBM_db2jdbc81  Version:8.1.0 Release:16
IBM_db2rte81  Version:8.1.0 Release:16
IBM_db2das81  Version:8.1.0 Release:16
IBM_db2smpl81  Version:8.1.0 Release:16
IBM_db2cc81  Version:8.1.0 Release:16
ldap-serverd  Version:5.1 Release:1
```

How to Use the cns-send and cns-listen Commands

Use the **cns-send** and **cns-listen** commands to send and receive test messages to the event gateway in the Cisco CNS Configuration Engine 1.4. These commands are located in the /opt/CSCOcnsie/tools directory.

cns-send

The syntax for the cns-send command is:

cns-send -version

or

cns-send [-service <*service*>**] [-network** <*network*>**] [-daemon** <*daemon*>**] [-file** <*filename*>**]** <*subject*> **[**<*message*>**]**

Syntax Description

-version	Outputs the version of cns-send.
-service <*service*>	(Optional) The port number (default: 7500).
-network <*network*>	(Optional) Network interface (in local machine) where messages are sent.
-daemon <*daemon*>	(Optional) Internal port of application to the rvd daemon (default: 7500).
-file <*filename*>	(Optional) Filename containing the XML-message. The filename can be sent instead of individual subject/messages.
<*subject*>	Subject name of the message.
<*message*>	(Optional) Message in the message field.

To use the cns-send command, follow these steps:

Step 1 Log into the CNS 2100 Series system as root.

Step 2 Change directories to **/opt/CSCOcnsie/tools**.

Step 3 Type **./cns-send -file** <*filename*> <*subject*>

Note The cns-send command sends messages in the opaque data format.

cns-listen

The syntax for the cns-listen command is:

cns-listen -version

or

cns-listen [-service <*service***>] [-network <***network***>] [-daemon <***daemon***>] <***subject_list***>**

Syntax Description

-version	Outputs the version of cns-listen.
-service <*service*>	(Optional) The port number (default: 7500).
-network <*network*>	(Optional) Network interface (in local machine) where messages are received.
-daemon <*daemon*>	(Optional) Internal port of application to the rvd daemon (default: 7500).
<*subject_list*>	Subjects listen to.

To use the cns-listen command, follow these steps:

Step 1 Log into the CNS 2100 Series system as root.

Step 2 Change directories to **/opt/CSCOcnsie/tools**.

Step 3 Type **./cns-listen** <*subject_list*>

Usage Guidelines

Use the greater than symbol (>) for a wildcard.

Examples

./cns-listen “cisco.cns.config.load”

./cns-listen “cisco.cns.>”

How to Re-activate IBM Director Agent After Setup

In this release, one of the IBM Director agents is disabled at the end of **Setup**. This happens to release unused CPU cycles.

To re-activate this agent follow these steps:

Step 1 Login as root.

Step 2 Type the following command string:

cp /etc/TWGagent/TWGagent.orig /etc/TWGagent/TWGagent

/opt/CSCOcnsie/bin/TWGagent start

Note This procedure must be run after each **Setup**.

APPENDIX B

How to Use the IMGW Device Module Development Toolkit

This appendix explains how to add, update, and delete device modules using the IMGW Device Module Development Toolkit.

Overview

The program can be a script or a binary program. It must take command line arguments with the following format:

- For config event:

  <**plugin program**> <*temp_logfile_name*> <*logging_level*> <*device_id*> <*action_type*> <*warning_logifle_name*> <*error_logfile_name*> <*hop_information_string*> <*configuration_file_name*> <*persistence*> <*operation_timeout_value*> <*prompt_timeout_value*>

- For exec event:

  <**plugin program**> <*temp_logfile_name*> <*logging_level*> <*device_id*> <*action_type*> <*hop_information_string*> <*command_to_be_executed*> <*command_arguments*> <*exec_response_logfile_name*> <*operation_timeout_value*> <*prompt_timeout_value*>

- For hoptest:

  <**plugin program**> <*temp_logfile_name*> <*logging_level*> <*device_id*> <*action_type*> <*hop_information_string*> <*operation_timeout_value*> <*prompt_timeout_value*>

Input Parameters

The following is a list of arguments and their descriptions for the current supported device program. A plug-in program can interpret the meaning of passed arguments differently, and does not necessarily use all the arguments passed to it.

plug-in program – The plug-in program that executes in the child process forked by IMGW runtime. System administrator gives this information to IMGW runtime during registration.

temp_logfile_name – The full path to the device module temporary log file, which should be used by the device module to log the processing history of one instance of operation (configuration download, command execution or hop test). This file is by default located at */tmp* directory on CNS 2100 Series system. After the plug-in program exits, IMGW runtime puts the content of this file into a centralized log file named after */opt/CSCOimgw/bin/IMGW-DEVMOD_LOG* for debugging purpose and then unlink this file.

logging_level – The value could be verbose, error or silent. This flag can be set by running setup command on the CNS 2100 Series system. It is recommended that the device module log information into the file of <*temp_logfile_name*> based on the specified logging level.

device_id – The identification of the device that is processed by the device module. It is passed in by the *cisco.mgmt.cns.config.load* or *cisco.mgmt.cns.exec.cmd* event.

action_type – It could be **config**, **exec**, or **hoptest**. The action type **config** notifies the device module to update the device configuration; **exec** notifies the device module to execute a command on the device; **hoptest** notifies the device module to test if the device is reachable by means of the hop information provided in <*hop_information_string*>. The device module should do the proper operation in response to this flag.

warning_logfile_name – The full path to the file that is used by the device module to log all warning messages and its corresponding configuration command line numbers. This parameter is supplied by IMGW runtime only when the action type is **config** because the information in this file is only used to generate the response message to the *cisco.mgmt.cns.config.load* event if the configure succeeds with warnings. In order for the IMGW runtime to generate the proper response message, each warning message should begin a new line and be prefixed with the string of **LINE** <*line number of the configuration command that causes the warning message*>**:**. An example of the warning file is as follows:

```
LINE 3: The interface has already been removed
.
.
.
LINE 7: The interface already exists.
```

The location of this file is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime will put the content of this file into the response event payload and then unlink this file immediately.

error_logfile_name – The full path to the file that is used by the device module to log the occurrences of the error messages and their corresponding configuration command line numbers. This parameter is supplied by IMGW runtime only when the action type is **config** because the information in this file is only used to generate the response message to the *cisco.mgmt.cns.config.load* event if the configure fails. In order for the IMGW runtime to generate the proper response message, each error message should begin a new line and be prefixed with the string of **LINE** <*line number of the configuration command that causes the error message*>:. An example of the error file is as follows:

```
LINE 3: % Invalid input detected at
LINE 7: % Incomplete command
.
.
.
LINE 12: % The interface already exists
```

The location of this file is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime will put the content of this file into the response event payload and then unlink this file immediately.

exec_response_logfile_name – The full path to the file that is used to log the output of command execution on the device. It is supplied by IMGW runtime only when the action type is **exec** and its location is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime will put the content of this file into the response event payload and then unlink this file immediately.

hop_information_string – The string used to store the access information of the device. It is the string concatenation of all individual hop information of the device in order. An example the hop information and its <*hop_information_string*> are as follows:

Hop type	IP address	Port	Username	Password
IOS_LOGIN	172.29.145.45		Admin	Cisco
IOS_EN			Lab	Lab

The corresponding <*hop_information_string*> should be as follows:

```
"IOS_LOGIN" "172.29.145.45" " " "Admin" "Cisco" "IOS_EN" " " " " "Lab" "Lab"
```

Note For those fields of hop information with null value, IMGW runtime automatically adds a space before passing it to the child process.

command_to_be_executed – The command to be executed on the device. It is supplied by IMGW runtime only when the action type is **exec**.

command_arguments – The arguments of the command to be executed on the device. It is supplied by IMGW runtime only when the action type is **exec**.

configuration_file_name – The full path to the configuration file which will be downloaded onto the device. It is supplied by IMGW runtime only when the action type is **config** and its location is under */tmp* on the CNS 2100 Series system. After the plug-in program exits, IMGW runtime will unlink this file immediately.

persistence – **y** or **n**. The symbol **y** means the configuration needs to be written into non-volatile storage and so forth. It is supplied by IMGW runtime only when the action type is **config**. This option is dependent on the device type. It means the device module can ignore it if the device type does not support it.

operation_timeout_value – The maximum time period allowed to execute a command on the device. This parameter is now used by Expect scripts in IMGW legacy device module for IOS, CatOS, CatIOS, PIX, CSS and CE devices. User-defined device module can ignore this parameter if they do not use it.

prompt_timeout_value – The maximum time period allowed to wait for the next prompt during login session to the device. This parameter is now used by Expect scripts in IMGW legacy device module for IOS, CatOS, CatIOS, PIX, CSS and CE devices. User-defined device module can ignore this parameter if they do not use it.

Exit Code

When the forked process (in which the plug-in program is executed) exits, the following exit code is expected by IMGW runtime from the forked process:

For config event

0 – Download succeeds

1 – Download fails

2 – Download succeeds but with warning messages

For exec event

0 – Command execution succeeds

1 – Command execution fails

For hop test

0 – Hop test succeeds

1 – Hop test fails

Flow of Events for Plug-in Device Module

The following is a brief description of program flow for the three different commands: **config**, **exec**, and **hoptest**. The first two functionalists are in response to the *cisco.mgmt.cns.config.load* and *cisco.mgmt.cns.exec.cmd* events respectively, while the last one is an internal routine operation required by IMGW runtime, thus is transparent to network operators.

After IMGW runtime spawns a child process to execute the plug-in program, the corresponding device module should read the action type from the parameter list. If the action type is **config**, then the device module should do device configuration update; if it is **exec**, then the device module should do command execution; if it is **hoptest** the device module should do hop test.

Device Configuration Update

1. Access the device by means of the <*hop_information_string*>.
2. Download the configuration file named after <*configuration_file_name*> onto the device.
3. If above download operation succeeds, the <*persistence*> is set to **y** and the device supports this option, write the configuration to non-volatile storage.
4. Write all warning messages prompted by the device and their corresponding configuration command line numbers into the file named after <*warning_logfile_name*>. The content of this file will be part of the payload of the response event if the download succeeds but with warning messages.
5. Write all error messages prompted by the device and their corresponding configuration command line numbers into the file named after <*error_logfile_name*>. The first error message and its corresponding configuration command line number will be part of the payload of the response event if the download fails.
6. Based on the <*logging_level*>, selectively redirect the processing history into the file named after <*temp_logfile_name*> for debugging purpose during the whole procedure.
7. Exit with proper exit code to return control to IMGW runtime

Command Execution

1. Access the device by means of the <*hop_information_string*>.
2. Execute on the device the <*command_to_be_executed*> with the <*command_arguments*>.
3. Capture all output from the command execution into the file named after <*exec_response_logfile_name*>. The content of this file will be part of the payload of the response event.

4. Based on the <*logging_level*>, selectively redirect the processing history into the file named after <*temp_logfile_name*> for debugging purpose during the whole procedure.
5. Exit with proper exit code to return control to IMGW runtime.

Hop Test

1. Access the device by means of the <*hop_information_string*>.
2. Based on the <*logging_level*>, selectively redirect the processing history into the file named after <*temp_logfile_name*> for debugging purpose during the whole procedure.
3. Exit with proper exit code to return control to IMGW runtime.

A simple example is given in “Code Sample” section on page B-7. The sample program is a script that connects to a UNIX/Linux workstation by means of **rlogin** and runs a command passed to it. It responds to exec events.

How to Add a New Device Module

Step 1 Create a device module plug-in program.

Step 2 Unit test the program created in Step 1.

Step 3 Copy the program to the CNS 2100 Series system under */opt/CSCOimgw/plugin-modules/<device_type>*.

Make sure that it has execute permission.

Assume the device type is MYDEV, an example would be: */opt/CSCOimgw/plugin-modules/MYDEV/my-handler.exp*

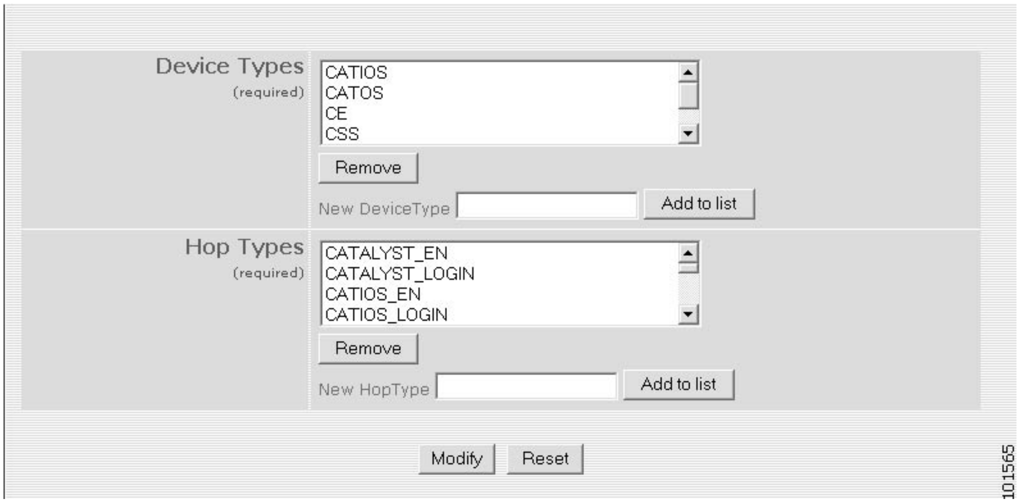
Step 4 To register the program with the CNS 2100 Series system, type the following command (assuming the CNS 2100 Series system gateway ID is **imgw-test1**):

% imgw-devmod-register –gateway imgw-test1 –devtype MYDEV –optype exec –cmd /opt/CSCOimgw/plugin-modules/MYDEV/my-handler.exp

Step 5 Add device type and hop type through DAT (see

a. From the Home page, click on the **Tools** tab.
b. Click on **DAT** and login.
c. From the DAT page, click on **IMGW**.
d. Click on **Edit Hop/Device Type**.
e. Type in device type from Step 3 into the **New DeviceType** box and click **Add to list**. (see Figure B-1)
f. Type a new hop type into the **New HopType** box and click **Add to list**.
g. Click **Modify**.

Figure B-1 Add Device Module



How to Update an Existing Device Module

Step 1 Get a new device module plug-in program.

Step 2 To deregister the old program as follows, type the following command:

```
% imgw-devmod-deregister –gateway imgw-test1 –devtype MYDEV –optype exec
```

Step 3 Copy the program created in Step 1 to the CNS 2100 Series system under */opt/CSCOimgw/plugin-modules/<device_type>*.

For example, the new file is:

/optCSCOimgw/plugin-modules/MYDEV/new_handler.exp

Step 4 To register the new program with the CNS 2100 Series system as follows, type the following command:

```
% imgw-devmod-register –gateway imgw-test1 –devtype MYDEV –optype exec -cmd
/optCSCOimgw/plugin-modules/MYDEV/new_handler.exp
```

How to Delete a Device Module

Step 1 Remove device type and hop type through DAT

a. From the Home page, click on the **Tools** tab.

b. Click on **DAT** and login.

c. From the DAT page, click on **IMGW**.

d. Click on **Edit Hop/Device Type.**

e. Select the device type removed, and click **Remove** (see Figure B-1).

f. Select hop type associated with the deleted device type and click **Remove**.

g. Click **Modify**.

Step 2 To deregister the program, type the following command:

% imgw-devmod-register –gateway imgw-test1 –devtype MYDEV –optype exec

Step 3 To remove plug-in program from /opt/CSCOimgw/plugin-modules, type the following command:

% rm –fr /opt/CSCOimgw/plugin-modules/MYDEV/

Code Sample

```
#!/usr/bin/expect

# exit status:
# 0: success
# 1: failure

#exp_internal 1

###################################################################
#
# Get necessary arguments
#
###################################################################

# arg 1 loglevel is not used in this script
# arg 2 deviceid is not used in this script

# the contents of log is written to /opt/CSCOimgw/bin/IMGW-DEVMOD-LOG
set log [lindex $argv 0]

set action [lindex $argv 3]

###################################################################
#
# Hopinfo contains information to access a device.
# Hopinfo format:
# <hoptype> <ip> <port> <username> <password>
# eg)
# "IOS_LOGIN" "10.1.2.3" "0" "admin" "cisco"
# "IOS_EN" "" "" "labuser" "labpasswd"
#
###################################################################

set hopinfo [lindex $argv 4]

# hostname is 1st arg in hopinfo, username is 3rd and password the 4th
set hostname [lindex $argv 5]
set username [lindex $argv 7]
set password [lindex $argv 8]

set f [open $log w]
puts $f "hostname= $hostname, user= $username, passwd=$password"

###################################################################
#
# Get command to be executed.
#
```

```
####################################################################

# for this test script, there is only one hop entry, so the next arg is at
# [hopindex + 5]. If more than one hop entry exists, the next arg will be
# at [hopindex + x*5] where x is the number of hop entries.

set cmd [lindex $argv 9]
set cmdargs [lindex $argv 10]


####################################################################
#
# the contents of response log is included in the response event,
# and is logged in /opt/CSCOimgw/bin/IMGW-LOG-<hostname>
#
####################################################################

set reslog [lindex $argv 11]

# the remaining args op_timeout and prompt_timeout are not used

puts $f "Executing rlogin.exp"
puts $f "action= $action, cmd= $cmd, cmdargs= $cmdargs, hopinfo= $hopinfo"


####################################################################
#
# Do some error checking for input arguments.
#
####################################################################

if { [string match $action "exec"] !=1 } {
   puts $f "Error: Unknown action type, exit program."
   close $f
   exit 1
}

####################################################################
#
# Actual work here
#
####################################################################

puts $f "Calling command rlogin $hostname -l $username"
eval spawn -noecho "rlogin $hostname -l $username"

log_file -noappend $reslog
expect {
    -nocase "Password:" { send "$password\r" }
}

expect {
    -re "\-\>" {
        send "$cmd $cmdargs\r"
    }
    -re "\\$" {
        send "$cmd $cmdargs\r"
    }
}

expect {
    -re "\-\>" {
        send "exit\n"
    }
    -re "\\$" {
        send "exit\n"
    }
}
log_file

puts $f "Done"
close $f

###################################################################
#
# Return success exit code here
#
###################################################################

exit 0
```

Software Licenses and Acknowledgements

This appendix lists licenses for the following private and, so called, public domain software used by this product:

- OpenSSL
- Apache and Tomcat
- ssldump

OpenSSL

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).”

4. The names “mod_ssl” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called “mod_ssl” nor may “mod_ssl” appear in their names without prior

written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).”

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE

LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache and Tomcat

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).” Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names “Apache” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>. Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

ssldump

Mozilla Public License

The Original Code is RHINO v 1.5.3.

GNU General Public License

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

GNU Lesser General Public License

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages—typically libraries—of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”).

Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

“Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

> a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
>
> b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2 will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

INDEX