# Cisco CNS Configuration Engine Administrator's Guide

Version 1.3

**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-1791-02

*Cisco CNS Configuration Engine Administrator's Guide*

# CONTENTS

# Preface

This document describes how to install and configure the software for the Cisco CNS Configuration Engine 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:

- *Release Notes for Cisco CNS Configuration Engine*
- *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 Software Development kit Programmer's Guide and API Reference*

# Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

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

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

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/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

## Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

- Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

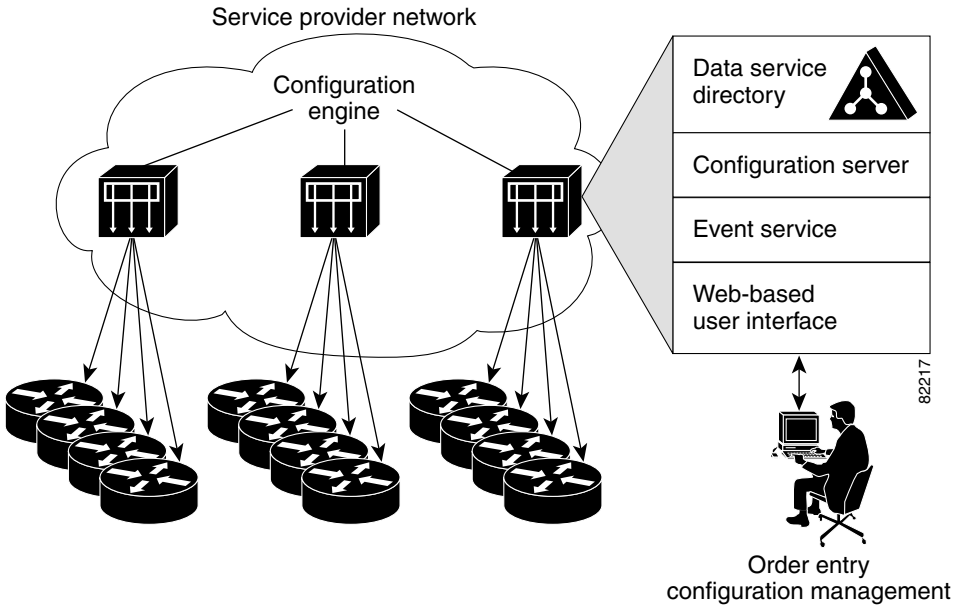

# Product Overview

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

- Modes of Operation
- CNS Configuration Service
- CNS Event Service
- Intelligent Modular Gateway
- Data Administration Tool
- How the Cisco CNS Configuration Engine Works
- Network Management Tools

The Cisco CNS Configuration Engine 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 runs on the Cisco CNS 2100 Series Intelligence Engine (CNS 2100 Series system) hardware platform.

***Figure 1-1 Cisco CNS Configuration Engine Architectural Overview***



Each Cisco CNS Configuration Engine manages a group of Cisco IOS devices (routers) and services they deliver, storing their configurations and delivering them as needed. The Cisco CNS Configuration Engine 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.

The Cisco CNS Configuration Engine is a web-based system for automatically distributing configuration files to Cisco IOS network devices running Cisco IOS version 12.2(2) T, or later where authentication is NOT used. Cisco IOS version 12.2(11)T is required if encryption or authentication is used.

**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 1-5.

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

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

The Cisco CNS Configuration Engine 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.

# Modes of Operation

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

- Internal Directory Mode
- External Directory Mode

## Internal Directory Mode

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

- Novell Directory Services
- Microsoft Active Directory
- iPlanet

# CNS Configuration Service

The CNS Configuration Service is the core component of the Cisco CNS Configuration Engine. 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 3-42).

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 uses the CNS Event Service for receipt and generation of configuration 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.

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.

# NameSpace Mapper

The Cisco CNS Configuration Engine includes the NameSpace Mapper (NSM) that provides a lookup service for managing logical groups of devices based on application, device/group ID, and event.

For a subscriber, when given a unique device ID and event, the namespace mapping service returns a set of events to which to subscribe. Similarly, for a publisher, when given a unique group ID, device ID, and event, the mapping service returns a set of events on which to publish.

The CNS Namespace Mapping Service 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.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.cns.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 three NSM modes:

- Default
- Provider
- None

The NSM mode is set when you run the **Setup** program (see "Running the Setup Program" section on page 2-1).

## Default Mode

No directory setup is required for Default mode. The DeviceID is just appended to the subject. This allows you to individually address a device.

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

## 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.

### None Mode

No directory setup is required for None mode. No subject mapping is done. All devices are subscribed to the same subject and respond on the same subject.

**Note** This mode should be used only for broadcast events.

To set None mode, use **none** 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 Programmer's Guide and API Reference*.

Directory setup can be done using the Directory Administration Tool (see "Directory Administration Tool" section on page 5-1.

## 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**.

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 prompts for this parameters value during **Setup** with the message:

```
Enter NSM directive (none, default, http):
```

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

**Note** If you are migrating groups and devices from Release 1.2 to 1.3, you must use the value for this parameter when you establish reference to an application namespace for this NSM mode. For more information, see "Importing Groups and Devices from Release 1.2 to 1.3" section on page 2-22.

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 1-9) 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:
```

# Intelligent Modular Gateway

Intelligent Modular Gateway allows you to run the Cisco CNS Configuration Engine 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 methods are Telnet or 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 a Telnet or SSH transport creates some restrictions in terms of how the Cisco CNS Configuration Engine architecture is used.

- When using Telnet or 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 architecture is accomplished by an intelligent agent in the device that has access to internal parser functions. A Telnet or 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 Telnet or 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 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 Telnet or SSH as a transport. If an initial configuration needs to be delivered by the Cisco CNS Configuration Engine, 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 2511 communication server.

  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 Telnet or 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.

# Modular Router Support

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. 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 interface cards or line cards (see Figure 1-3 on page 1-8). Device management has been extended to support sub-devices representing line cards.

*Figure 1-2 Cisco 3660 Modular Router*

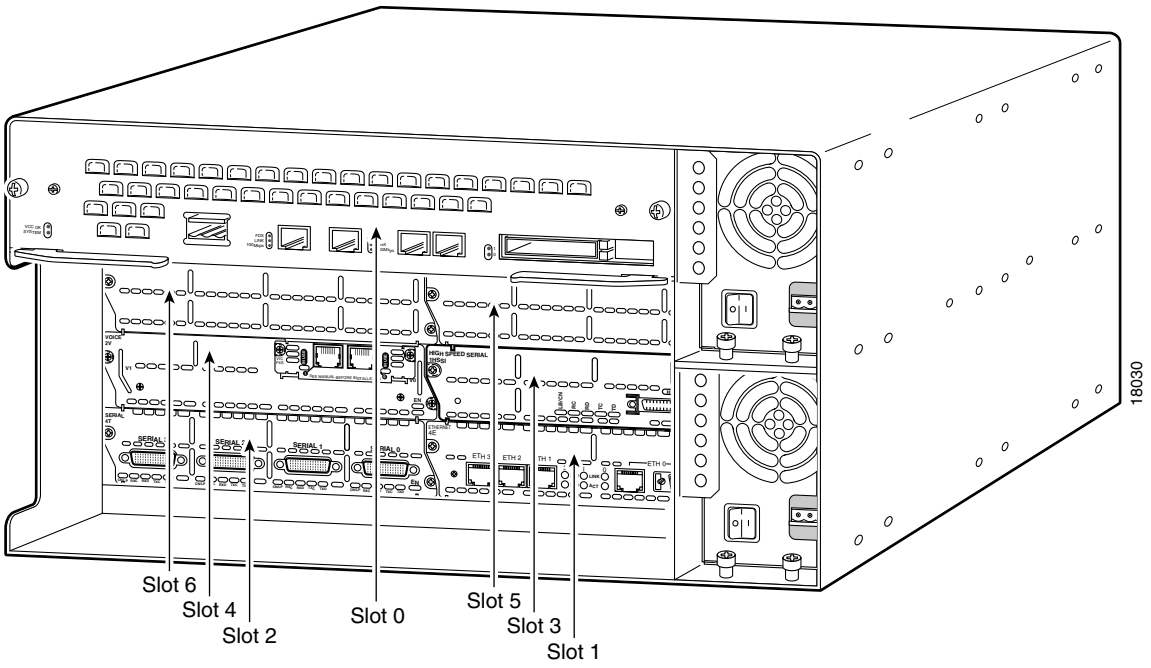
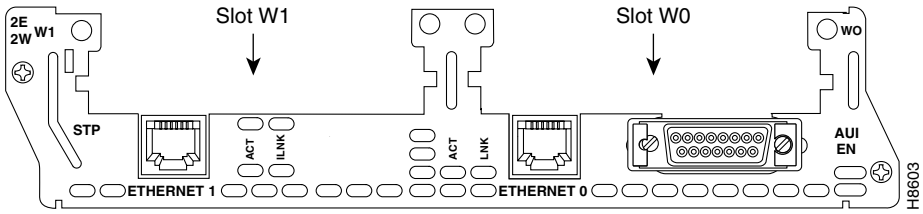



*Figure 1-3 Interface or Line Card Slots*




Additional attributes representing line card type and sub-devices 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.cns.config.device-details* event after hardware discovery. The Cisco CNS Configuration Engine 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 all three modes (see "NSM Modes" section on page 1-4).

# 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 1-5), 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 5-1.

# 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 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 to recognize 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 {hostname:cns_password} over the encrypted pipe. The device uses a CNS password to be authenticated by the Cisco CNS Configuration Engine.

**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.

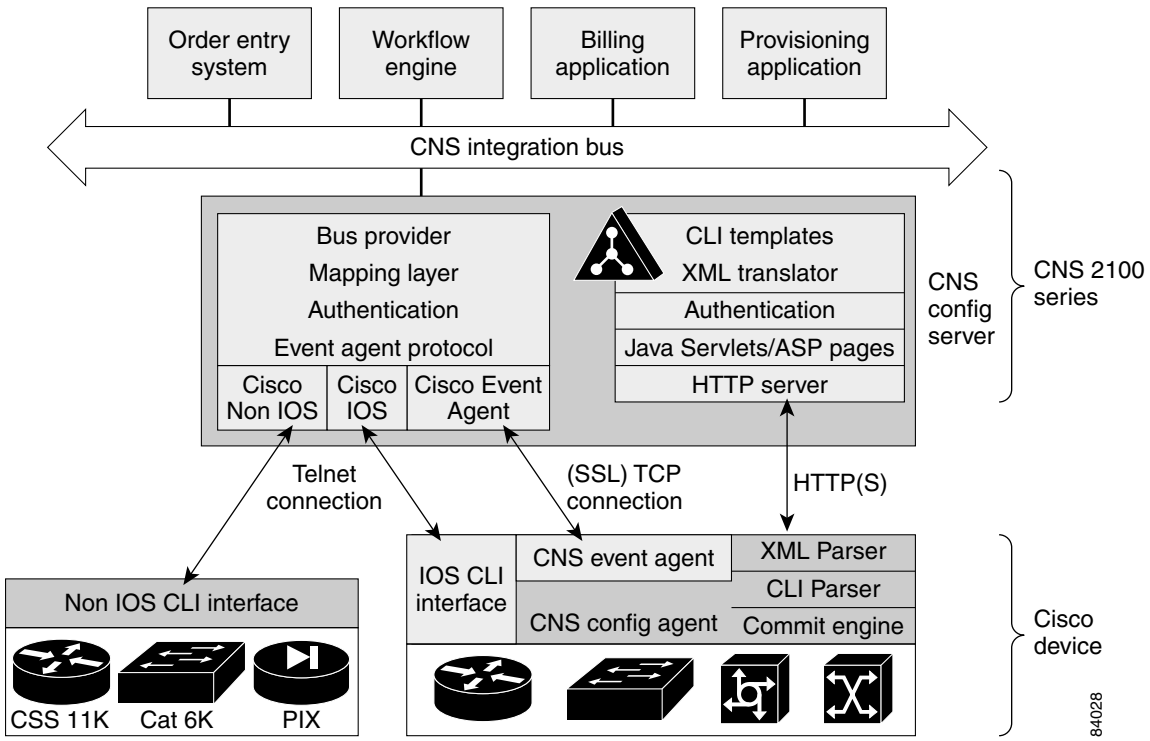
Once the server is secured, it is no longer be able to process requests that do not have a password. It cannot tell the difference between a clear-text request from a device in a secure environment from a device in an non-secure environment.

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 {hostname: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.

# How the Cisco CNS Configuration Engine Works

The Cisco CNS Configuration Engine 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 1-10). This takes place in response to a *pull* (get) operation.

***Figure 1-4 Configuration Registrar Functional Diagram***

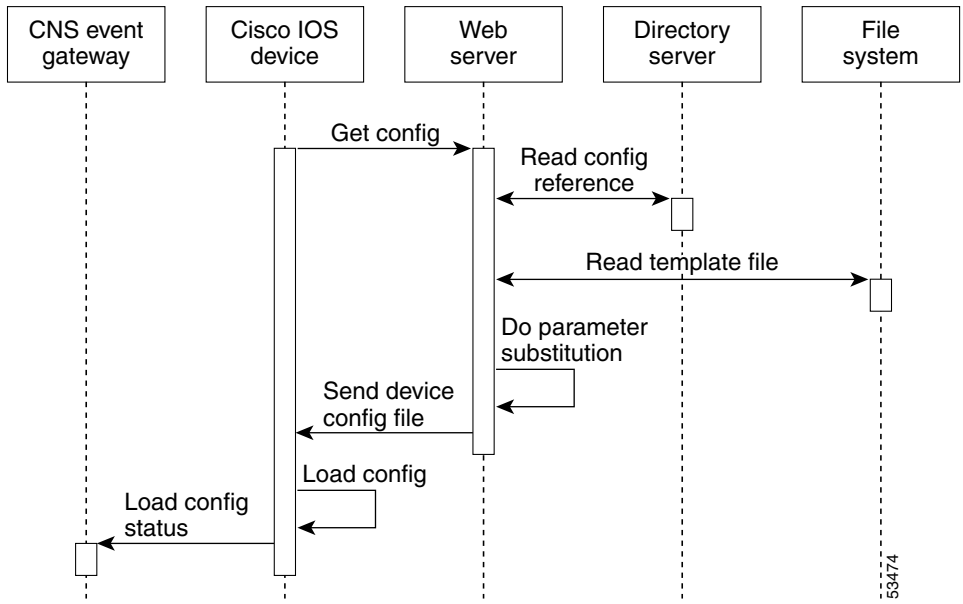



A Cisco IOS device initiates a get operation when it first appears on the network (**cns config init…**) or when notified (by subscribed event) of a configuration update (**cns config partial…**).

**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 reads the template files.
2. The Cisco CNS Configuration Engine does the parameter substitution.
3. The Cisco CNS Configuration Engine 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 for the initial configuration.
2. The Cisco CNS Configuration Engine 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 reads the template files.
4. The Cisco CNS Configuration Engine does the parameter substitution.

5. The Cisco CNS Configuration Engine 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 user interface.
2. The template contents are passed to the Cisco CNS Configuration Engine.
3. The Cisco CNS Configuration Engine 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 publishes a *cisco.cns.config.load* event.
6. The Cisco IOS device retrieves the *cisco.cns.config.load* event.
7. The Cisco CNS Configuration Engine reads the template files.
8. The Cisco CNS Configuration Engine does the parameter substitution.
9. The Cisco CNS Configuration Engine 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 user interface.
2. The template contents are passed to the Cisco CNS Configuration Engine.
3. The Cisco CNS Configuration Engine 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 publishes a *cisco.cns.config.load* event.
6. The modular router retrieves the *cisco.cns.config.load* event.
7. The Cisco IOS device posts a HTTP request containing the hardware configuration to the Cisco CNS Configuration Engine for the partial configuration.
8. The Cisco CNS Configuration Engine reads the template files.
9. The Cisco CNS Configuration Engine does the parameter substitution.
10. The Cisco CNS Configuration Engine 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 intersects two name spaces, one for the event bus and the other for the configuration server. One is used when a device communicates with the Cisco CNS Configuration Engine using the HTTP protocol. The other one is used when the device communicates with the Cisco CNS Configuration Engine using the publish and subscribe mechanism of the CNS Integration Bus (event bus).

The device must be uniquely identified in these namespaces. The ConfigID uniquely identifies the device in the HTTP domain. The EventID uniquely identifies the device in the CNS event domain.

Because the Cisco CNS Configuration Engine uses both the 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 "How to Manage Devices" section on page 3-10).

# Dynamic ConfigID and EventID Change Synchronization

The Cisco IOS, version 12.2.10T, has been enhanced with new CLI ID commands that can modify the EventID and ConfigID, then reconnect the device to the Cisco CNS Configuration Engine with the new IDs. For example, a device is connected to the Event Gateway with a hostname, say *XYZ*.

The gateway has created a listener for device on events coming on the subscribed subject, say **cisco.cns.config.load.xyz**. There is an entry for this device in the Cisco CNS Configuration Engine directory with attributes, such as IOSEventID and IOSConfigID.

The Cisco CNS Configuration Engine uses IOSEventID to send events to the device. The Cisco CNS Configuration Engine uses IOSConfigID when the device sends an **http get** request to the Cisco CNS Configuration Engine or its configuration template.

If the hostname of the device is changed to, say *ABC*, then the device publishes events **cisco.cns.config.id-changed** and **cisco.cns.event.id-changed** to the Event Gateway. The gateway goes to the directory and fetches the publisher mapping for this subject in the application associated with the group to which the device belongs. The configuration server updates the IOSEventID and IOSConfigID attributes.

# 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, see "Initializing Tivoli Management Agent" section on page 2-27.

CHAPTER 2

# Installing the Software and Configuring the Cisco CNS 2100 Series Intelligence Engine

This chapter describes how to install the Cisco CNS Configuration Engine 1.3 software and configure the Cisco CNS 2100 Series Intelligence Engine.

## Installing the Software

The Cisco CNS Configuration Engine 1.3 software is contained on a CD-ROM that is in the accessory kit.

To be able to monitor the installation activity, you should have a local keyboard-mouse and a VGA screen to your system C2T (out) port using a K/M/V (keyboard, mouse, VGA cable (IBM P/N 00N6954).

To install the software, follow these steps:

**Step 1** Verify that the CNS 2100 Series system is powered down.

**Step 2** Power on the system and quickly insert the Cisco CNS Configuration Engine 1.3 CD-ROM in the CD drive.

**Step 3** Push the **Reset** button to restart the system from the CD-ROM.

The software installs automatically. When the install sequence completes, the system automatically ejects the CD-ROM and restarts into Linux from the hard drive.

**Step 4** Go to Running the Setup Program to run the **Setup** program.

## Running the Setup Program

You must run the **Setup** program when you start the system for the first time.

You must connect to the system using the serial port to use the **Setup** program. The parameters for using the serial port are 9600-N-8-1. Alternatively, you can connect a VGA monitor to the CNS 2100 Series.

If this is the first time running **Setup**, or you have just run **reinitialize** or **relocate**, you cannot connect to the system using Telnet. Telnet is only possible if the network interfaces are configured.

To run **Setup**, follow these steps:

**Step 1** Start the system.

When the system finishes the startup routine, a login prompt appears.

**Step 2** Log in with username **setup**.

The **Setup** program starts.

**Step 3** Enter responses to the prompts that appear.

For information about valid values for each parameter, see Table 2-1 on page 2-5 through Table 2-9 on page 2-14.

Use the following conventions when running the **Setup** program:

- Press **Enter** to enter a response and proceed to the next prompt.

  After you enter a response, you cannot edit it again. To change an entered response you must exit the **Setup** program and enter your responses again. You can exit the **Setup** program in two ways:

  – Press **Ctrl-c**.

    The login prompt appears. Use the login **setup** to run the **Setup** program.

  – Enter **n** at the final prompt, Committed changes: [y/n].

    The **Setup** program exits without saving the configuration, then restarts.

- Press **Backspace** or **Delete** to delete characters.

**Step 4** Provide values where prompted.

For an example of the Internal Directory mode prompts, see "Internal Directory Mode Setup Prompts"on this page.

For an example of the External Directory mode prompts, see "External Directory Mode Setup Prompts" section on page 2-10.

**Step 5** Review your **Setup** configuration.

**Step 6** To commit (save) your changes, type **y**.

After you save the configuration, the shell prompt appears.

# How to Re-execute Setup

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. To re-execute **Setup**, login as root, then enter the **setup** command in the shell prompt.

# Internal Directory Mode Setup Prompts

The following sample shows the standard set of prompts for Internal Directory mode:

```
Entering Network Appliance Setup
Type ctrl-c to exit

       For detail information about the parameters in this setup, refer to "Cisco
```

```
        Intelligence Engine 2100 Series Configuration Engine Administrator's Guide".

Interactive or non-interactive setup? 0=interactive, 1=non-interactive. 0

        Note: Modular router support is available only in internal directory mode.

Choose operational mode of system. 0=internal directory mode, 1=external directory mode. 0

        Please enter the password you would like to use as the root password for the
        IE2100. Warning: If you lose this password, the root account will be locked out
        of maintaining the IE2100.

Enter root password: ******
Re-enter root password: ******
Enter hostname: rain
Enter domain name: cisco.com

        User-level shell account for IE2100 has read-only monitoring and troubleshooting.
        However, no configuration changes are possible with this account.

Enter username for user-level shell account: admin
Enter password for user-level shell account: *****
Re-enter password for user-level shell account: *****

        You must configure eth0 or eth1. Press <Enter> to skip!

Enter eth0 IP address: 10.1.19.12
Enter eth0 network mask: 255.255.255.0
Enter eth0 default gateway IP address: 10.1.19.6
Enter eth1 IP address:
Enter primary DNS server IP address: 171.68.226.120
Enter secondary DNS server IP address (optional):
Enter country code: us
Enter company code: cisco

        Configuration Engine user ID is used to log in to the web-based GUI and manage
        network device objects and templates. This account does NOT have shell access.

Enter Configuration Engine login name: admin
Enter Configuration Engine login password: *****
Re-enter Configuration Engine login password: *****
Enter internal LDAP server password: *****
Re-enter internal LDAP server password: *****

Encryption settings:
------------------------

Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s) (y/n)?
[y]
Certificates already exist. Overwrite (y/n)? [y]
Enter certificate FTP server (hostname.domainname or IP address): [ringer]
Enter username used for FTP server: [anrichar]
Enter FTP password: [********]
Re-enter FTP password: [********]
Enter absolute pathname of remote key file: [/users/anrichar/cert/server.key]
Enter absolute pathname of remote certificate file: [/users/anrichar/cert/server.crt]

        Enabling plaintext operation will increase security risk.

Enable plaintext between Config Server and devices/GUI administration (y/n)? [n] y
Enable plaintext operation between Event Gateway and devices (y/n)? [n] y

Authentication settings:
-----------------------------
```

```
        IOS Devices are normally authenticated before being allowed to connect to the
        Event Gateway/Config Server. Disabling authentication will increase security risk.

Enable authentication (y/n)? [n] y

Event services settings:
----------------------------

Enter NSM directive (none, default, http): [default]
Enable Event Gateway debug log (y/n)? [n]

        Each Event Gateway process serves 500 devices. Maximum number of Event Gateways
        allowed is 11.

Enter number of Event Gateways that will be started with crypto operation: 10
Enter number of Event Gateways that will be started with plaintext operation: [0]1

Enter CNS event bus network parameter: [rain]
Enter CNS event bus service parameter: [7500]

Current settings for IMGW:
--------------------------------

Gateway ID: rain
Run as daemon (y/n)? y
Timeout in seconds for entire Telnet operation to complete: 180
Timeout in seconds between prompts during Telnet session: 60
Concurrent Telnet session limit: 100
Remove temporary logs of Telnet sessions into devices (y/n)? y
Location of temporary logs of Telnet sessions into devices: /tmp
Hoptest success retry interval (sec): 7200
Hoptest failure retry interval (sec): 3600
Logging level (verbose, error, silent): error
Log file prefix: IMGW-LOG
Log file size (bytes): 50331648
Log file rotation timer (minutes): 60
Logging mode (append, overwrite): append

Re-configure IMGW (y/n)? [n]
```

## Parameter Descriptions

**Interactive or non-interactive setup**: In interactive setup, you set up the appliance by entering all configuration inputs manually. In non-interactive setup, you download a configuration file that can be run and set up the box automatically.

**Internal/external directory mode**: Internal Directory mode uses the embedded directory service. External Directory mode uses an external directory service.

**Root password**: This is the password for logging into the root-user account of Linux. **Setup** prompts you to redefine the root password whenever it detects that the root password is set to the factory default **blender**. Later, you can change root password using the Linux password command **passwd**.

**Hostname**: The name of the CNS 2100 Series system.

**Domain name**: The name of the domain in which the CNS 2100 Series system exists.

**Username/password for user-level shell account**: This is the username-password pair to be created in Linux for administrative purpose. This account does not have root privileges.

**Eth0/Eth1 IP address/network mask**: IP address and network mask of the system. You can configure one or both Ethernet card(s) for network connectivity.

**Default gateway IP address**: This is the gateway IP address that makes up the default route in the routing table.

**Primary/secondary DNS server IP address**: This is the server that provides domain-name to IP address translation service. Only the first one is required. The second one is optional.

**Country/company code**: These are the information used to define the internal storage structure of DCL.

**Configuration Engine login name/password**: Defines the administrator account and password for accessing the configuration server user interface.

**Enter internal LDAP server password**: Defines internal-directory-account password for the two internal administrative users: **dcdadmin** and **cdauser1**.

*Table 2-1 Valid Values for General Parameters*

| Parameter | Type | Length |
|---|---|---|
| Interactive or non-interactive setup? | 0=interactive, 1=non-interactive | |
| Choose operational mode of system. | 0=internal directory mode, 1=external directory mode | |
| Root password | Password | 6—12 |
| Hostname | Alphanumeric, dash | 1—32 |
| Domain name | Alphanumeric, dash, dot | 1—unlimited |
| User-level shell account | Alphanumeric, dash | 1—32 |
| User-level shell account password | Password | 6—12 |
| [eth0/eth1] IP address | IP address | |
| [eth0/eth1] Network mask | Network mask | |
| [eth0/eth1] Default gateway ip address | Gateway IP | |
| [Primary/Secondary] DNS server IP address | IP address | |
| Country code | Country Code | |
| Company code | Alphanumeric, dash | 1—80 |
| Configuration Engine login name | Alphanumeric, dash | 1—30 |
| Configuration Engine login password | Password | 1—12 |
| Internal LDAP server password | Password | 1—20 |

- Alphanumeric type refers to alphabetic and numeric characters plus the underscore "_" symbol**.**
- Password type refers to ASCII characters that are between the octal values 040 (space) and 176 ("~") inclusive.
- IP address must be entered in the format **a.b.c.d**, where a, b, c, and d are decimal values from 0 to 255. IP address must pass four more checks:
  - It cannot be a class D (multi-class 0xE0 00 00 00) address.
  - It cannot be in class A network zero (0x00 00 00 00).
  - It cannot be in class A network 127 (0x7F 00 00 00).
  - It must be either a class A, B, or C address.
- Network mask refers to a valid IP address that obeys the following rules:

  - Network mask must be composed of contiguous 1s.
  - It cannot be 0x00000000 or 0xFFFFFFFF.
  - When applying to the host IP address, the host address cannot be a subnet broadcast address; for example, all ones or zeros in the IP host portion.
- A Gateway IP address is a valid IP address and must be in the same subnet as the host.
- Country code refers to ISO two-letter codes for country identification (ISO 3166). There are 241 of them. See Appendix B, "Country Codes" for a list of the valid country codes.

## Encryption Settings

**Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s) (y/n)**: This option enables crypto (SSL) operation. The web server listens on TCP port 443, and responds to https requests (https://machine/config/login.html). The event gateway listens to ports 11012, 11014, and so on (depending on the number started).

All data between the IE2110 and the far end are encrypted. The SSL protocol (combined with valid certificates) ensures that the IE2110 is authenticated by the far end. In order to complete SSL configuration, valid certificates need to be placed on the IE2110 (see "Configuring SSL Certificates" section on page 2-17).

If disabling crypto operation, the remaining prompts in this section are omitted.

**Certificates already exist, Overwrite (y/n)**: If a certificate already exists, choose whether to download and overwrite the existing one. If there is no certificate initially on the system, this prompt is disabled.

**Certificate FTP server**: Specifies the location of the FTP server for downloading the certificate. Input can either be an IP address or in the form of *hostname.domain*. For the latter case, the DNS entered earlier is used for the *hostname.domain*-to-IP address resolution.

**Username/password for FTP server**: Specifies the login name and password for accessing the FTP server.

**Absolute pathname of remote key file and certificate file**: Specifies the locations of the key and certificate files on the FTP server.

**Enable plaintext between Config Server and devices/GUI administration (y/n)**: This option enables plaintext configuration server operation. In addition to listening on TCP port 443 for crypto connection (https://machine/config/login.html), the web server also listens on TCP port 80 for plaintext connection, responding to **http** requests (http://machine/config/login.html).

**Note** If crypto is disabled, plaintext between the configuration server and devices and operators is enabled.

**Enable plaintext operation between Event Gateway and devices (y/n):** This prompt enables/disables the prompt: number of Event Gateways that will be started with plaintext operation, which appears under Event service settings.

*Table 2-2 Valid Values for Encryption Parameters*

| Parameter | Type | Length |
|---|---|---|
| Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s) | y, n | |
| Certificate ftp server | IP address or<br>hostname.domainname | <br>1—63 |

*Table 2-2 Valid Values for Encryption Parameters (continued)*

| Parameter | Type | Length |
|---|---|---|
| Username used for ftp server | Alphanumeric,dash | 1—32 |
| FTP password | Password | 1—20 |
| Absolute pathname of remote key file | Alphanumeric, dash, slash | 1—255 |
| Absolute pathname of remote certificate file | Alphanumeric, dash, slash | 1—255 |
| Enable plaintext between Config Server and devices/operators | y, n | |
| Enable plaintext operation between Event Gateway and devices | y, n | |

### Authentication settings

**Enable Authentication (y/n)**: Enables Cisco IOS device authentication mechanism within the IE2110.

**Note** If bypassing device authentication, connection to devices with a Cisco IOS release earlier than 12.2(11)T is implicitly allowed. There is a security risk associated with disabling authentication.

*Table 2-3 Valid Values for Authentication Parameters*

| Parameter | Type | Length |
|---|---|---|
| Enable authentication | y, n | |

### Event Service Settings

**NSM directive**: Defines NameSpace Mapper mapping modes. Valid modes are **http**, **none**, and **default** (see "NSM Modes" section on page 1-4). If input to NSM directive is **http**, you must answer the **Event Gateway application parameters** prompt (see "Setting NSM Directive to http" section on page 2-8).

**Event Gateway debug log**: Turns on Event Gateway debug logging.

**Number of Event Gateways that will be started with crypto operation**: Specifies the number of Event Gateway processes that should be started in crypto mode (the number of Event Gateways that communicate with devices using SSL). If crypto operation is disabled, this prompt is also disabled.

**Number of Event Gateways that will be started with plaintext operation**: Specifies the number of Event Gateway processes that should be started in plaintext mode (the number of Event Gateway that communicate with devices without using SSL). The total number of Event Gateways, whether it is started for crypto operation or not, should not exceed 11.

**CNS Event Bus Network Parameter**: Specifies the outbound network interface of CNS 2100 Series for publishing events. It can be an IP address, the name of the local network interface, a hostname, or multicast address.

**CNS Event Bus Service Parameter**: Specifies the ports used for publishing and listening to events.

**Timesaver** Dedicating a port for the communication between an CNS 2100 Series and its managing devices can reduce traffic caused by listening to other unrelated events

**Re-configure IMGW**: This **y/n** prompt determines whether setup should display the section of prompts for re-configuring IMGW related parameters. Regular users should always answer **n**.

*Table 2-4 Valid Values for Event Service Parameters*

| Parameter | Type | Length |
|---|---|---|
| NSM directive | none, default, http | |
| Event Gateway debug log | y, n | |
| Number of Event Gateways that will be started with crypto operation | Range from 1 to 11 | |
| Number of Event Gateways that will be started with plaintext operation | Range from 0 to 11 (number of event gateways started with crypto) if crypto is enabled.<br>Range from 1 to 11 if crypto is disabled. | |
| CNS event bus network parameter | Network parameter | |
| CNS event service parameter | Range from 0 to 65535 | |
| Re-configure IMGW | y, n | |

- Valid inputs for the network parameter consists of up to three parts, separated by semicolons—network, multicast groups, and send address—as in these examples:

```
eth0                                    network only
eth0;224.1.1.1                          one multicast group
eth0;224.1.1.1,224.1.1.5;224.1.1.6      two multicast groups, send address
```

  - **Part One—Network:** Identifies the network, which you can specify in several ways: Host name, Host IP address, Network name (where supported), Network IP number, or Interface name (where supported; for example, **eth0**).
  - **Part Two—Multicast Groups:** A list of zero or more multicast groups specified as IP addresses, separated by commas. Each address in part two must denote a valid multicast address.
  - **Part Three—Send Address:** A single send address. If present, this item must be an IP address, not a hostname or network name.

## Setting NSM Directive to http

The previous prompt example has NSM directive set to **default**. When the NSM directive is set to **http**, you are prompted for an additional namespace parameter, Enter Event Gateway application parameter(s) for NSM:

```
Enter NSM directive (none, default, http): [default] http
Enter Event Gateway application parameter(s) for NSM: [config]
```

The new prompt definition and input format is as follows:

**Event Gateway application parameter(s) for NSM**: Specifies the application namespace to be used in NameSpace Mapper for resolving mapping. The default namespace used is **config**.

*Table 2-5 Valid Values for NSM Directive Parameter*

| Parameter | Type | Length |
|---|---|---|
| Event Gateway application parameters | Alphanumeric, dash, space | 1—unlimited |

## Re-configure IMGW Parameters

This section shows the set of prompts required for re-configuring the IMGW settings.

```
Re-configure IMGW (y/n)? [n] y
Enter Gateway ID: [rain]
Run as daemon (y/n)? [y]
Enter timeout in seconds for a CLI command to complete: [180]
Enter timeout in seconds to get the next prompt in Telnet session: [60]
Enter concurrent Telnet session limit: [100]
Remove temporary logs of Telnet sessions into devices (y/n)? [y]
Enter location of temporary logs of Telnet sessions into devices: [/tmp]
Enter hoptest success retry interval (sec): [7200]
Enter hoptest failure retry interval (sec): [3600]
Enter logging level (verbose, error, silent): [error]
Enter log file prefix: [IMGW-LOG]
Enter log file size (bytes): [50331648]
Enter log file rotation timer (minutes): [60]
Enter logging mode (append, overwrite): [append]
```

### Parameter Descriptions

**Gateway ID**: Unique identifier assigned to the IMGW process. It is always set to hostname by default.

**Run as daemon**: Set to **y** for normal use. **n** is only used for debugging purpose.

**Timeout in seconds for a CLI command to complete**: The maximum waiting time in seconds for a CLI to complete.

**Timeout in seconds to get the next prompt in Telnet session:** The maximum waiting time in seconds to get the next prompt in Telnet session.

**Concurrent Telnet session limit:** The maximum simultaneous Telnet connections that IMGW supports.

**Remove temporary logs of Telnet sessions into devices**: The y/n value that determines if IMGW should remove the temporary files it creates for download/exec.

**Location of temporary logs of Telnet sessions into devices**: File system location where IMGW should create the temporary files.

**Hoptest success retry interval:** Time interval in minutes for IMGW to check device in the Success list (devices for which connectivity-check succeeded).

**Hoptest failure retry interval**: Time interval in minutes for IMGW to check device in the Failure list (devices for which connectivity-check failed).

**Logging level:** Verbose mode logs both error and debugging messages. Error mode logs only error messages. Silent mode does not log any message.

**Log file prefix:** A prefix used to construct the name of the log file. The resulting filename is made up of the prefix and the IMGW gateway ID.

**Log file size**: Log file size that triggers log rotation.

**Log file rotation timer**: Time in seconds after which to check log-file size for log rotation.

**Logging mode**: Select whether to append new log to the end of the log file or overwrite the previous log.

*Table 2-6 Valid Values for IMGW Parameters*

| Parameter | Type | Length |
|---|---|---|
| Gateway ID | Alphanumeric, dash | 1—32 |
| Run as daemon | y, n | |
| Timeout in seconds for a CLI command to complete | Range from 30 to 7200 | |
| Timeout in seconds to get the next prompt in Telnet session | Range from 30 to 7200 | |
| Concurrent Telnet Session Limit | Six digits numeric 0 to 999999 | |
| Remove temporary logs of Telnet sessions into devices | y, n | |
| Location of temporary logs of Telnet sessions into devices | Alphanumeric, dash, slash | 1—255 |
| Hoptest success retry interval (sec) | Range from 0 to 2147483647 | |
| Hoptest failure retry interval (sec) | Range from 0 to 2147483647 | |
| Logging level | verbose, error, silent | |
| Log file prefix | Alphanumeric, dash | 1—32 |
| Log file size (bytes) | Range from 5242880 to 4294967295 | |
| Log file rotation timer (minutes) | Range from 0 to 2147483647 | |
| Logging mode | append, overwrite | |

# External Directory Mode Setup Prompts

Most of the prompts in External Directory mode are identical to those for the Internal Directory mode except for the introduction of the External Directory mode settings and sample schema.

In the External Directory mode, the system is configured to contact the external directory storage for device information. Certain information that makes up the schema of the external directory such as attribute names (in the device class) and container locations must be entered during **Setup**.

To simplify the inputs, you can choose to use the predefined sample schema and construct your external directory accordingly.

The sample shows the prompts for External Directory mode where the sample schema is enabled.

```
Entering Network Appliance Setup
Type ctrl-c to exit

        For detail information about the parameters in this setup, refer to "Cisco
        Intelligence Engine 2100 Series Configuration Registrar Administrator's Guide".

Interactive or non-interactive setup? 0=interactive, 1=non-interactive. 0

        Note: Modular router support is available only in internal directory mode.

Choose operational mode of system. 0=internal directory mode, 1=external directory mode. 1

        Please enter the password you would like to use as the root password for the
        IE2100. Warning: If you lose this password, the root account will be locked out
```

```
       of maintaining the IE2100.

Enter root password: ******
Re-enter root password: ******
Enter the hostname: rain
Enter the domain name: cisco.com

       User-level shell account for IE2100 has read-only monitoring and troubleshooting.
       However, no configuration changes are possible with this account.

Enter username for user-level shell account: admin
Enter password for user-level shell account: *****
Re-enter password for user-level shell account: *****

       You must configure eth0 or eth1. Press <Enter> to skip!

Enter eth0 IP address: 10.1.19.12
Enter eth0 network mask: 255.255.255.0
Enter eth0 default gateway IP address: 10.1.19.6
Enter eth1 IP address:
Enter primary DNS server IP address: 171.68.226.120
Enter secondary DNS server IP address (optional):
Enter country code: us
Enter company code: cisco

Encryption settings:
------------------------

Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s) (y/n)?
[y]
Certificates already exist. Overwrite (y/n)? [y]
Enter certificate FTP server (hostname.domainname or IP address): [ringer]
Enter username used for FTP server: [anrichar]
Enter FTP password: [********]
Re-enter FTP password: [********]
Enter absolute pathname of remote key file: [/users/anrichar/cert/server.key]
Enter absolute pathname of remote certificate file: [/users/anrichar/cert/server.crt]

       Enabling plaintext operation will increase security risk.

Enable plaintext operation between Config Server and devices/GUI administration (y/n)? [n]
y
Enable plaintext operation between Event Gateway and devices (y/n)? [n] y

Authentication settings:
------------------------------

       IOS Devices are normally authenticated before being allowed to connect to the
       Event Gateway/Config Server. Disabling authentication will increase security risk.

Enable authentication (y/n)? [n] y

Event services settings:
----------------------------

Enter NSM directives (none, default, http): [default]
Enable Event Gateway debug log (y/n): [n]

Each Event Gateway process serves 500 devices. Maximum number of Event Gateways allowed is
11.

Enter number of Event Gateways that will be started with crypto operation: 10
Enter number of Event Gateways that will be started with plaintext operation: [0]1
```

```
Enter CNS event bus network parameter: [rain]
Enter CNS event bus service parameter: [7500]

External directory settings:
--------------------------------

Enter IP address of remote directory server: 10.10.18.7
Enter port number of remote directory server: 389
Enter external directory server login name: admin
Enter external directory server password: *****
Re-enter external directory password: *****
Enter User DN: cn=admin,o=butterfly
Enter CNS context: ou=cns,o=butterfly
Use sample schema (y/n): [y]

Current settings of IMGW:
--------------------------------
Gateway ID: rain
Run as daemon (y/n)? y
Timeout in seconds for a CLI command to complete: 180
Timeout in seconds to get the next prompt in Telnet session: 60
Concurrent Telnet session limit: 100
Remove temporary logs of Telnet sessions into devices (y/n)? y
Location of temporary logs of Telnet sessions into devices: /tmp
Hoptest success retry interval (sec): 7200
Hoptest failure retry interval (sec): 3600
Logging level (verbose, error, silent): error
Log file prefix: IMGW-LOG
Log file size (bytes): 50331648
Log file rotation timer (minutes): 60
Logging mode (append, overwrite): append

Re-configure IMGW (y/n)? [n]
```

## Parameter Descriptions

These parameter descriptions are for those parameters unique to the External Directory mode. The general parameter descriptions for the sample above (common to both modes) are listed beginning with "Parameter Descriptions" section on page 2-4.

**IP address of remote directory server**: The location of the external directory expressed as IP address.

**Port number of remote directory server**: The service port number of the external directory.

**Remote directory server login name**: Directory user that has the administrative privileges for all objects under CNS context; for example, **admin**.

**Remote directory server password**: Directory user password. This same password is also used to define the passwords of two internal administrative accounts (**dcdadmin** and **cdauser1**) of the internal directory storage.

**User DN**: The complete distinguished name for the remote directory administrative user.

**CNS context**: Directory context (DN) under which all CNS objects are created. This includes device objects, group objects, application objects, and event objects. These objects can be created inside containers under CNS context.

**Use sample schema**: Select **y** for enabling the predefined sample schema and **n** for otherwise. See "Sample Schema" for the definition and default values of sample schema.

*Table 2-7 Valid Values for General External Directory Mode Parameters*

| Parameter | Type | Length |
|---|---|---|
| IP address of the remote Directory Server | IP address | |
| Port number of the remote Directory Server | Range between 0 to 65535 | |
| Remote directory server login name | Alphanumeric,dash | 1—32 |
| Remote directory server password | Alphanumeric,dash | 1—20 |
| User DN | Name-value pair with space | 3—unlimited |
| CNS context | Name-value pair with space | 3—unlimited |

## Sample Schema

Table 2-8 lists the parameters and default values that define the sample schema:

*Table 2-8 Sample Schema Parameters*

| Prompt | Value |
|---|---|
| objectclass for device object: | deviceclass |
| container name under which device objects are stored: | ou=CNSDevices |
| container name under which group objects are stored: | ou=CNSGroups |
| container name under which application objects are stored: | ou=CNSApplications |
| template attribute name in device objectclass: | IOSconfigtemplate |
| config id attribute name in device objectclass: | IOSConfigID |
| event id attribute name in device objectclass: | IOSEventID |
| CNS group attribute in device objectclass: | parent |
| CNS password attribute name in the device object class: | AuthPassword |
| objectclass for bootstrap password object: | CNSBootstrapPwdClass |
| bootstrap password attribute name in bootstrap password objectclass: | CNSBootPassword |

This sample shows the schema prompts that need to be answered when sample schema is disabled:

```
Use sample schema (y/n): n
Enter container name under which device objects are stored: [ou=CNSDevices]
Enter container name under which group objects are stored: [ou=CNSGroups]
Enter container name under which application objects are stored: [ou=CNSApplications]
Enter objectclass for device object: [deviceclass]
Enter template attribute name in device objectclass: [IOSconfigtemplate]
Enter config id attribute name in device objectclass: [IOSConfigID]
Enter event id attribute name in device objectclass: [IOSEventID]
Enter CNS group attribute name in device: [parent]
Enter CNS password attribute name in device object class: [AuthPassword]
Enter objectclass for bootstrap password object: [CNSBootstrapPwdClass]
Enter bootstrap password attribute name in bootstrap password objectclass:
[CNSBootPassword]
```

## Parameter Descriptions

**Device objects container name:** The container in the directory under which device objects are created.

**Groups objects container name:** The container in the directory under which group objects are created.

**Application objects container name:** The container in the directory under which application objects are created.

**Object class:** The name of the user defined object class for device object.

**Template attribute name:** Attribute of the device class (as specified in the Object-class prompt) that specifies the template file for the device object. This is not the template file itself, just the name of the attribute that has the value of the template filename.

**Config ID attribute name:** Attribute of the device class that uniquely identifies the device in the config-server domain.

**Event ID attribute name:** Attribute of the device class that uniquely identifies a device within the Event Gateway server.

**CNS group attribute:** The attribute of the device class that specifies the group(s) to which the device object belongs. Note that this is only an attribute name, but not the groups themselves. In addition, it is required only when NSM directive is set to http mode.

**CNS password attribute name in device object class**: The attribute of the device class that stores the value that the CNS 2100 Series expects as the CNS password from the Cisco IOS device. If disabling authentication, this prompt is disabled.

**objectclass for bootstrap password object**: The name of the user defined object class for the bootstrap password object. If disabling authentication, this prompt is disabled.

**Bootstrap password attribute name in bootstrap password object class**: The attribute of the bootstrap password class that stores the value that the CNS 2100 Series system uses as the bootstrap password. If disabling authentication, this prompt is disabled.

*Table 2-9 Valid Values for Sample Schema Parameters*

| Parameter | Type | Length |
|---|---|---|
| Device container name | Name-value pair with space | 3—unlimited |
| Group container name | Name-value pair with space | 3—unlimited |
| Application container name | Name-value pair with space | 3—unlimited |
| Object class | Alphanumeric,dash | 1—80 |
| Template attribute name | Alphanumeric,dash | 1—80 |
| Device IP address attribute name | Alphanumeric,dash | 1—80 |
| Config ID attribute name | Alphanumeric,dash | 1—80 |
| Device ID attribute name | Alphanumeric,dash | 1—80 |
| Event ID attribute name | Alphanumeric,dash | 1—80 |
| CNS group attribute | Alphanumeric,dash | 1—80 |
| CNS password attribute name | Alphanumeric,dash | 1—80 |
| Container name under which bootstrap password object is stored | Alphanumeric,dash | 1—80 |
| Bootstrap password attribute name | Alphanumeric,dash | 1—80 |

# Non-Interactive Setup

For non-interactive **Setup**, a Perl script for setting up CNS 2100 Series must be created and stored on a remote FTP server.

## Sample Scripts

Two sample scripts are provided for non-interactive mode. They are *internaldir.pl* used for internal-directory mode and *externaldir.pl* for external-directory mode. They are installed in the directory */opt/CSCOcnsie/bin* of CNS 2100 Series. They can be used as a template for crafting a specific setup.

The sample scripts are basically setup scripts without prompts; in other words, a non-interactive setup script. All required inputs are hard-coded in the variable initialization section. For ease of identification, associated prompts are listed as comments before each variable assignment.

Upon receiving the non-interactive setup script, it is executed and performs the followings:

1. Read in previously stored inputs from */opt/CSCOcnsie/bin/varsetup.dat*, if already exists, as default values.
2. Go through the variable initialization section and override default values.
3. Execute the remaining setup procedures that are carried out after prompting in interactive setup.

## General Guidelines

Here are some general guidelines for the non-interactive **Setup**:

- Variable inputs are not validated.
- Variable **$rainmaker_mode_flag** must be set to **0** for internal directory mode and **1** for external directory mode.
- All password variables can be assigned a plaintext password or an encrypted password. If encrypted password is required, it should be generated using the shell command **encrypt** and passed as a function argument to the decrypt function **do_decrypt**. For example, root password variable **$rootpassword** can be set to **blender** as follows:

  ```
  $rootpassword="blender";
  ```

  or

  ```
  $rootpassword=do_decrypt("52616e646f6d49565b909053af1db595ca8823f2ddf29317");
  ```

  where the encrypted password is generated as follows:

  ```
  [root@rain106 /root]# encrypt blender
  52616e646f6d49565b909053af1db595ca8823f2ddf29317
  [root@rain106 /root]#
  ```

  **encrypt** is a Perl script that takes a plaintext string input from **stdin** and generates the associated, encrypted string at **stdout**.

**Note** The encryption key used by **encrypt** is erased after each **reinitialize** and a new one is generated when **encrypt** or **setup** is run. Accordingly, all encrypted passwords in the non-interactive setup scripts must be re-generated after each **reinitialize**.

- The value of **$rootpassword** is used to re-define the root password only if the password is formerly set to **blender** (the factory default); otherwise, the value would be ignored.
- Variables **$hostname**, **$domain_name**, **$dcl_country_code**, and **$dcl_company_code** cannot be changed in subsequent **Setup**. These parameters can only be changed after running **reinitialize**.
- Ethernet IP address, either Ethernet eth0 (**$eth0_ip**, **$eth0_network_mask**, **$eth0_gateway_ip**) or eth1 (**$eth1_ip**, **$eth1_network_mask**, **$eth1_gateway_ip**) must be defined. If both are initialized, input of **$eth1_gateway_ip** is ignored.

## Encryption Settings

If variable **$enable_ssl** is **n** (disable crypto), **$plaintext_httpd** must be set to **y** so that httpd (the web server) listens on port 80 (the plaintext port). If **$enable_ssl** is **y** (enable crypto), **$cert_overwrite** (a y/n prompt) must be defined to indicate whether to download new certificate and key. If defined **y**, all related FTP server information (such as **$cert_ftp_server**, **$cert_ftp_username**, **$cert_ftp_user_password**, **$cert_ftp_keyfilename**, **$cert_ftp_crtfilename**) must be provided or else, they can be omitted.

## Event Services Settings

- Variable **$EventGatewayAppParam** needs to be defined only when **$NSMDirective** is set to **http** mode.
- Variable **$EventGatewayNumberCrypto** (number of crypto event gateway) must be set to 0 if **$enable_ssl** (crypto) is **n**.
- The total of **$EventGatewayNumber** and **$EventGatewayNumberCrypto** must be less than 11.

## External Directory Settings

The current schema definition provided in *externaldir.pl* defines sample schema (see Section “Sample Schema” section on page 2-13).

## Other Information

- Perl experts are invited to tailor the **Setup** script as required.
- The main function of **Setup** is located in */opt/CSCOcnsie/bin/setupint.pl*.
- All supporting functions can be found in */opt/CSCOcnsie/bin/setuputils.pm*.
- Prompts-related supporting functions can be found in */opt/CSCOcnsie/bin/PromptSupp.pm*.

# Configuring SSL Certificates

To configure SSL, you must generate a valid certificate:

**Step 1** On any UNIX host that has OpenSSL installed, enter the following commands:

```
% openssl genrsa -out server.key 1024
% chown root:root server.key
% chmod 400 server.key
% openssl req -new -key server.key -out server.csr
```

**Step 2** Ensure that the Common Name is the fully qualified name of the IE2110, for example: www.company.com

**Step 3** Send the file *server.csr* to the Certificate Authority for signing.

Assuming that the signed file is *server.crt*, then the files *server.key* and *cerver.crt* are transferred (FTP) into the CNS 2100 Series as part of its setup process.

**Note** The *server.key* file contains the certificate key. You must ensure that access to this file is restricted because the information in this file can be used to create a machine that can masquerade as a CNS 2100 Series. This would compromise system security.

# How to Verify the Configuration on the CNS 2100 Series System

After you run the **Setup** program, verify that the CNS 2100 Series system is configured correctly:

**Step 1** Log in with the username and password you created during **Setup**.

If you cannot log in, refer to the "Cannot Log In to the System" section on page A-1 for troubleshooting information.

**Step 2** Enter the following command to verify that the system can obtain DNS services from the network:

```
# nslookup <dns_name>
```

where <*dns_name*> is the DNS name of a host that is registered in DNS. If the system cannot obtain the IP address of the host from DNS, run the **Setup** program again and verify the correct IP address for the DNS Server(s).

**Step 3** Enter the following command to verify that the system can communicate with the network:

```
# ping <ip_address>
```

where <*ip_address*> is the IP address of a host that is accessible on the network. A DNS server is an excellent host to ping because it should always be running and accessible.

If the system cannot communicate with the network, refer to the "System Cannot Connect to the Network" section on page A-2 for troubleshooting information.

**Step 4** Enter the command **ifconfig -a** to verify that the configuration is as you expected.

**Step 5** Connect to the system using a web browser to verify HTTP connectivity:

Enter the system IP address in a web browser.

For example, if the system IP address is 10.1.58.5, in a web browser enter the URL **http://10.1.58.5/config/login.html**. If plain text has NOT been enabled for the configuration server, enter **https://10.1.58.5/config/login.html**.

If you cannot connect to the system using a web browser, refer to the "Cannot Connect to the System Using a Web Browser" section on page A-3 for troubleshooting information.

**Step 6** Enter the **exit** command to log out of the system.

# How to Verify the Installation of the Cisco CNS Configuration Engine

Once the system has been installed, you can verify the installation of the Cisco CNS Configuration Engine by following these steps:

**Step 1** Go to a different computer and bring up a web browser.

The Cisco CNS Configuration Engine supports Microsoft Internet Explorer 5.0 or Netscape 4.7 or later.

**Step 2** On the net-site window enter the URL for the Cisco CNS Configuration Engine.

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

where: <*ip_address*> is the IP address you entered during CNS 2100 Series system **Setup**. You can use the hostname if the name has been defined and registered within your DNS domain.

**Note** If you have enabled encryption in the **Setup** program, you must use **https://<***ip_address***>.**

The Cisco CNS Configuration Engine login page appears (see Figure 2-1 on page 2-19).

**Step 3** Enter the ConfigService AdminID and Password that you entered during CNS 2100 Series system **Setup**.

The Home page appears (see Figure 2-2 on page 2-19).

If you have reached the Cisco CNS Configuration Engine Home page, you have verified the successful installation on the Cisco CNS Configuration Engine.

*Figure 2-1 Login Page*

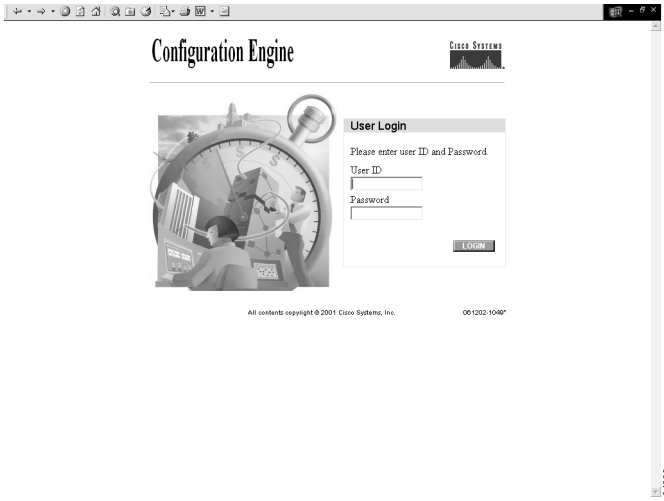
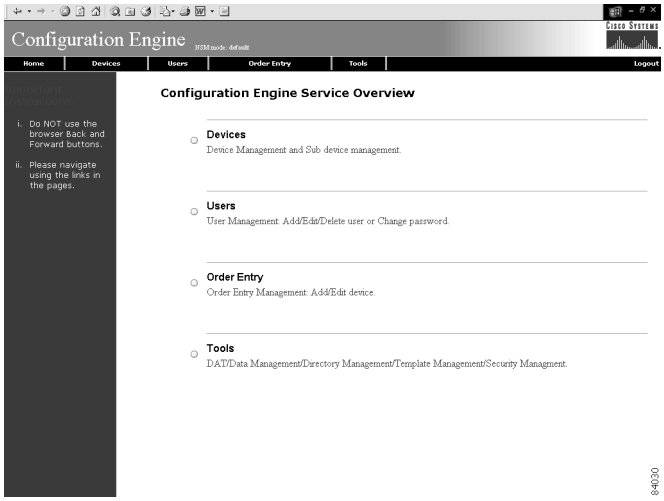



*Figure 2-2 Internal Directory Mode Home Page*




# Migrating DCL Data and Templates from Release 1.2 to 1.3

The migration utility provides a mechanism for upgrading your CNS 2100 Series environment from Release 1.2 to Release 1.3. The utility contains some Perl and Unix shell scripts that help carry out a data migration process. It is a three step process:

1. Export data to a remote FTP site
2. Install Release 1.3 software
3. Retrieve data from the FTP site and setup the box.

Here are the details of each steps:

# Export Data Onto a Remote FTP Site

Before exporting the data, it is assumed that the CNS 2100 Series system has already been setup and is up running.

To export your system data onto a remote FTP site, follow these steps:

**Step 1** Insert the Release 1.3 CD-ROM into the CD drive of the CNS 2100 Series system to be upgraded.

**Step 2** To mount the CD-ROM, login as root and type:

**mount /mnt/cdrom**

**Step 3** Change directory into:

**/mnt/cdrom/DataExport**

**Step 4** Issue the data export command:

**./dataexport**.

**Step 5** Follow the sequence of prompts to enter information of the FTP site and storage location (absolute pathname including filename).

# Install Release 1.3 Software

To re-image the system, while the Release 1.3 CD-ROM is still in the CD drive, at the command line,

**Step 1** Enter the **sync** command two times:

```
[root@abhishek-storm bin]#sync
[root@abhishek-storm bin]#sync
```

**Step 2** Restart the system by hitting the **Reset** button.

# Migrate Data and Setup the CNS 2100 Series System

After the system restarted 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. Acquires information about the FTP server that stores the migration data and retrieves the data.

2. Starts Release 1.3 **Setup** prompts and configures the system.
3. Populates internal directory storage with retrieved data.

Your interface with the first stage is shown below. It employs the same interface as the non-interactive setup, except it also allows the use of **eth1** (see "Non-Interactive Setup" section on page 2-15).

```
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
```

# XML Transform Tool for Users Migrating from Release 1.2 to 1.3

An XML transformation script is added to DAT for automating the XML file conversion process that takes care of the following two problems:

- DAT uses XML file format for bulk uploading data. In release 1.2, the XML file for Bulk Upload feature conforms to a particular DTD that is published for release 1.2. In release1.3, a new DTD is introduced. XML files in release 1.2 DTD format need to be converted to release 1.3 DTD format.
- In addition, there is a release 1.2-to-release 1.3 change of the device object class attribute name for Internal Directory mode from **IOSDeviceID** to **IOSConfigID**. To comply with this change, the data present in the IOSDeviceID attribute for release 1.2 should be copied into the IOSConfigID attribute for release 1.3.

## Usage

For XML file conversion, run the following shell script on the CNS 2100 Series console:

```
/opt/CSCOdat/XMLTransform/datxmltransformer.sh <Path to old xml> <true | false>
```

The system generates an XML file conforming to 1.3 DTD with the same data. The shell script takes two input arguments. The first one specifies the absolute pathname to the old (1.2) XML file. The second one, if set to **true**, starts the conversion of IOSDeviceID to IOSConfigID; default is false if omitted.

For example, given an XML file say "Bulkdata.xml" in release 1.2 DTD format, here is the list of steps for the conversion:

**Step 1** Login to the console of CNS 2100 Series system.

**Step 2** Change directories to:

**/opt/CSCOdat/XMLTransform**

**Step 3** Issue command:

**./datxmltransformer.sh ./Bulkdata.xml**

The XML that is to be converted (Bulkdata.xml) must be present on the CNS 2100 Series system. The script creates a new file with the name "Bulkdata-new.xml" in the same directory as the old file. This file conforms to release 1.3 DTD. You can use it to upload the Bulkdata in Cisco CNS Configuration Engine 1.3.

# Importing Groups and Devices from Release 1.2 to 1.3

In Configuration Registrar 1.2 all devices are stored in the DCL directory in the Internal Directory (Standalone) mode. In this configuration, the only NSM mode supported is **default** mode.

In Cisco CNS Configuration Engine 1.3, Internal Directory mode, all NSM modes (**none**, **default**, and **http** algo/non-algo) are supported.

When you import groups from a Release 1.2 system to a Release 1.3 system, and the Release 1.3 system is setup in NSM **default** mode, devices in the default group and imported groups can receive configurations sent to them. However, when the Release 1.3 system is setup in the NSM **http** mode, sending events to the imported groups (non-default groups) fail.

For imported groups to work in Release 1.3 (NSM **http** mode), you must create a reference for the imported group to an application namespace. The reason is, that NSM **http** mode was not available in Release 1.2 Internal Directory (Standalone) mode.

The value for the application namespace is set during **Setup** with the prompt:

```
Enter the Event Gateway Application Parameter:
```

By default value for this parameter is **config**. You can override this value during Setup with one of your own.

To create the reference to an application namespace (**config** by default) for an imported group, follow these steps:

**Step 1** Log in to your Release 1.3 system user interface.

See "How to Log In" section on page 3-2.

**Step 2** Click on **Tools**.

See "Management Tools" section on page 3-32.

**Step 3** Click on **DAT**.

**Step 4** Log in to DAT.

See "How to Log In" section on page 5-1.

**Step 5** From DAT main menu, click on **Groups**.

See "How to Manage Groups" section on page 5-11.

**Step 6** From the Groups Management page, click Update Groups.

See "Modifying Groups" section on page 5-14.

**Step 7** Select the group to which you want to add the application reference to **config**.

**Note** If during **Setup**, you set a value other than **config** for the Event Gateway Application Parameter, use this value when setting the application reference.

See "How to Add Applications to a Group" section on page 5-17.

**Step 8** Check the check box for **config**.

**Step 9** Click **Add**.

# How to Revert to Factory Setting

To revert to factory settings, follow these steps:

**Step 1** Initiate a system backup.

For information about backup, see "Backup and Restore" section on page 3-54.

**Step 2** Log in as root.

Use your root password.

**Step 3** Type **reinitialize**.

This program clears your system configuration and returns you to **Setup**.

**Step 4** Run **Setup** (see "Running the Setup Program" section on page 2-1).

# How to Reconfigure System Network Information

To reconfigure system network information, such as CNS 2100 Series system IP address and hostname, 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** (see "Running the Setup Program" section on page 2-1).

## Hostname Updates

If you want to change the hostname, country code, or location code without destroying the DCL data and templates, use the **relocate** command. You can use the **relocate** command in both internal (user-created devices and templates) and external (IMGW data) directory modes.

# How to Recover and Redefine Your Root Password

To recover and redefine your root password, follow these steps:

**Step 1** Verify that the default account has been redefined:

Login: **root**

Password: **blender**

If it has, continue to Step 2 to erase the root account password.

**Step 2** Restart the system by pressing the reset button and watch the output at your serial port (or VGA) console.

**Step 3** At the LILO boot prompt (**boot:**), press the **TAB** key.

The the name of the boot image appears.

**Step 4** At the boot prompt, type:

**linuxserial single** (or **linuxvga single**).

This starts you into single-user mode on your serial port (or VGA console) where you should see the prompt:

**sh-2.04#**

**Step 5** Redefine the root password using the **passwd** command as follows:

```
sh-2.04 # passwd
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
sh-2.04#
```

**Step 6** At the prompt **sh-2.04#** type:

**exit**

This returns you to the remaining startup sequence.

**Step 7** At the login prompt, login as root with the new password defined in Step 5.

# Registering the System in DNS

Register the system in DNS, using the system hostname as its DNS name.

**Caution** If you do not register the system in DNS using the system hostname as its DNS name, network connectivity problems will occur.

Events are sent to the router with the hostname as the identifier, not the IP address. Consequently, if the CNS 2100 Series system is not registered in DNS, the routers are not able to find it and cannot download configurations.

# Installing a Replacement CNS 2100 Series System

This section describes the tasks you should perform when installing a replacement CNS 2100 Series system (a new unit intended to replace an existing unit). These tasks are in addition to the installation and configuration processes described in the "Running the Setup Program" section on page 2-1.

## How to Remove the Old System

Before removing the old system:

**Step 1** Initiate a system backup.

For information about backup, see "Backup and Restore" section on page 3-54.

**Step 2** Verify the backup data is where you expect it to be.

**Step 3** Enter the **shutdown** command.

The system shuts down.

**Step 4** Power down and remove the old system.

## How to Install a Replacement System

To install a replacement system, complete the following steps:

**Step 1** Install and power on the new system.

Refer to the *Cisco CNS 2100 Series Intelligence Engine Installation Guide*.

**Step 2** Run the **Setup** program.

See the "Running the Setup Program" section on page 2-1.

**Step 3** Use the configuration settings that you recorded from the old system to answer the **Setup** program prompts.

**Step 4** Restore system data.

For information about restore, see "Backup and Restore" section on page 3-54.

# How to Restart the Cron Daemon

The time base for the CNS 2100 Series system should be set to Coordinated Universal Time (UTC). If time is changed, you must restart the cron daemon.

To restart the cron daemon, follow these steps:

**Step 1** Connect to the console if you cannot connect using Telnet.

**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** 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 Reimage Your System

If the image on your hard disk has become corrupted, but the disk is operational (you can restart from the hard disk), simply reimage your system by installing the Cisco CNS Configuration Engine 1.3 CD-ROM.

## Critical System Information

Before you reimage your CNS 2100 Series system, record the following information about your CNS 2100 Series system:

- IP address
- Gateway address
- Network mask
- DNS name server address

You will need this information when you run **Setup** after the reimage procedure.

# Initializing Tivoli Management Agent

This section describes how to:

- Register and de-register the Tivoli Management Agent (TMA) to the system start and stop service
- Initialize the TMA
- Connect the agent to an Endpoint Gateway
- Enable the TMA to start during system boot

This Linux TMA supports Tivoli Framework environment 3.7 and up.

## Procedure Overview

- Register Tivoli agent to system start/stop service.
- Install the agent and attach target Endpoint Gateway

## Register and De-register Tivoli Agent to System Start and Stop Service

**Step 1** To register the Tivoli agent start/stop script (*/etc/rc.d/init.d/Tivoli_lcf1*) to system start and stop service, use the following command:

**chkconfig --add Tivoli_lcf1**

Once the script is registered, Tivoli agent automatically stops and starts at system restart.

**Step 2** To de-register the agent from system start/stop service, use:

**chkconfig --del Tivoli_lcf1**

## How to Initialize the TMA

To install and initialize the agent on the system and connects it to the Endpoint Gateway passed as an argument from the command line, use the following commands:

**cd /opt/Tivoli/lcf/dat/1**

**./lcfd.sh install –g <***gateway_name***>+<***gw_port***> -P <***lcfd_port***> <***plus any other lcfd options***>**

The <*lcfd_port*> argument must be unique for the Endpoint Gateway environment where you are installing the agent.

## How to Verify the TMA is Running

**Step 1** From the command line, enter:

**ps –ef | grep lcf**

This should return the **pid** and information about the running **lcf** process.

**Step 2** From the Tivoli Desktop, validate that the agent appears in the target Gateways Endpoint list.

**Step 3** From the command line, enter:

**wep <***endpoint_name***> status**

This should respond with the message:

```
<endpoint_name> is alive.
```


# Cisco CNS Configuration Engine Administration for Internal Directory Mode

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

- Levels of Access
- How to Log In and Out of the System
- How to Manage User Accounts
- How to Manage Devices
- Device Configuration Order Entry
- Management Tools
- Backup and Restore

## 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 Log In and Out of the System

You can connect to the system by means of:

- Telnet
- System console

# How to Log In

To log into 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.

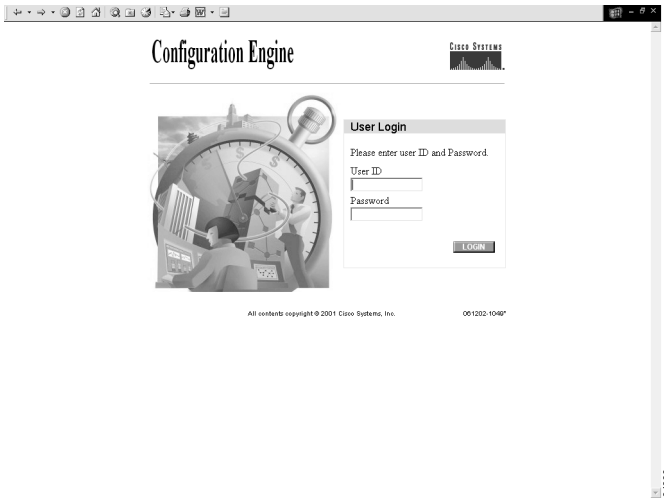
**Step 2** Go to the Cisco CNS Configuration Engine URL.

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***




**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 Home page appears (see Figure 3-2).

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

*Figure 3-2 Administrator Home Page*

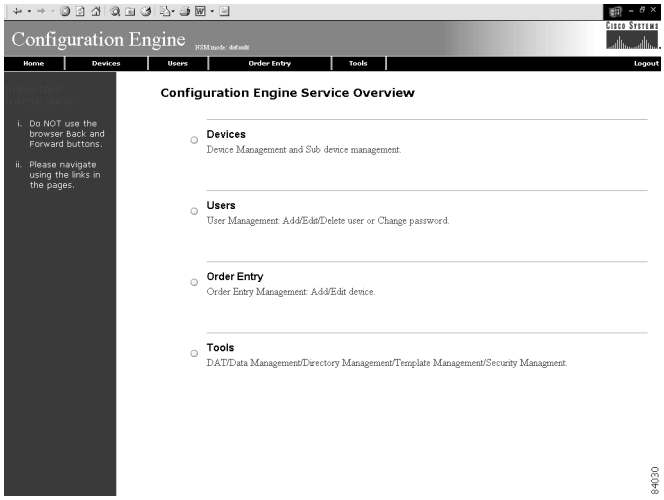
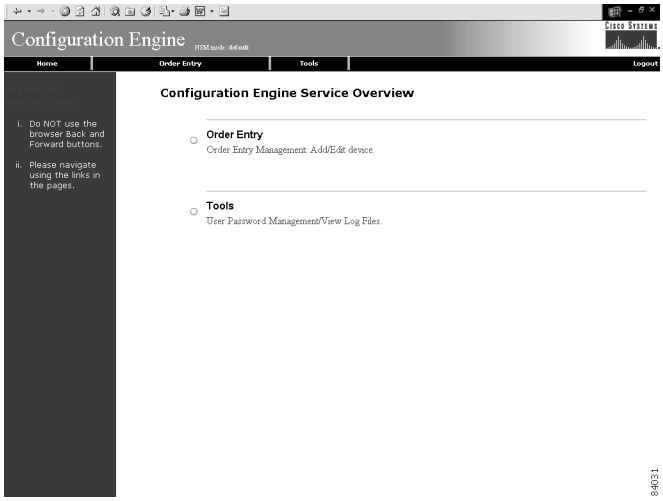



*Figure 3-3 Operator Home Page*




## 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, an Operator has access to the following functions:

- Order Entry
  - New Order
  - Edit Order

  - Subdevice Order
- Tools
  - Change Password
  - View Event Log

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.

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

# Device Configuration Order Entry

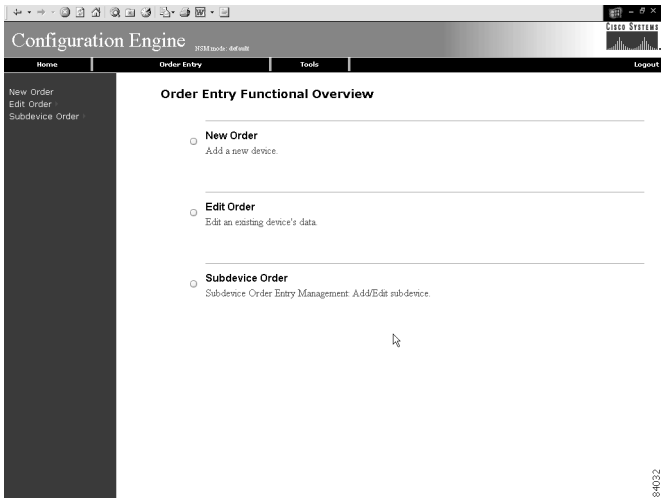
To conduct device configuration order entry operations as an Operator, follow these steps:

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

The Order Entry page appears (see Figure 3-4).

**Step 2** To add and edit device configuration orders, see "Device Configuration Order Entry" section on page 3-24.

***Figure 3-4 Order Entry for Operator-Level User***



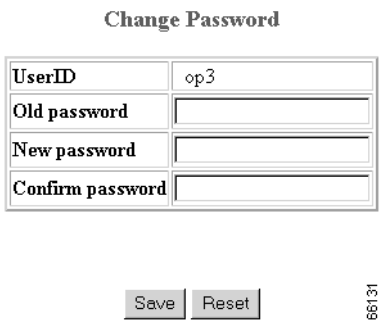

# How to Change or Reset a Password at the Operator Level

To change or reset a password at the operator level, follow these steps:

**Step 1** From the Home page, click **Tools**.

The password editor appears (see Figure 3-5).

*Figure 3-5 Operator Password Editor*




**Step 2** Enter your old password.

**Step 3** Enter your new password, then repeat.

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

**Step 5** To save your edits, click **Edit**.

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

# How to View the Event Log

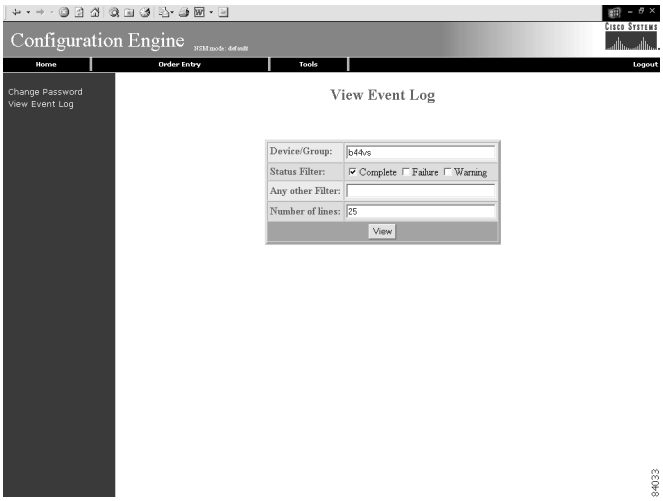
As an operator, to view the Event Log, follow these steps:

**Step 1** From the Home page, click **Tools**.

**Step 2** To view the Event Log, click **View Event Log**.

The Event Log control panel appears (see Figure 3-6)

*Figure 3-6 Operator-Level Event Log Control Panel*



# Administrator-Level Operations

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

## How to Manage User Accounts

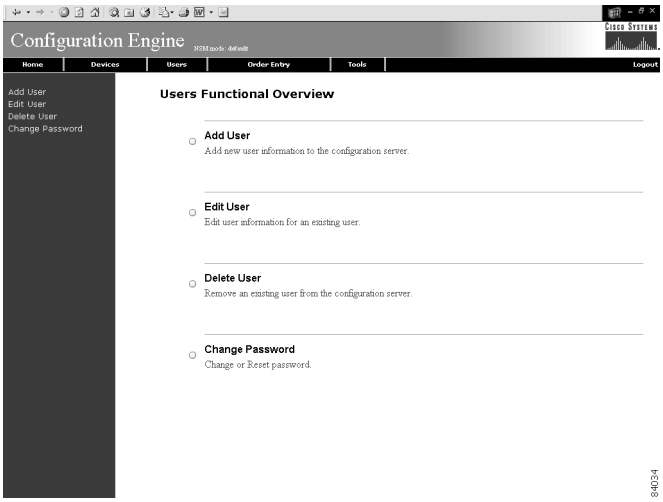
To begin managing user accounts, follow these steps:

**Step 1** Log into the system (see "How to Log In and Out of the System" section on page 3-1).

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

A functional overview of the user administration options appears (see Figure 3-7).

***Figure 3-7 User Administration Overview***



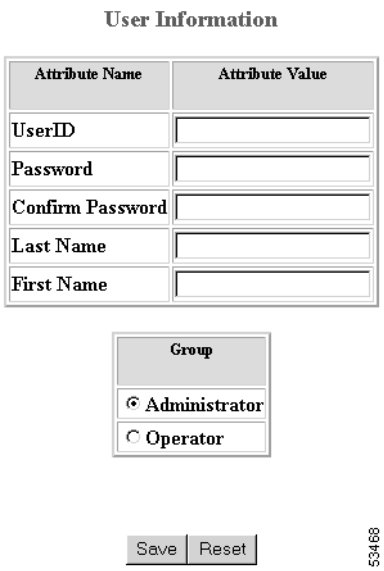

### How to Add a User Account

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 3-8).

*Figure 3-8 User Information*




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

**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 main menu, click on the **User** tab.

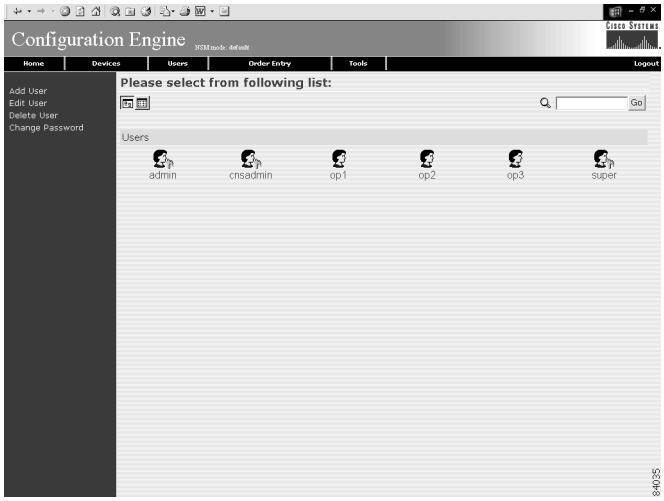
## How to Edit a User Account

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 3-9).

*Figure 3-9 User 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 3-10).

*Figure 3-10 User Information*


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

**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.

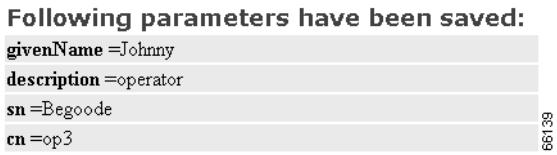
**Step 7** To clear your entries, click **Reset**.

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

User information update status appears (see Figure 3-11).

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

*Figure 3-11 User Information Update Status*




## 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 3-9), click on the icon for the user account you wish to delete.

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

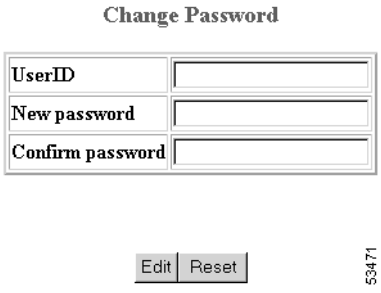
## How to Change or Reset a User Password

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 3-12) appears.

*Figure 3-12 Change Password*




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

**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 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 3-9).

The User Information page appears (see Figure 3-13).

***Figure 3-13 User Information***


**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 main menu, click on the **User** tab.

# How to Manage Devices

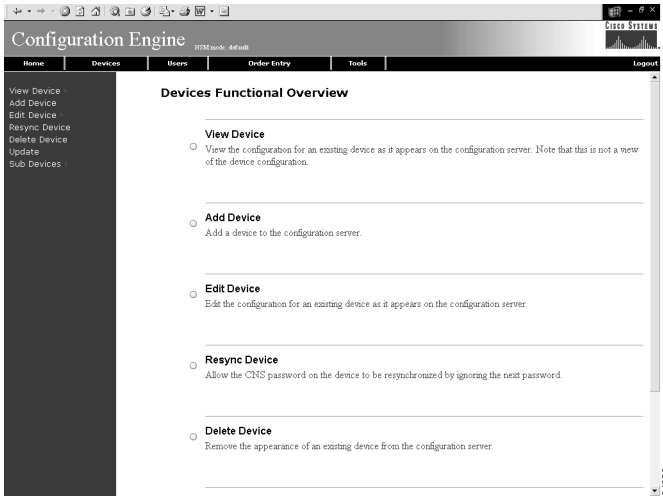
To begin managing devices, follow these steps:

**Step 1** Log into the system (see "How to Log In and Out of the System" section on page 3-1).

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

A functional overview of the device administration options appears (see Figure 3-14).

*Figure 3-14 Device Administration Overview*



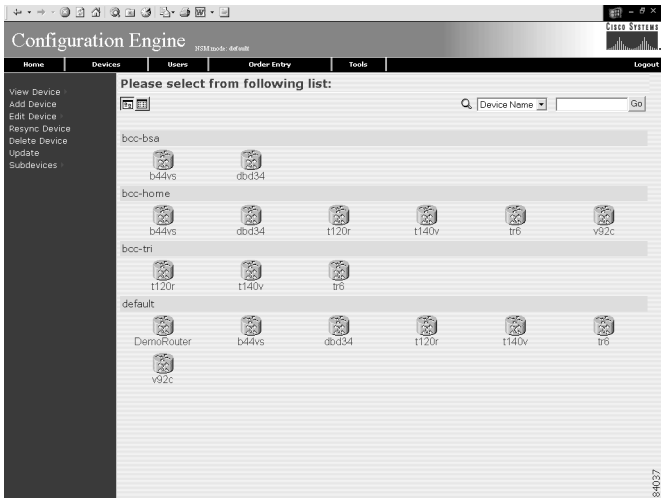

## How to View Device Configuration

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 3-15).

*Figure 3-15 Device List*




**Step 2** 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 3** To return to the main menu, click on the **Devices** tab.

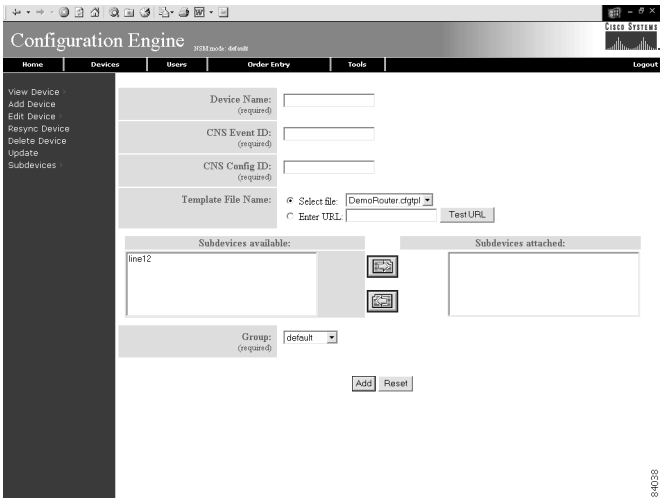
## How to Add a Device

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 3-16).

***Figure 3-16 Device Information Page***




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

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

**Step 4** Accept the default value that appears or enter another valid value (no spaces) in the **Config ID** field.

The ConfigID must match the one used to manage this particular device.

**Step 5** Choose a template file.

To use a template on your Cisco CNS Configuration Engine:

a. Choose **Select file**.

b. Use the pull-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** If applicable (modular router), choose subdevices.

**Step 7** Choose a group.

**Tip** Use the Group Manager under DAT (see "How to Add a Group" section on page 5-13) to set up groups before you add a device.

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

**Step 9** To add this device, click **Add**.

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

## How to Edit a Device

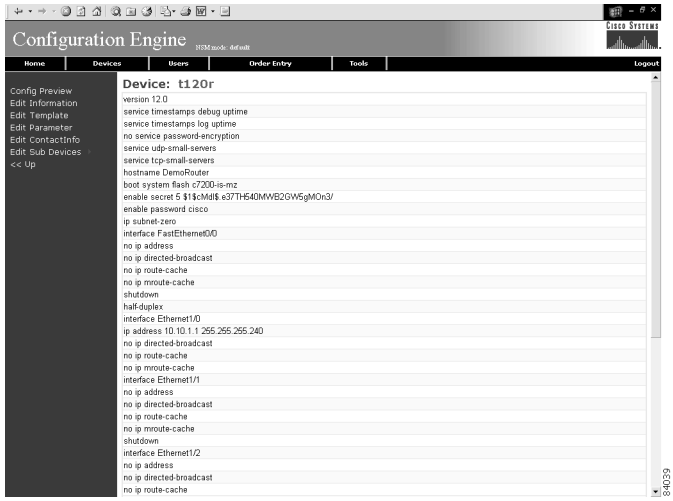
To edit information associated with a particular device, follow these steps:

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

**Step 2** From the Device List page (see Figure 3-15), 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 3-17).

***Figure 3-17 Device Configuration***




**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 main menu, click on the **Devices** tab.

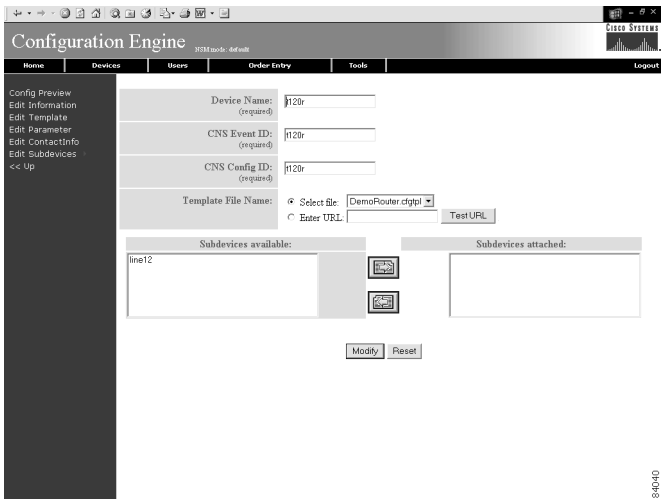
## How to Edit Device Information

To edit device information, follow these steps:

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

The device information dialog box appears (see Figure 3-18).

***Figure 3-18 Device Information Editor***




**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** Modify the template file as required.

**Step 6** Use the Arrow buttons to modify the status of subdevices attached to this device.

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

**Step 8** To update device information, click **Modify**.

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

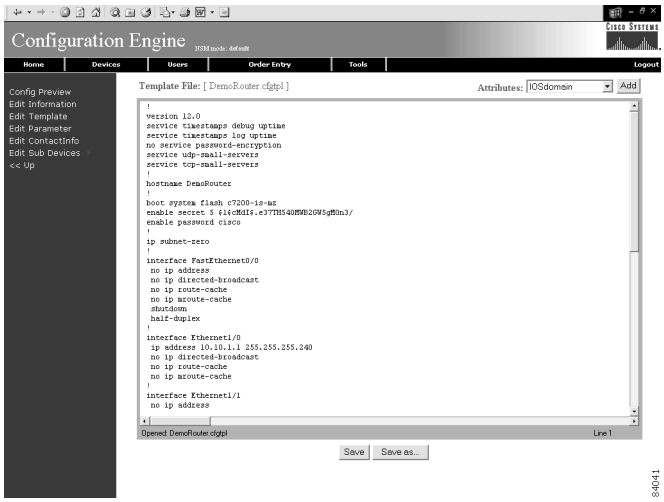
## How to Edit Device Templates

To edit a device template, follow these steps:

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

The template editor appears (see Figure 3-19).

*Figure 3-19 Template Editor*




**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 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 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 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 Devices Functional Overview page (see Figure 3-14), click **Resync Device**.

**Step 2** From the Device Selection page (see Figure 3-15), click on the icon for the device you wish to re-synchronize.

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

**Step 4** To return to the 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 3-14), click **Delete Device**.

**Step 2** From the Device Selection page (see Figure 3-15), click on the icon for the device you wish to delete.

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

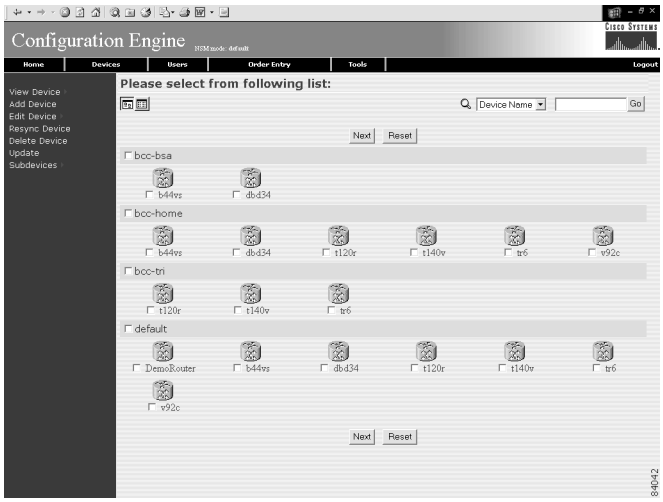
## How to Update a Device Configuration

To send an updated version of the configuration to a device, follow these steps:

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

The Device Update List page appears (see Figure 3-20).

*Figure 3-20 Device Update List*

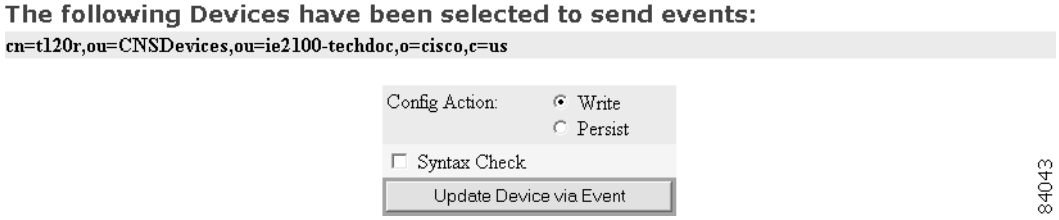



**Step 2** Click on the check box next to the icon for the device(s) or group(s) you wish to update.

**Step 3** Click **Next**.

The update task dialog box appears (see Figure 3-21)

*Figure 3-21 Update Task*




**Step 4** 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 5** If required, check the **Syntax Check** check-box.

**Step 6** Click **Update Device via Event**.

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

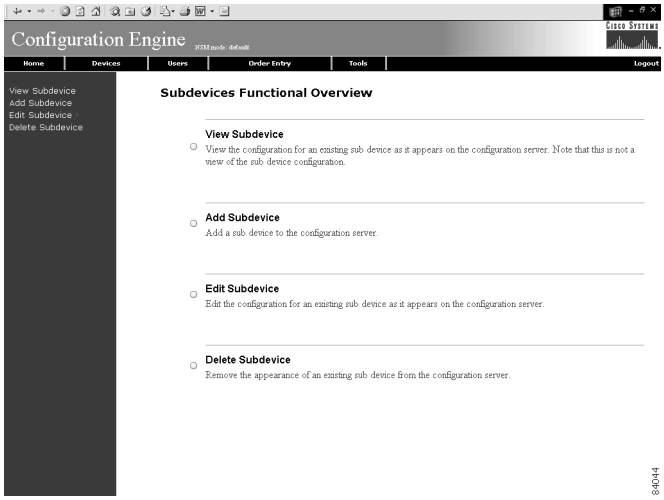
## Working with Subdevices

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 3-22).

*Figure 3-22 Subdevices*



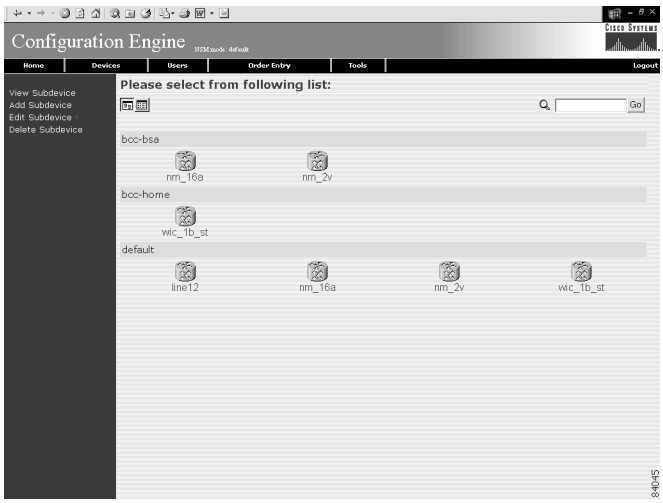

## How to View Subdevices

To view subdevices, follow these steps:

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

The list of subdevices appears (see Figure 3-23).

*Figure 3-23 Subdevice List*




**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 main menu, click on the **Devices** tab.

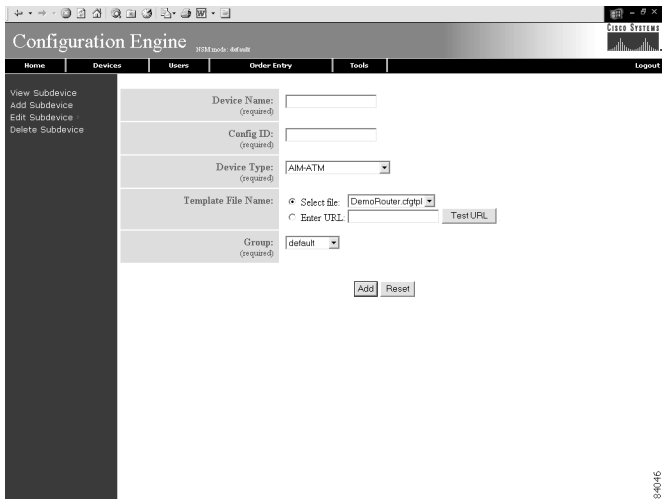
## How to Add Subdevices

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 3-24).

***Figure 3-24 Subdevice Information Page***




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

**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** pull-down menu, 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:

a. Choose **Select file**.

b. Use the pull-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 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 main menu, click on the **Devices** tab.

## How to Edit Subdevices

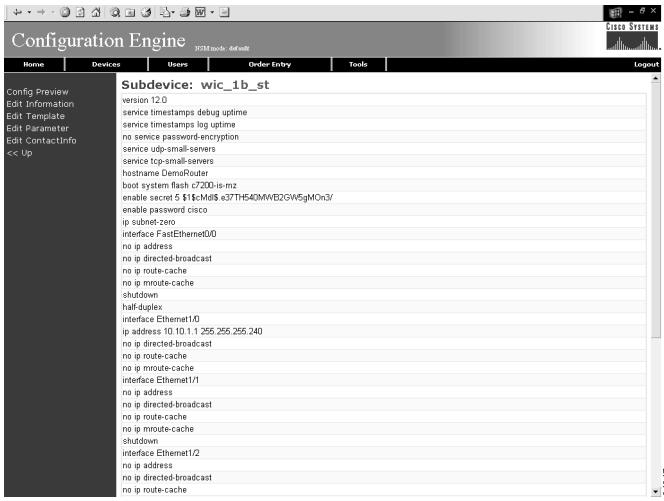
To edit information associated with a particular subdevice, follow these steps:

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

**Step 2** From the Subdevice List page (see Figure 3-23), 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 3-25).

***Figure 3-25 Subdevice Configuration***




**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 main menu, click on the **Devices** tab.

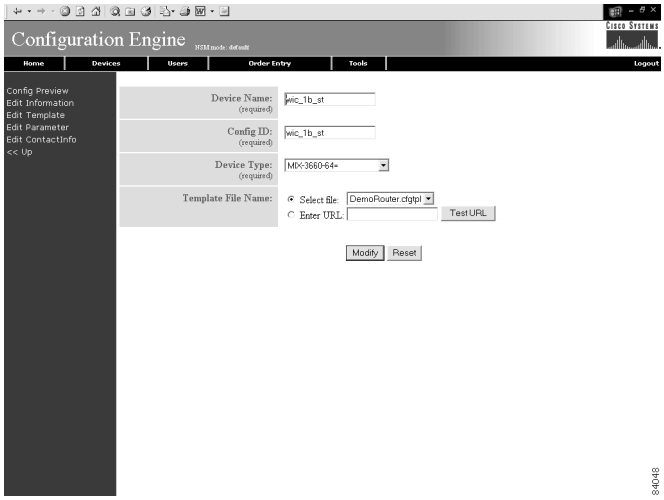
## How to Edit Subdevice Information

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 3-26).

*Figure 3-26 Device Information Editor*




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

**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 main menu, click on the **Devices** tab.

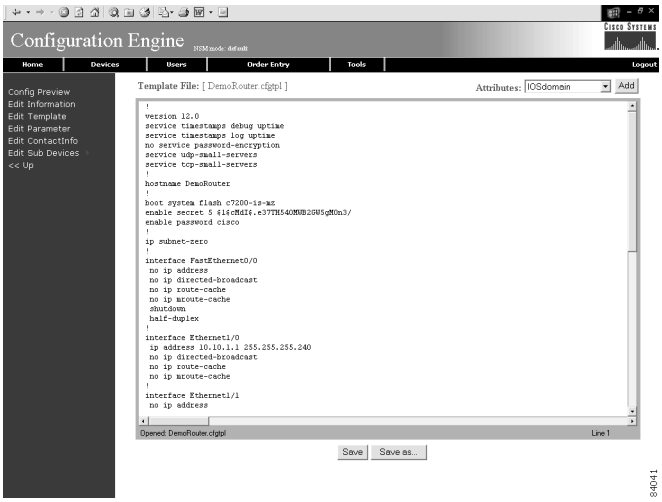
## How to Edit Subdevice Template

To edit a device template, follow these steps:

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

The template editor appears (see Figure 3-27).

*Figure 3-27 Template Editor*




**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 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 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 main menu, click on the **Devices** tab.

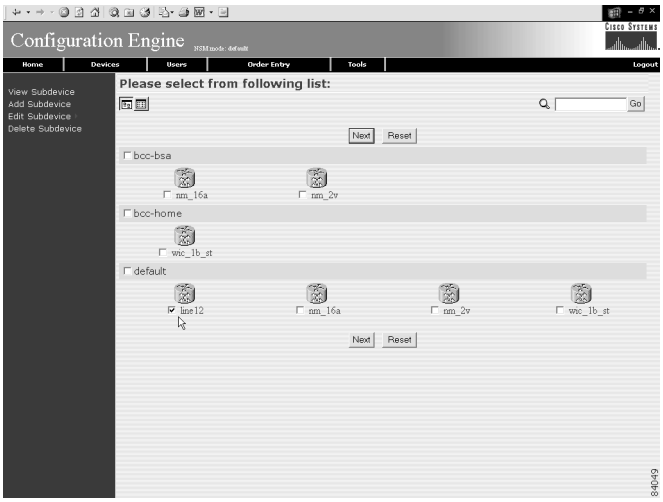
## How to Delete Subdevices

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 3-22), click **Delete Device**.

The Subdevice Selection list appears (see Figure 3-28).

***Figure 3-28 Subdevice Selection List***

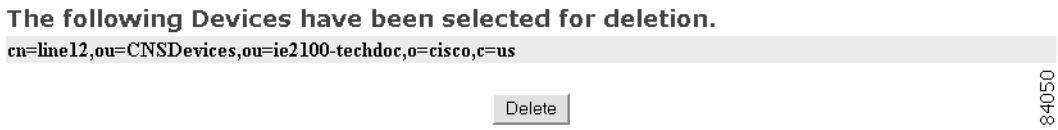



**Step 2** From the Subdevice Selection list, check the subdevices you wish to delete.

**Step 3** To proceed, click **Next**.

A status page appears indicating that the subdevice has been selected for deletion (see Figure 3-29).

*Figure 3-29 Delete Subdevice*



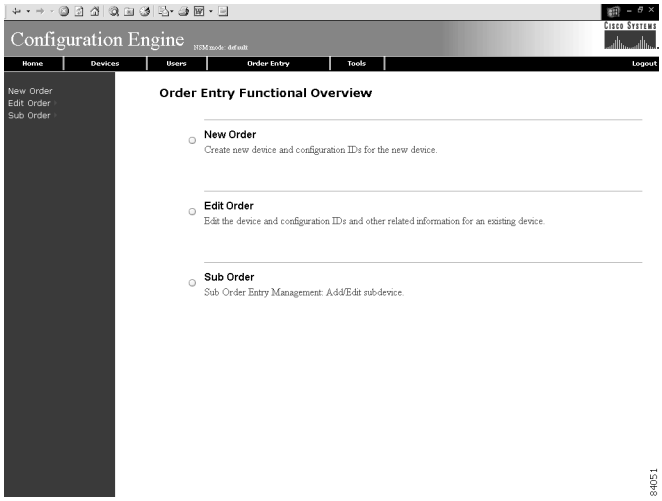

**Step 4** To delete this subdevice, click **Delete**.

**Step 5** To return to the main menu, click on the **Devices** 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 3-30).

*Figure 3-30 Device Configuration Order Entry*



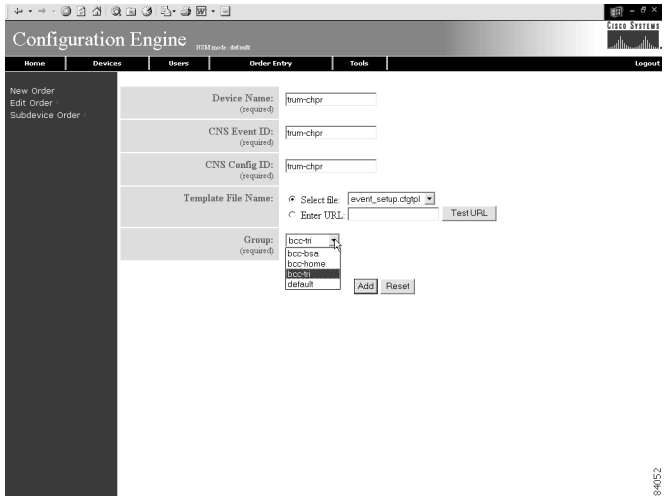

## How to Enter an Order for a New Device Configuration

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 3-31).

*Figure 3-31 New Device Configuration Order*




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

**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:

a. Choose **Select file**.

b. Use the pull-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 5-13) 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**.

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

# Editing an Existing Configuration Order

To edit an existing configuration order, follow these steps:

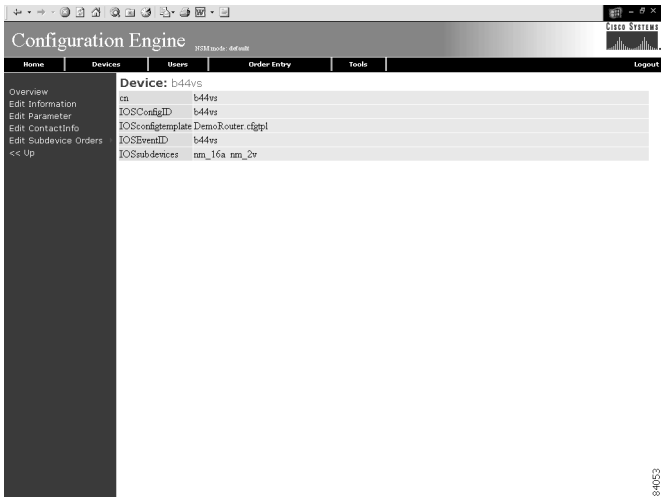
**Step 1** From the Order Entry Functional Overview page, click Edit Order.

The Device List page appears (see Figure 3-15).

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

The device configuration order editor appears (see Figure 3-32) with a menu of edit functions in the left pane.

***Figure 3-32 Device Configuration Order Editor***



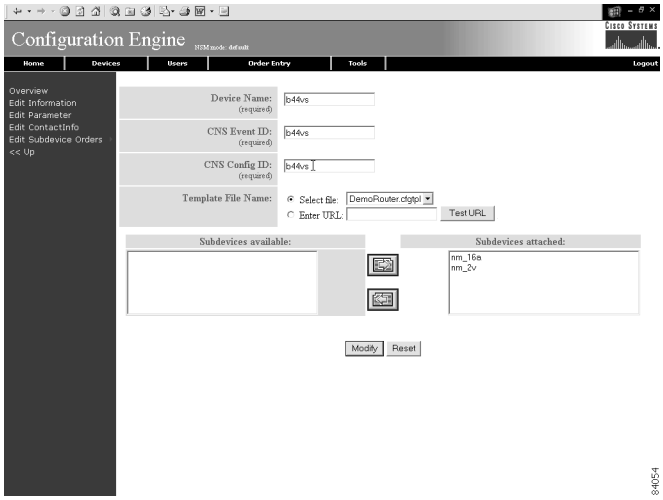

## How to Edit Existing Order Information

To edit existing order information, follow these steps:

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

The order information dialog box appears (see Figure 3-33).

*Figure 3-33 Order Information Editor*




**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 main menu, click on the **Order Entry** tab.

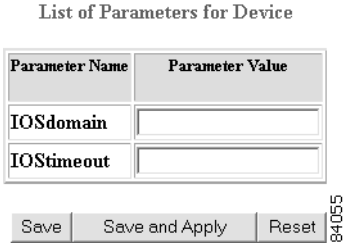
## How to Edit Parameters

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 3-34).

*Figure 3-34 Parameter Editor*




**Step 2** Edit the value of the **IOSConfigID** field.

When a devices is added, the **IOSDeviceID** field is set to device name.

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

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

A parameter save status page appears (see Figure 3-35).

***Figure 3-35 Parameter Save Status***


**Step 5** To save and apply your edits to the existing order, click **Save and Apply**.

A parameter save and apply status page appears (see Figure 3-36).

***Figure 3-36 Parameter Save and Apply Status***


**Step 6** To return to the 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 3-37).

*Figure 3-37 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 |

66112

**Step 2** Edit all active fields as required.

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

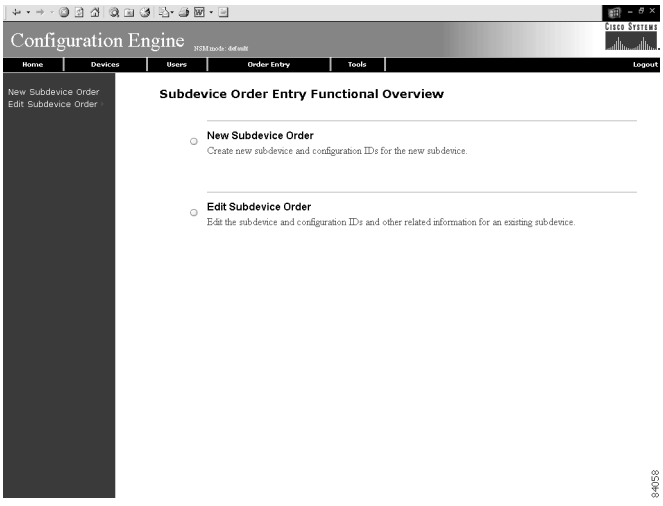
**Step 4** To save your edits, click **Update**.

**Step 5** To return the to the 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 3-38).

*Figure 3-38 Subdevice Order Entry*



### 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 3-24).

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

**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** pull-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:

a. Choose **Select file**.

b. Use the pull-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 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 main menu, click on the **Devices** tab.

### How to Edit an Existing Order for a Subdevice Configuration

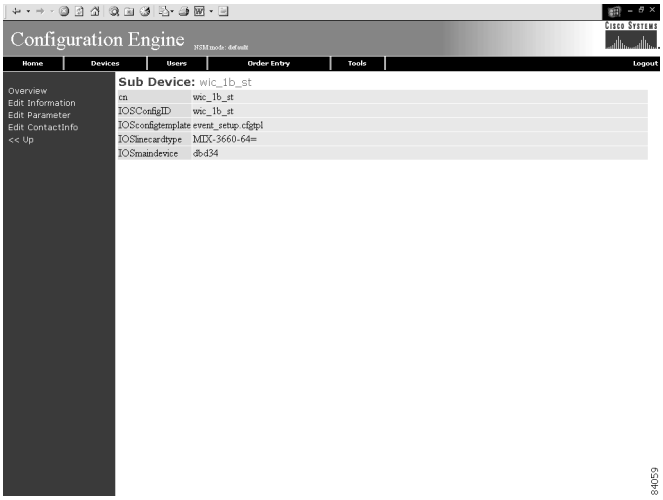
To edit an existing order for a new subdevice configuration, follow these steps:

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

**Step 2** From the Subdevice List page (see Figure 3-23), 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 3-39).

*Figure 3-39 Edit Subdevice Order*



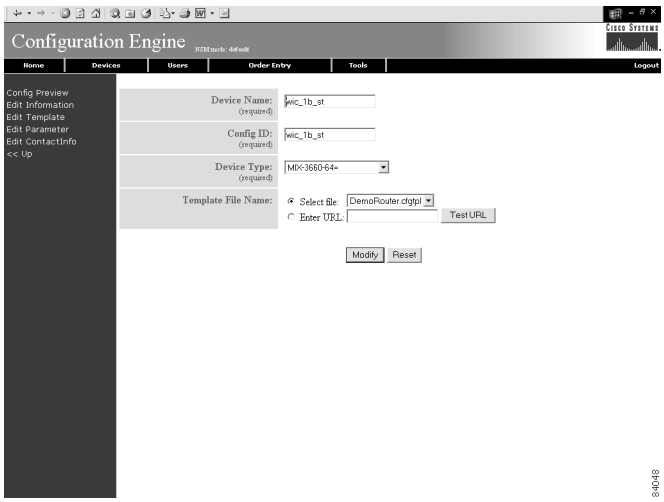

## How to Edit Subdevice Information

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 3-40).

*Figure 3-40 Device Information Editor*




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

**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 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 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 main menu, click on the **Devices** tab.

## Management Tools

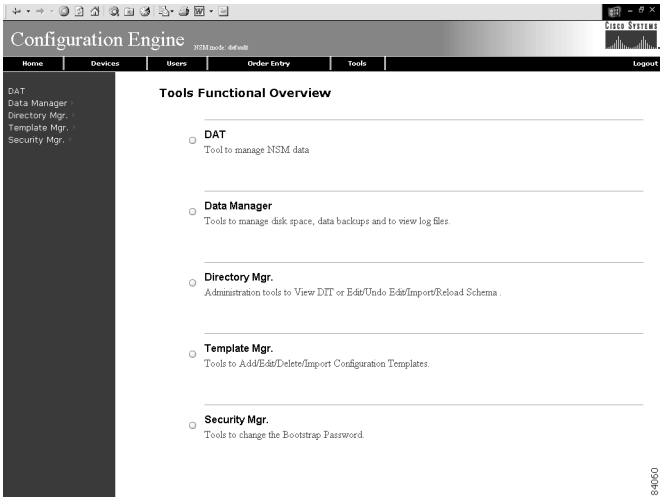
To use the management tools, from the Home page, click on the Tools tab.

The Tools page appears (see Figure 3-41).

From the Tools page, you can access the following management tools:

- DAT
- Data Manager
- Directory Manager
- Template Manager

*Figure 3-41 Management Tools*



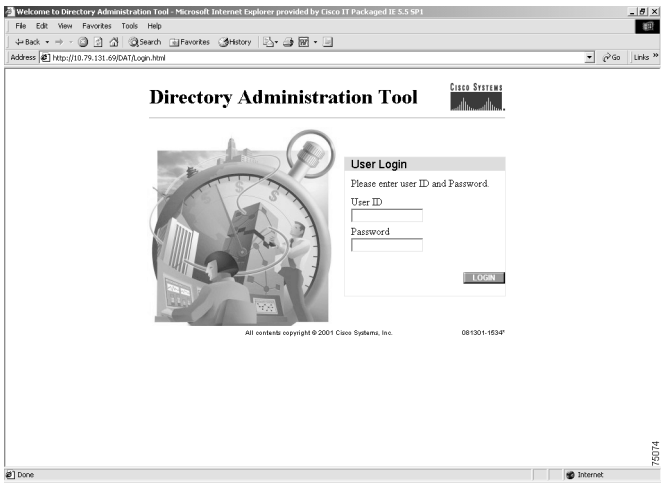

# How to Use DAT

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 3-42).

*Figure 3-42 Directory Administration Tool Login Window*




**Step 2** Enter your **User ID**.

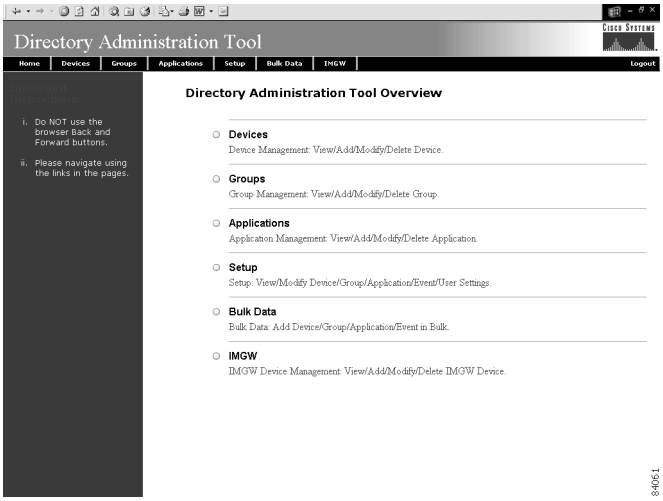
This is the LDAP proxy user name for the Cisco CNS Configuration Engine administrative account that you entered during **Setup**.

**Step 3** Enter your LDAP proxy password.

**Step 4** Click **LOGIN**.

The Directory Administration Tool Overview page appears (see Figure 3-43).

*Figure 3-43 DAT Home Page*




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

# Managing Data

The data manager tools allows you to:

- Schedule data backups
- View various logs files

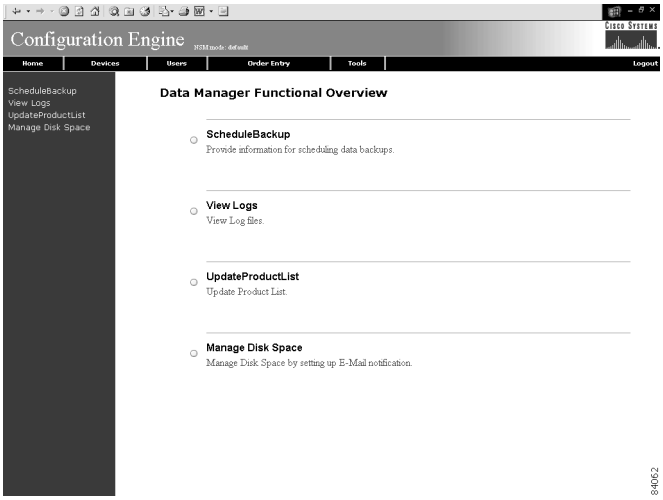
## How to Schedule Data Backup

To schedule a data backup, follow these steps:

**Step 1** From the Tools page, click **Data Manager**.

The Data Manager page appears (see Figure 3-44).

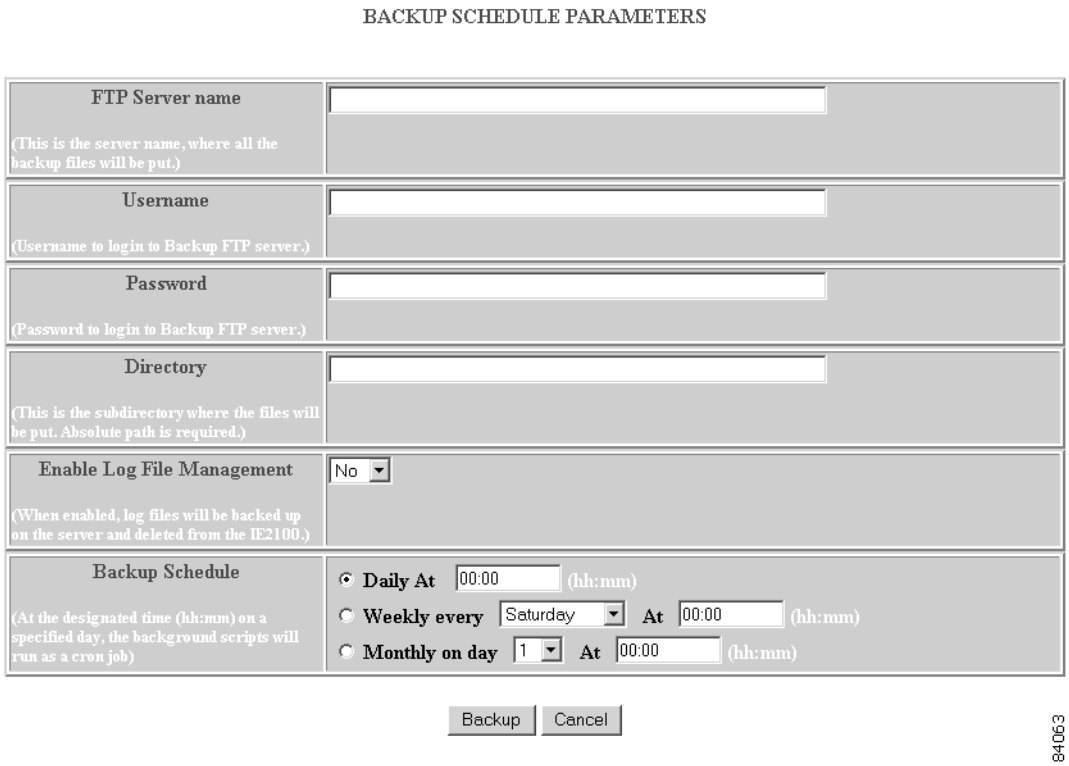
*Figure 3-44 Data Manager*




**Step 2** Click **ScheduleBackup**.

The backup information dialog box appears (see Figure 3-45).

*Figure 3-45 Backup Schedule Parameters*




**Step 3** To specify where you want the backup data to be stored, enter the FTP server name in the **FTP Server Name** field.

**Step 4** To specify the username to log into the FTP server, enter a valid username in the **Username** field.

**Step 5** To specify the password to use to log into 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, see "Backup and Restore" section on page 3-54.

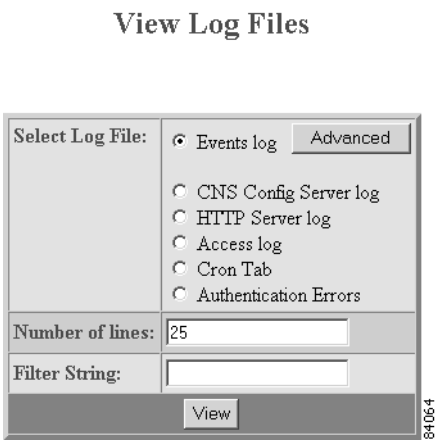
## How to View Log Files

To view various log files, follow these steps:

**Step 1** From the Group Manager page, click **View Logs**.

The View Log Files dialog box appears (see Figure 3-46).

***Figure 3-46 Log File Viewer***




**Step 2** Choose the log file you want to view.

**Step 3** Set the number lines you want to display.

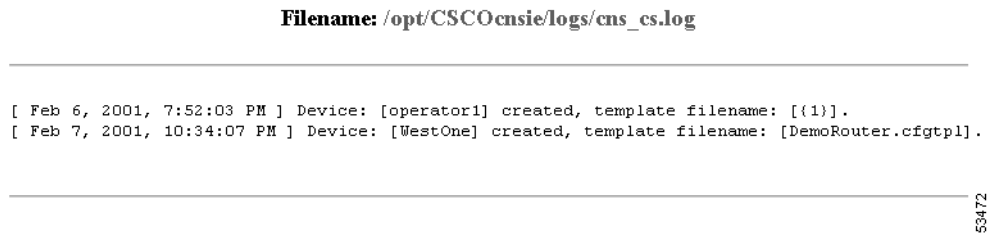
**Step 4** To limit the report to display only specific entries, set a case-sensitive keyword filter, or leave blank.

**Step 5** Click **View**.

A report displays (for an example see Figure 3-47).

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

*Figure 3-47 Log File*




## How to Update Product List

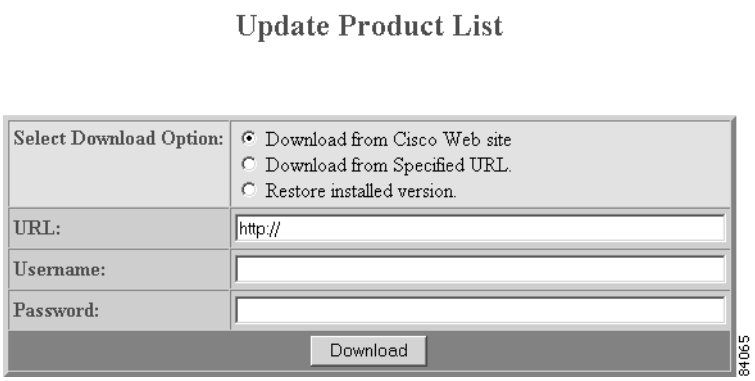
The product list is a mapping between product name of the network modules as specified in the pricing list and the numeric identification number stored in EPROM. As new products are added, this list grows and hence the need for the Cisco CNS Configuration Engine to update this list whenever new products 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 Group Manager page, click **Update Product List**.

The Update Product List dialog box appears (see Figure 3-48).

*Figure 3-48 Update Product List*




**Step 2** Select the appropriate download option.

**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 main menu, click on the **Tools** tab.

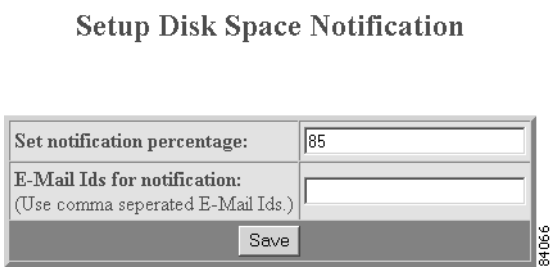
## How to Manage Disk Space

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 3-49).

***Figure 3-49 Disk Space Notification***




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

**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 main menu, click on the **Tools** tab.

# How to Manage Directory Content

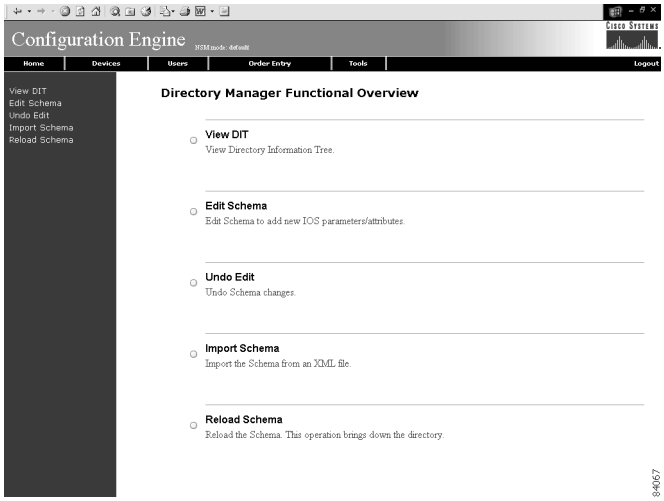
With the directory manager you can:

- View the directory information tree
- Edit the schema
- Import a schema from an XML file
- Reload the schema

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

The Directory Manager page appears (see Figure 3-50).

*Figure 3-50 Directory Manager*




## How to View the Directory Information Tree

To view the directory information tree (DIT), click **View DIT**. The DIT appears (see Figure 3-51).

*Figure 3-51 DIT (Partial View)*

**Output**

```
Country /c=us

Organization /c=us/o=cisco

OrganizationalUnit /c=us/o=cisco/ou=lizard

Person /c=us/o=cisco/ou=lizard/cn=cnsadmin
  GivenName                          "Jeff"
  UserPassword                       "********"
  Description                        "administrator"
  Surname                            "Bray"

Person /c=us/o=cisco/ou=lizard/cn=dcdadmin
  UserPassword                       "*********"
  Surname                            ""

Person /c=us/o=cisco/ou=lizard/cn=operator1
  GivenName                          "Go"
  UserPassword                       "********"
  Description                        "operator"
  Surname                            "Fast"

OrganizationalUnit /c=us/o=cisco/ou=lizard/ou=IOSConfigs

IOSConfigClass /c=us/o=cisco/ou=lizard/ou=IOSConfigs/cn=DemoRouter
  IOShostname                        "DemoRouter"
  IOSDeviceID                        "DemoRouter"
  IOSpassword                        "DemoRouter"
  IOSipaddress                       "10.10.1.1"
```

53444

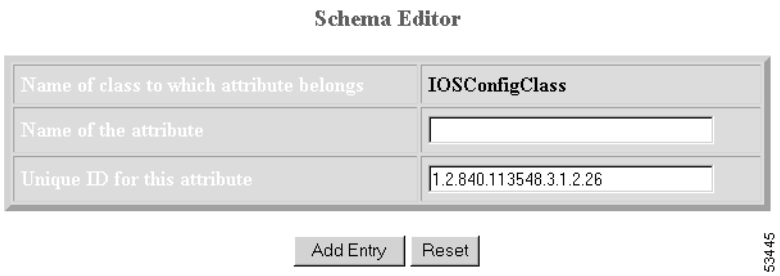
## How to Edit the Schema

To edit the schema, follow these steps:

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

The schema editor appears (see Figure 3-52).

***Figure 3-52 Schema Editor***




**Step 2** Enter the name of the new attribute in the **Name of the attribute** field.

**Step 3** Accept or modify the **Unique ID** for this attribute.

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

**Step 5** To add this attribute to the schema, click **Add Entry**.

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

## How to Undo Schema Edit

You can undo the last schema update and revert to the previous schema by clicking **Undo Edit** on the Directory Manager page.

## 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 3-53).

*Figure 3-53 Import Schema*


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

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 main menu, click on the **Tools** tab.

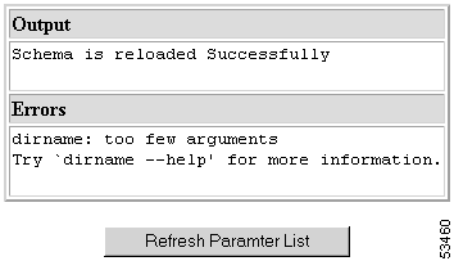
## How to Reload the Schema

To reload the schema, follow these steps:

**Step 1** From the Directory Manager page, click **ReloadSchema**.

The reload operation runs and a report displays (see Figure 3-54).

*Figure 3-54 Reload Schema*




**Step 2** To refresh the parameters, click **Refresh Parameter List**.

**Step 3** To return to the 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 3-58). 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 3-43). 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
```

## 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 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
```

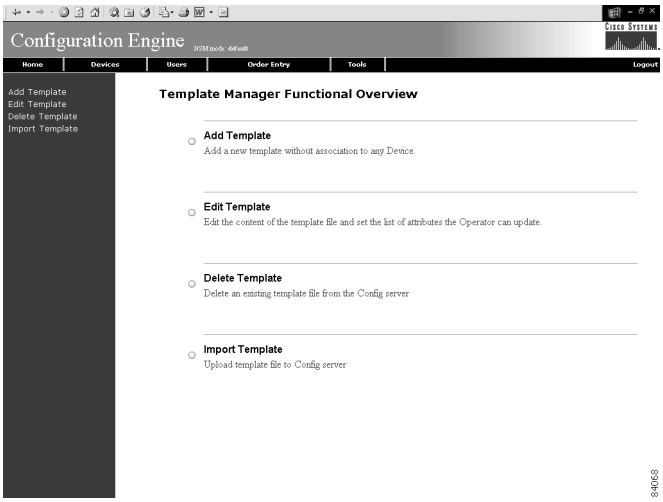
The parameter, `${LDAP://this:attrName=IPsubTemplate}` contains the location of the file.

# How to Manage Templates

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

The Template Manager page appears (see Figure 3-55).

***Figure 3-55 Template Manager***




## 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.

**Step 2** To choose the attributes you want to be included in this template, use the **Attributes** menu.

**Step 3** Enter the filename for this template in the **Template File** field.

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

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

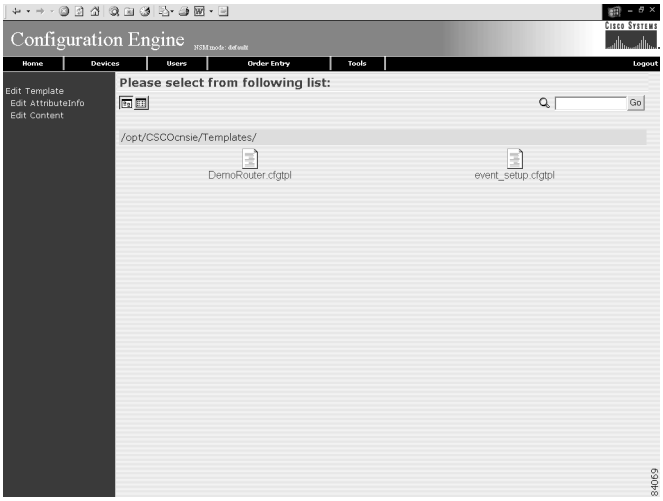
## How to Edit a Template

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 Template list appears (see Figure 3-56).

*Figure 3-56 Template List*




**Step 2** Click on the icon for the template file you wish to edit.

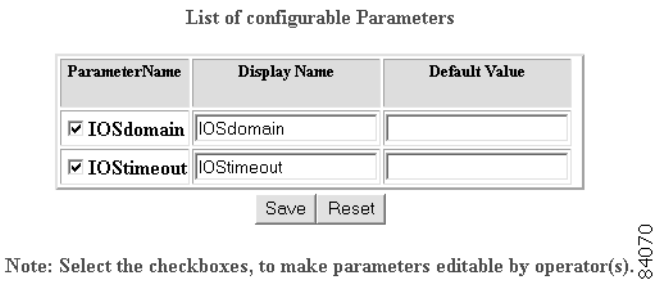
The template file appears.

**Step 3** To edit parameters (attribute information), follow these steps:

**a.** From the template file page, click **Edit AttributeInfo**.

The list of configurable parameters appears (see Figure 3-57).

*Figure 3-57 Parameter Editor*




**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**.

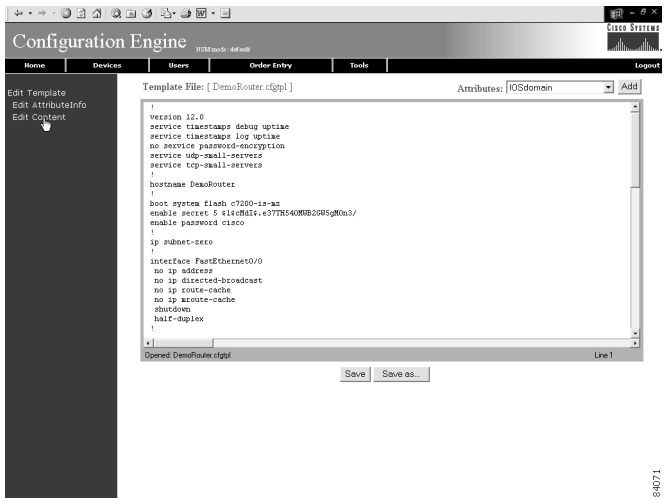
**e.** To return to the main menu, click on the **Tools** tab.

**Step 4** 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 3-58).

*Figure 3-58 Template Content*




**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 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 (see Figure 3-55), click **Delete Template**.

The template file list appears (see Figure 3-56).

**Step 2** Select the template you wish to delete.

**Step 3** Delete the desired template file.

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

# Security Manager

With the security manager tool you can change the bootstap 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 3-59).

***Figure 3-59 Security Manager***

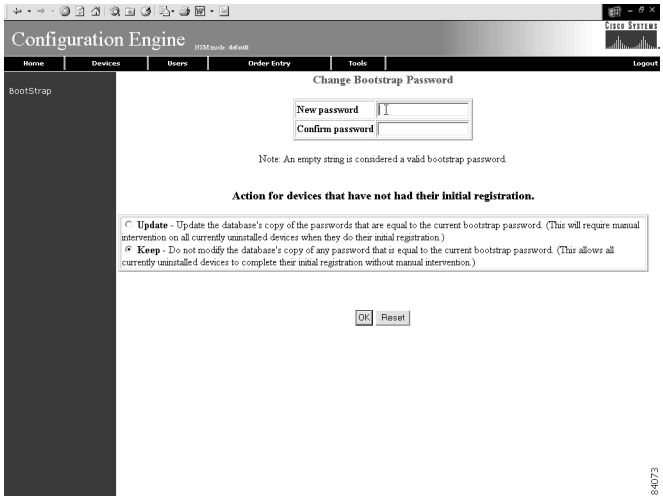

## How to Change Bootstrap Password

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 3-60).

*Figure 3-60 Change Bootstrap Password*




**Step 2** In the password dialog box, enter the new password.

**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 main menu, click on the **Tools** tab.

# Backup and Restore

This section explains how to backup and recover your directory store, templates, and certain configuration files.

## Backup

The backup function is a script that takes the values you enter in the dialog box for scheduling backups under the Directory Manager (**Tools > Directory Mgr. > ScheduleBackup**) in the Configuration Registrar (see "How to Schedule Data Backup" section on page 3-34).

### How the Backup Works

The backup sequence is as follows:

1. The backup script invokes backup commands for CNS Directory Service, template, and other configuration files.

   When the script backs up CNS Directory Service, it sets the directory in an inactive state until the backup completes.

2. When CNS Directory Service backup completes, the script restarts the directory server.

The script stores the database file in the `/extra` partition of the CNS 2100 Series system drive. All other files (templates, http.conf, jserv.properties, and so on) are saved as tar [tape archive] files, then zipped with the CNS Directory Service backup.

3. The zip file is sent, by means of FTP, to the server location specified by the Directory Manager ("How to Schedule Data Backup" section on page 3-34).
4. The file is copied to the `/extra/old` directory on the local CNS 2100 Series system.

   The `/extra/old` directory contains only one previous backup. Each backup operation overwrites this space with the new backup data.

# Restore

To restore CNS Directory Service, template, and other configuration files to the CNS 2100 Series system, complete the following steps:

**Step 1** Verify that the CNS 2100 Series system has IP connectivity.

For example, use the console interface to ping a known device on the network, such as the file server that has the backup file.

**Step 2** Locate the backup file.

**Step 3** Use FTP to transfer the backup file to the local / partition.

The backup file is in a zip format.

**Step 4** Type the command:

**zcat <*filename*>.gz | tar xvf -**

where <*filename*> consists of a date/time notation. For example,
`backup<date_and_timestamp_of_backup>`

## How to Restore the CNS Directory

To restore the CNS directory, complete these steps:

**Step 1** Recompile and load the CNS directory schema by using the command:

**su - dcdadmin -c /opt/CSCOcnsie/scripts/dclschemaload.txt**

This command will fail if the CNS directory server is not running.

**Step 2** Stop the CNS directory server by using the command:

**su - dcdadmin -c dcdstop**

(If the command fails, try running: **/etc/rc.d/init.d/NetAppDCL stop**)

**Step 3** Restore the CNS Directory Service data (DIB) from the /extra directory that contains the DATABASE.DAT file with:

**su - dcdadmin -c "dcbckdib /y restore /extra"**

**Step 4** Start the CNS directory server with the command:

**su - dcdadmin -c dcdstart**

**Step 5** Restart the HTTP and IMGW services with the commands:

**/etc/rc.d/init.d/httpd restart**

**/etc/rc.d/init.d/Imgw restart**


# Cisco CNS Configuration Engine Administration for External Directory Mode

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

- How to Log In and Out of the System
- How to View, Re-synchronize, and Update Devices
- Tools

# How to Log In and Out of the System

You can connect to the system by means of:

- Telnet
- System console

## How to Log In

To log into 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 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 4-1).

*Figure 4-1 Logging In to the Configuration Server*


**Step 3** Enter your **User ID**.

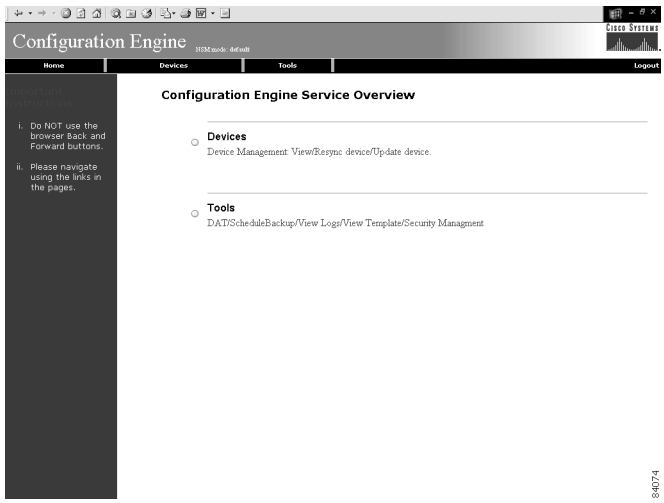
This is the user name for the Cisco CNS Configuration Engine administrative account that you entered during **Setup**.

**Step 4** Enter your password.

**Step 5** Click **LOGIN**.

The Cisco CNS Configuration Engine Home page for External Directory mode appears (see Figure 4-2).

*Figure 4-2 Cisco CNS Configuration Engine External Directory Mode Home Page*



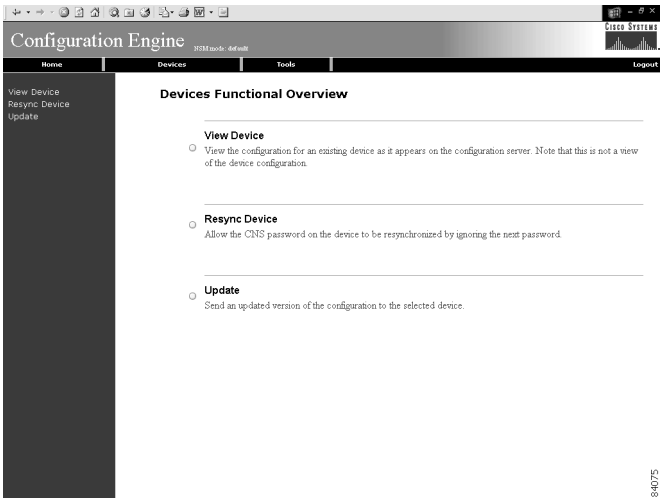

# How to Log Out

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

# 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 4-3).

***Figure 4-3 Devices Page***




# How to View Device Configuration

To view a device configuration, follow these steps:

**Step 1** From the Home page (Figure 4-2), click on the **Devices** tab.

**Step 2** From the Devices Functional Overview page (Figure 4-3), 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 4-2), click on the **Devices** tab.

**Step 2** From the Devices Functional Overview page (see Figure 4-3), 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 4-2), click on the **Devices** tab.

**Step 2** From the Devices Functional Overview page (Figure 4-3), 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 4-4)

***Figure 4-4 Update Task***


**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

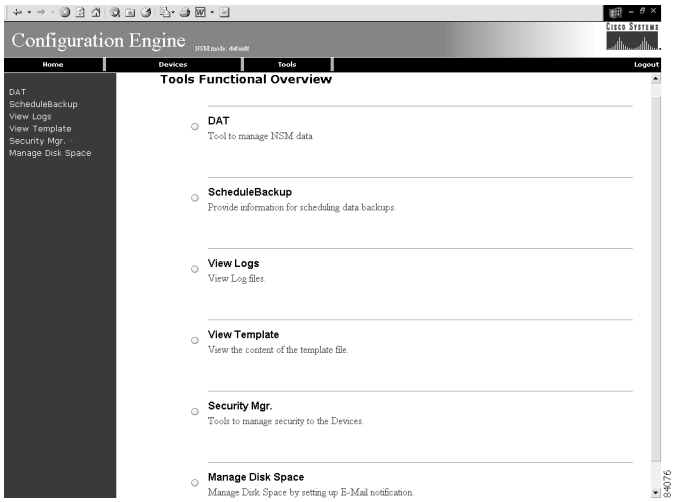
To use the tools feature, from the Home page, click on the **Tools** tab.

The Tools page appears (see Figure 4-5).

From the Tools page, you can access the following functions:

- DAT
- Schedule Backup
- View Logs
- View Templates
- Security Manager
- Manage Disk Space

***Figure 4-5 Tools Functional Overview***




# How to Use DAT

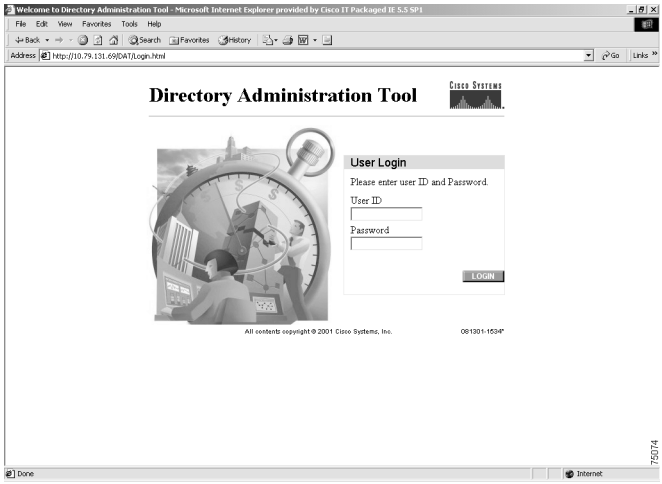
To connect to the user interface for the Directory Administration Tool (DAT), follow these steps:

**Step 1** From the Home page (Figure 4-2), click on the **Tools** tab.

**Step 2** From the Tools Functional Overview page (Figure 4-5), click **DAT**.

The DAT login window appears (see Figure 4-6).

*Figure 4-6 Directory Administration Tool Login Window*




**Step 3** Enter your **User ID**.

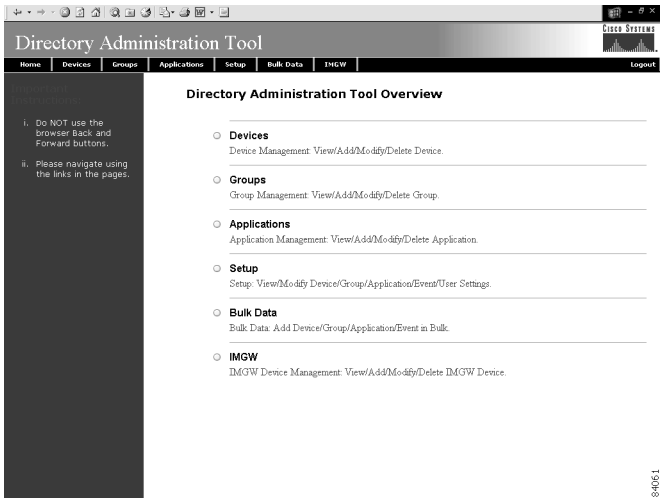
This is the LDAP proxy user name for the Cisco CNS Configuration Engine administrative account that you entered during **Setup**.

**Step 4** Enter your LDAP proxy password.

**Step 5** Click **LOGIN**.

The Directory Administration Tool Home page appears (see Figure 4-7).

*Figure 4-7 DAT Home Page*




**Step 6** From here, go to Chapter 5, "Directory Administration Tool" and follow the procedures for the tasks you want to run.

# How to Schedule Data Backup

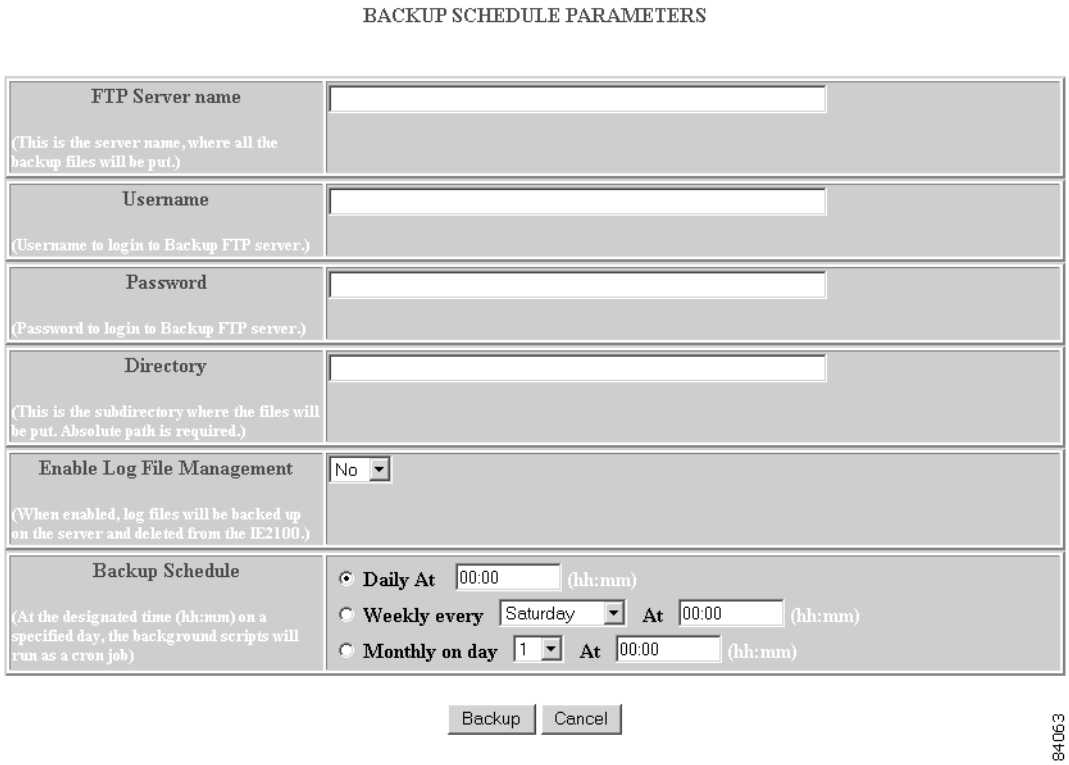
To schedule data backup, follow these steps:

**Step 1** From the Home page (Figure 4-2 on page 4-2), click on the **Tools** tab.

**Step 2** From the Tools Functional Overview page (Figure 4-5 on page 4-5), click **ScheduleBackup**.

The backup information dialog box appears (see Figure 4-8).

***Figure 4-8 Backup Schedule Parameters***




**Step 3** To specify where you want the backup data to be stored, enter the FTP server name in the **FTP Server Name** field.

**Step 4** To specify the username to log into the FTP server, enter a valid username in the **Username** field.

**Step 5** To specify the password to use to log into 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, see "Backup and Restore" section on page 3-54.

# How to View Logs

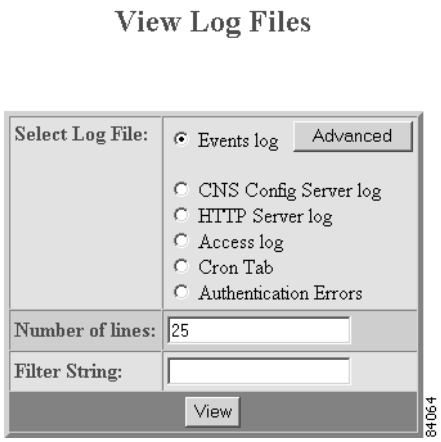
To view various log files, follow these steps:

**Step 1** From the Home page (Figure 4-2), click on the **Tools** tab.

**Step 2** From the Tools Functional Overview page (Figure 4-5), click **View Logs**.

The View Log Files dialog box appears (see Figure 4-9).

***Figure 4-9 Log File Viewer***




**Step 3** Choose the log file you want to view.

**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 4-10).

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

*Figure 4-10 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].
```

53472

# 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**.

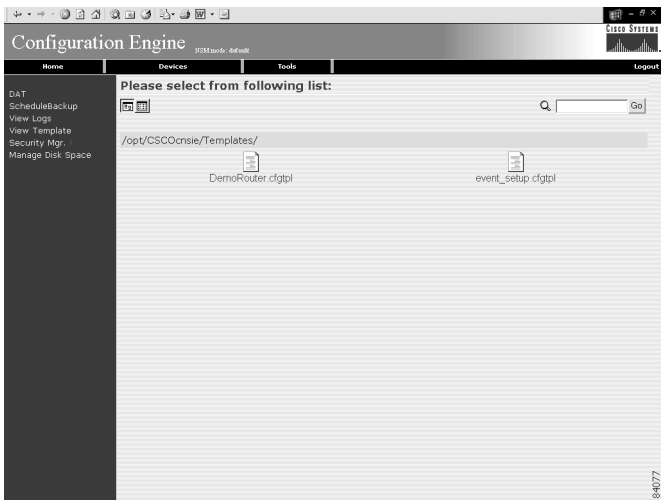
The Template page appears (see Figure 4-11).

**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 4-11 Template List*



# Security Manager

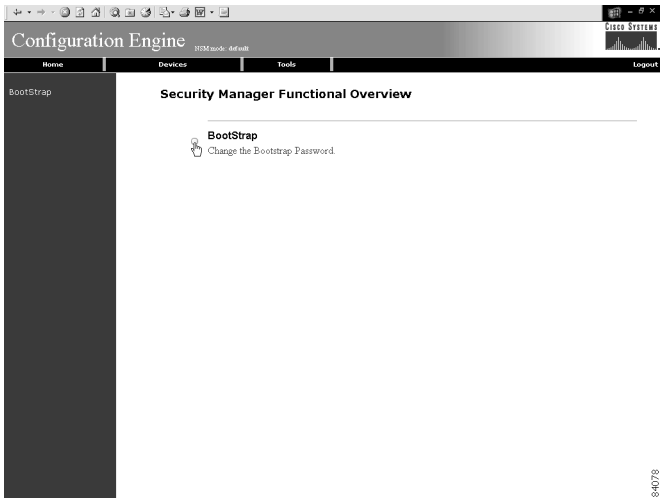
With the security manager tool you can change the bootstap password.

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 4-12).

***Figure 4-12 Security Manager***




## How to Change Bootstrap Password

To change the bootstrap password, follow these steps:

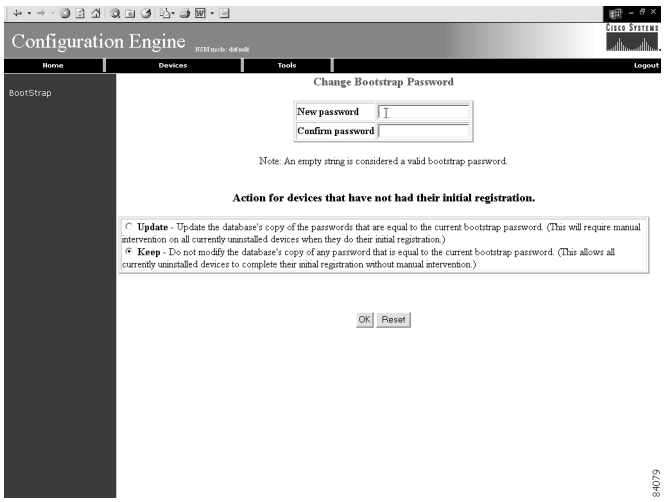
**Step 1** From the Home page, click on the **Tools** tab.

**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 4-13).

*Figure 4-13 Change Bootstrap Password*




**Step 4** In the password dialog box, enter the new password.

**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

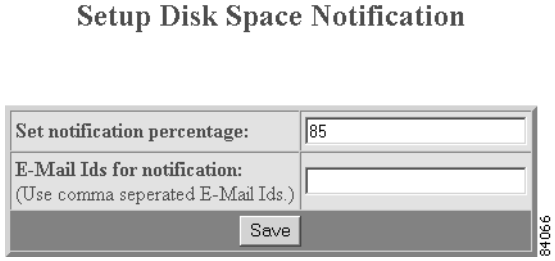
To setup disk space e-mail notification of disk space usage, follow these steps:

**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 4-14).

*Figure 4-14 Disk Space Notification*




**Step 3** Set the notification percentage to the value that triggers an e-mail notification.

**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.


# Directory Administration Tool

This chapter describes the Directory Administration Tool (DAT) including information about:

- How to Log In
- 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 1-5), 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.

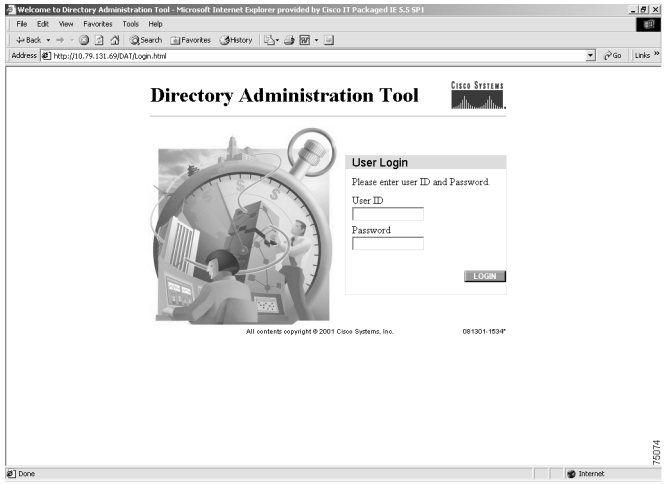
## How to Log In

To connect to the DAT user interface, follow these steps:

**Step 1** From the Tools main menu of the Cisco CNS Configuration Engine user interface, click **DAT**.

The login window appears (see Figure 5-1).

*Figure 5-1 Directory Administration Tool Login Window*




**Step 2** Enter your **User ID**.

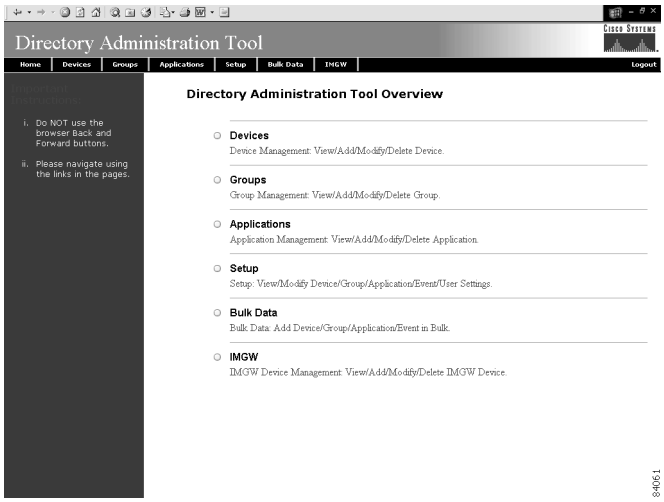
This is the user name for the Cisco CNS Configuration Engine administrative account that you entered during **Setup**.

**Step 3** Enter your password.

**Step 4** Click **LOGIN**.

The Directory Administration Tool Home page appears (see Figure 5-2).

*Figure 5-2 Directory Administration Tool Home Page*



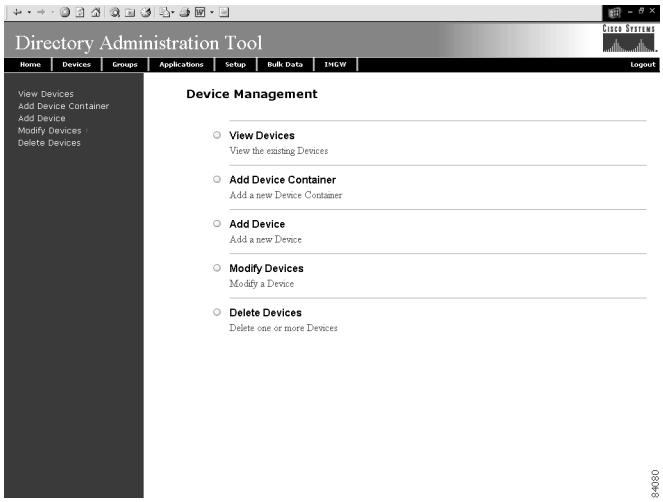

# How to Log Out

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

# How to Manage Devices

To view and modify devices, from the Home page, click **Devices**. The Device Management page appears (see Figure 5-3).

***Figure 5-3 Device Management Page***



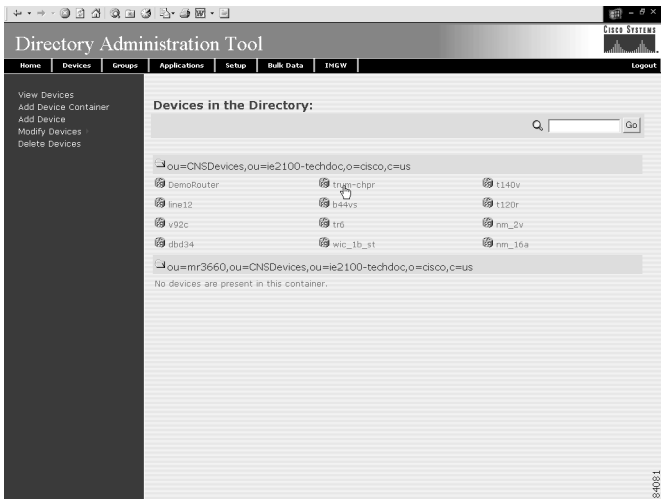

# How to View Devices in the System

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 5-4).

***Figure 5-4 Device List***



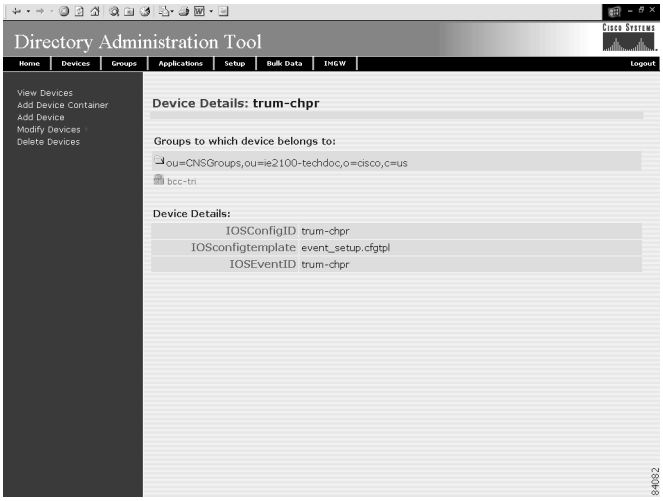
**Note** Devices with no parent attributes are shown with a dully-shaded icon, so you can easily identify the devices with no groups associated.

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

Information about that device appears (see Figure 5-5).

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

***Figure 5-5 Device Details***



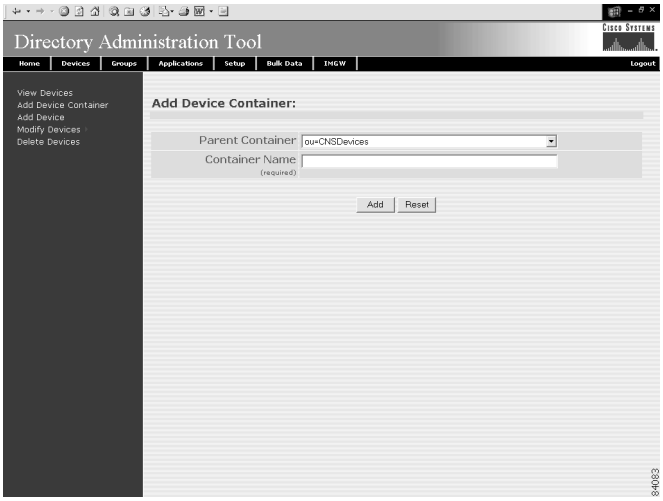

# How to Add a Device Container

To add a device container to the system, follow these steps:

**Step 1** From the Device Management page, click **Add Device Container**.

The Add Device Container page appears (Figure 5-6).

*Figure 5-6 Add Device Container*




**Step 2** Enter a value in the **Container Name** field.

**Step 3** To clear the field and enter a new value, click **Reset**.

**Step 4** To add this device container, click **Add**.

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

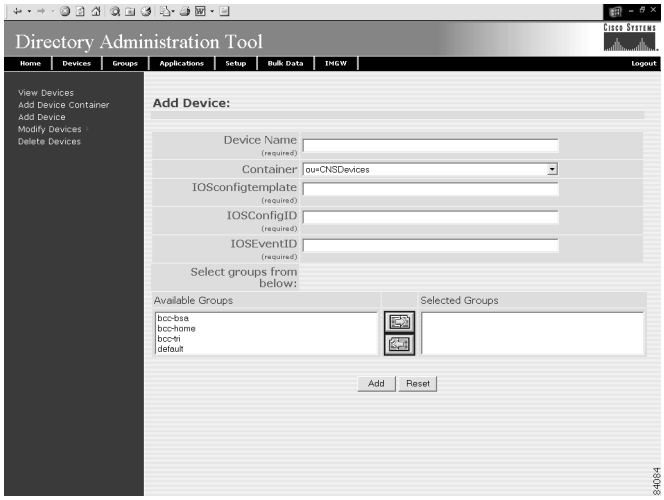
# How to Add a Device

To add a device to the system, follow these steps:

**Step 1** From the Device Management page, click **Add Device**.

The Add Device page appears (see Figure 5-7)

*Figure 5-7 Add Device*




**Step 2** Enter a value in the **Device Name** field.

**Step 3** Select a container from the Container pull-down menu.

**Step 4** Enter a template ID for this device in the **IOSConfigtemplate** field.

**Step 5** Enter a value for the unique configuration ID in the **IOSConfigID** field.

**Step 6** Enter a value for the unique event ID in the **IOSEventID** field.

**Step 7** From the **Available Groups** list, select the groups into which this device belongs.

**Step 8** To clear all field and enter new values, click **Reset**.

**Step 9** To add this device to the system, click **Add**.

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

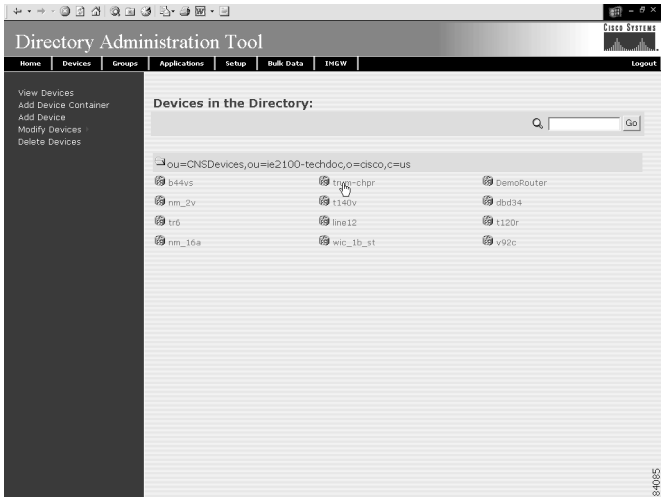
# How to Modify Devices Details

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 5-8).

***Figure 5-8 Devices in the Directory***

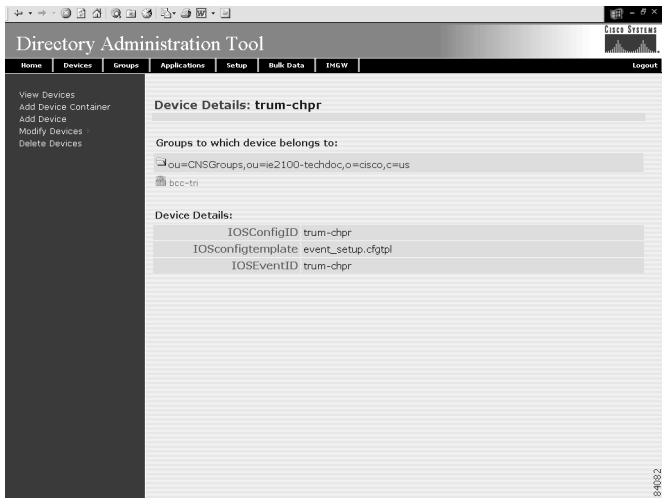



**Note** Devices with no parent attributes are shown with a dully-shaded icon, so you can easily identify the devices with no groups associated.

**Step 2** Click on the icon for the device you wish to modify.

The Device Details page appears (see Figure 5-9)

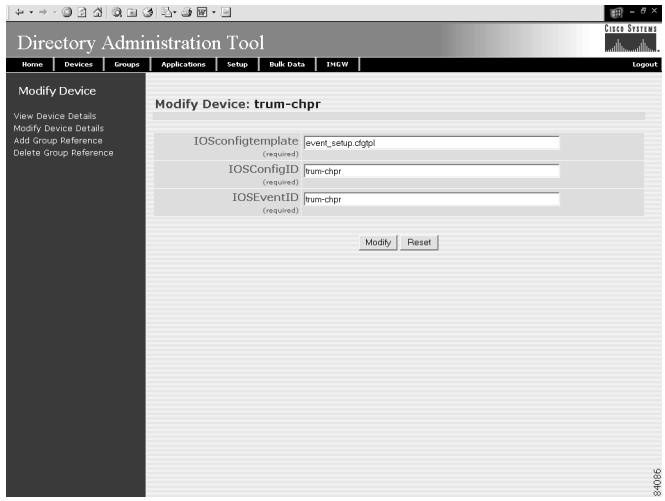
*Figure 5-9 Device Details*




**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 5-10).

*Figure 5-10 Modify Task*




**Step 4** Modify all appropriate fields.

**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.

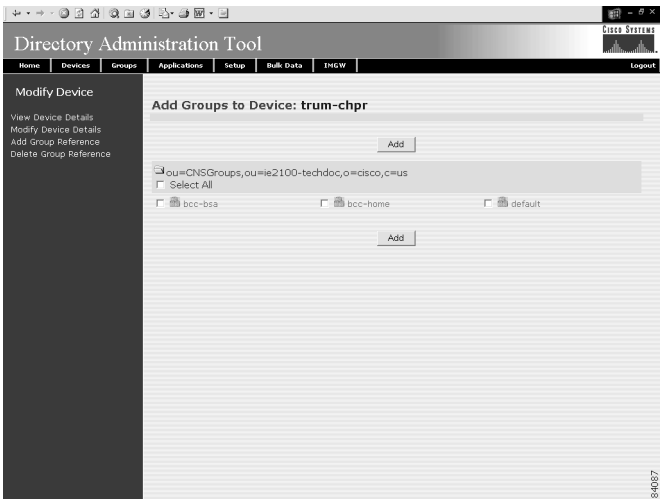
## How to Add Device Group References to a Device

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 5-11).

***Figure 5-11 Add Groups to Device***




**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.

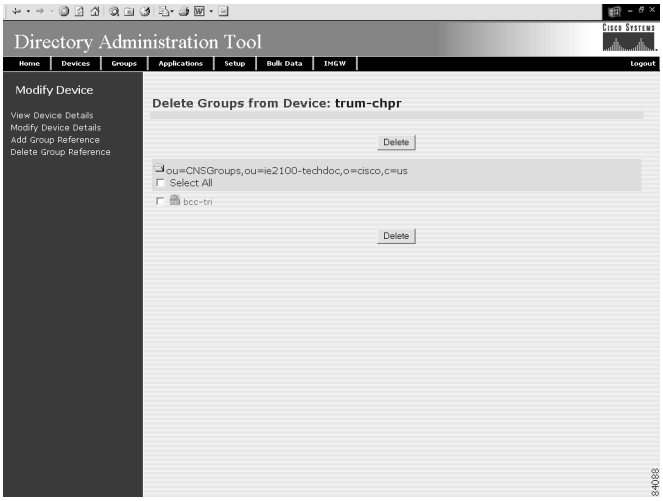
## How to Delete Device Group References to a Device

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 5-12).

*Figure 5-12 Delete Devices from Group*




**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 DCL, if the device is the only member of a group when you delete the device, the associated group is also deleted. This is because the group is now empty.

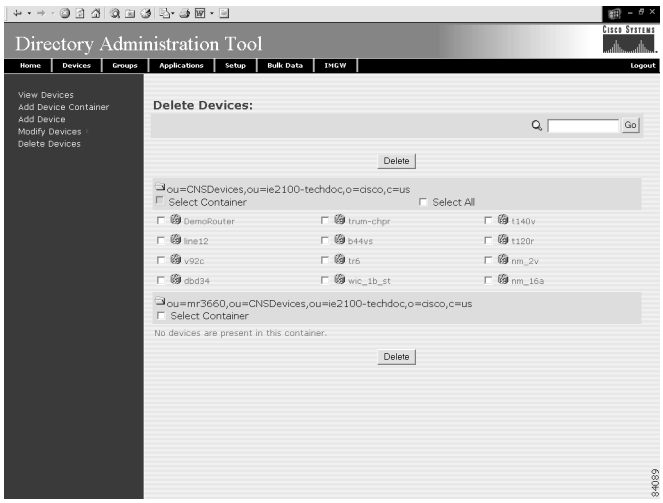
For AD, NDS, and iPlanet, if the device is the only member of a group when you delete the device, the group remains in an empty state. However, the device reference is deleted from the group.

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 5-13)

***Figure 5-13 Delete Devices***




**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**.

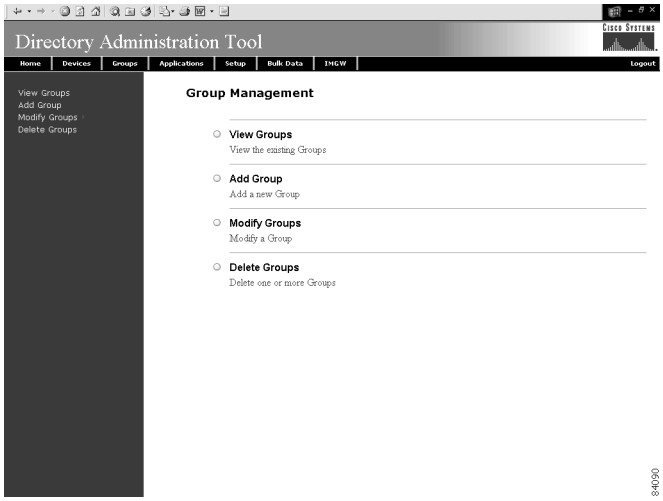
**Step 4** To return to the main menu, click the **Home** tab.

# How to Manage Groups

To view and modify groups, from the main menu, click the **Groups** tab.

The Group Management page appears (see Figure 5-14).

*Figure 5-14 Group Management*



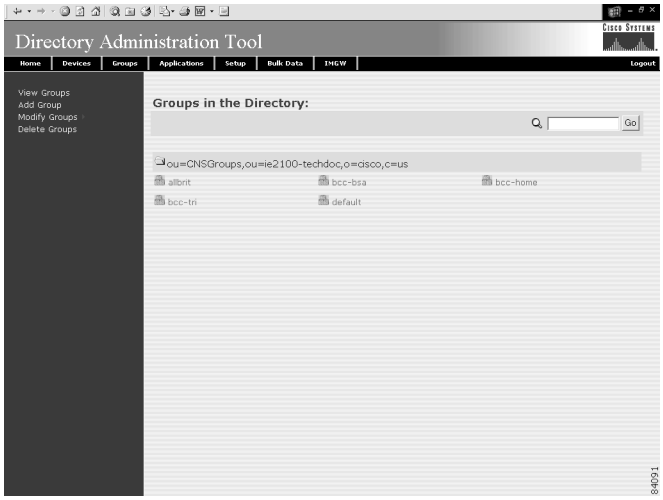

# How to View Groups in the System

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 5-15).

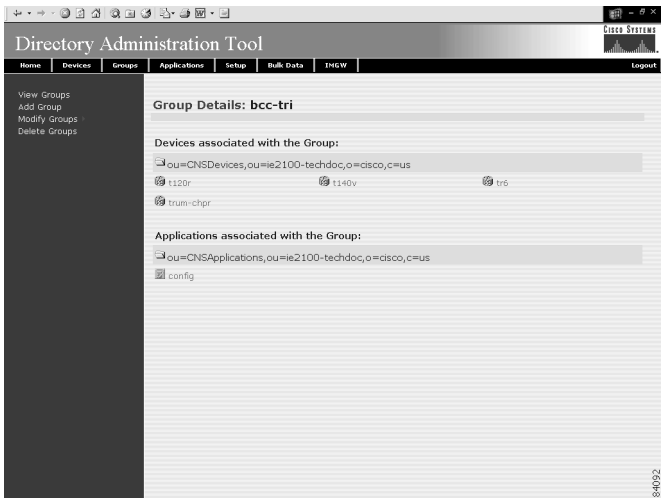
*Figure 5-15 Groups in the System*




**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 5-16).

*Figure 5-16 Groups Details*




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

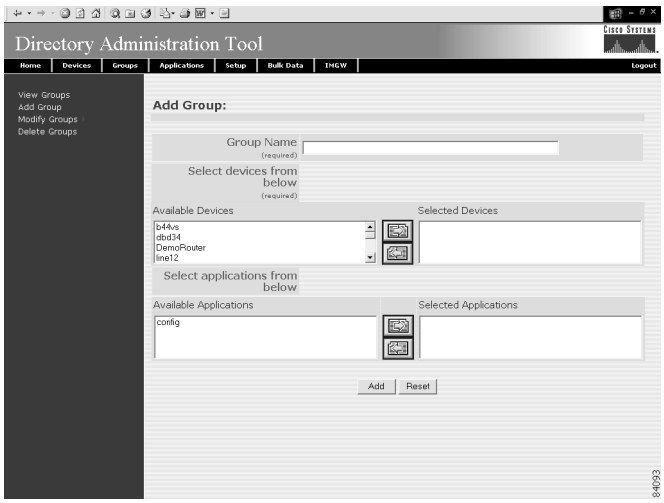
# How to Add a Group

To add a group to the system, follow these steps:

**Step 1** From the Group Management page, click **Add Group**.

The Add Group page appears (see Figure 5-17).

*Figure 5-17 Add Group*




**Step 2** Enter a value for the group name in the **Group Name** field.

**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 5-15).

**Step 2** Click on the icon associated with the group you want to modify.

The group details appear (see Figure 5-16).

**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 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 5-31.)

**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 5-15).

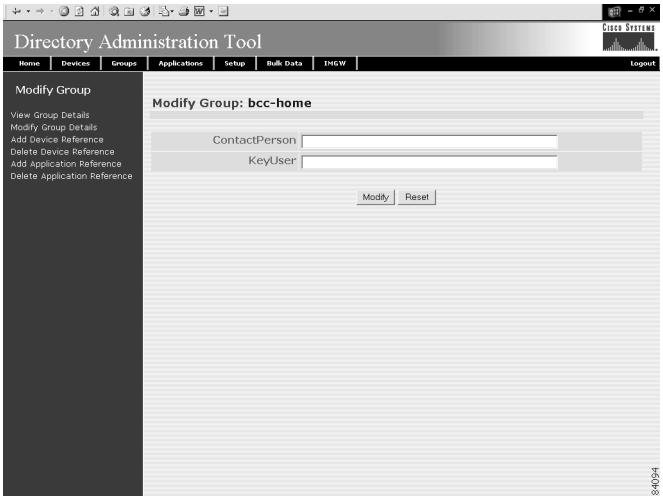
**Step 2** Click on the icon associated with the group you want to modify.

The Group Details page appears (see Figure 5-16).

**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 5-18).

***Figure 5-18 Modify Group Details***




**Note** The attributes shown in Figure 5-18 are sample values used only for illustration purposes. For more information about adding attributes to the directory, see "How to Modify Group Details" section on page 5-14.

**Step 4** Modify all appropriate attributes.

**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**.

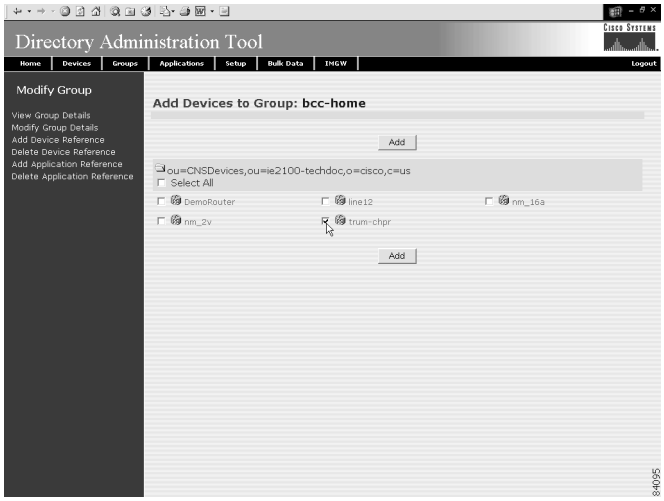
The group list appears (see Figure 5-15).

**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 5-19).

*Figure 5-19 Add Devices to Group*




**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:

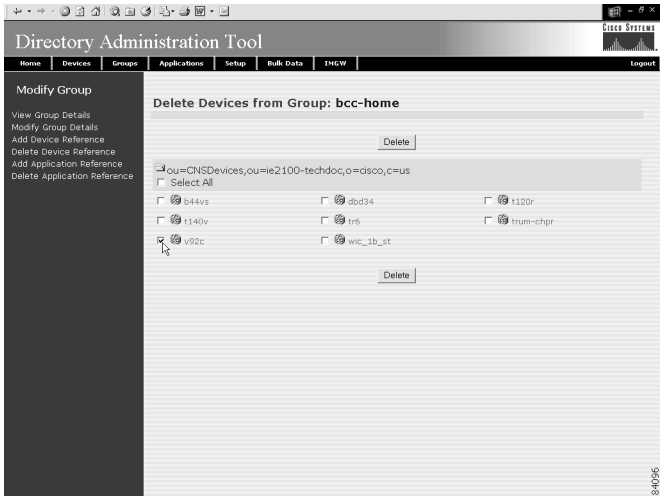
**Step 1** From the Group Management page, click **Modify Groups**.

The group list appears (see Figure 5-15).

**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 5-20).

*Figure 5-20 Delete Devices from Group*




**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**.

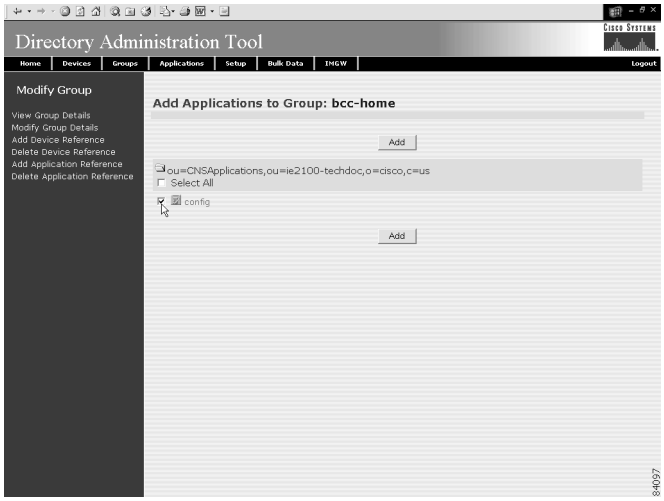
The group list appears (see Figure 5-15).

**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 5-21).

*Figure 5-21 Add Applications to Group*




**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:

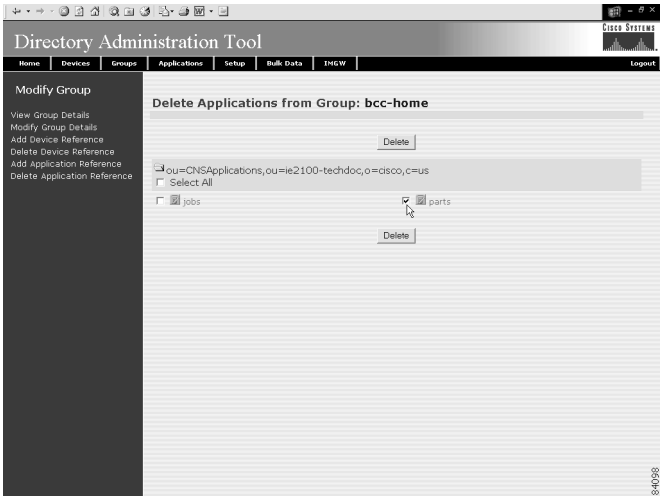
**Step 1** From the Group Management page, click **Modify Groups**.

The group list appears (see Figure 5-15).

**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 5-22).

*Figure 5-22 Delete Applications from Group*




**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**.

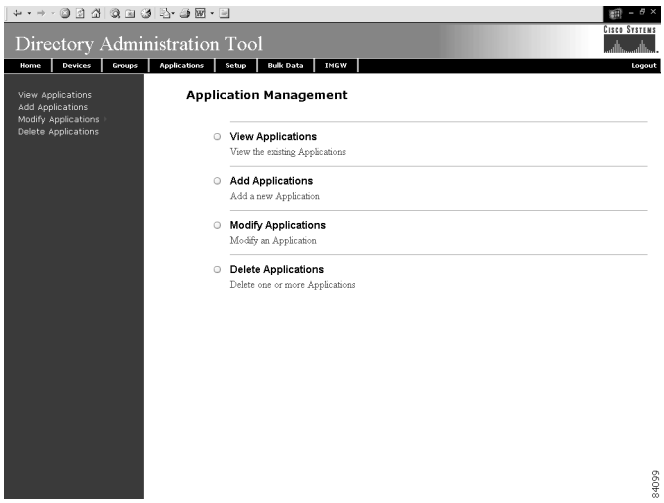
**Step 4** To return to the main menu, click the **Home** tab.

# How to Manage Applications

To view and modify applications, from the main menu, click the **Applications** tab.

The Application Management page appears (see Figure 5-23).

***Figure 5-23 Application Management***



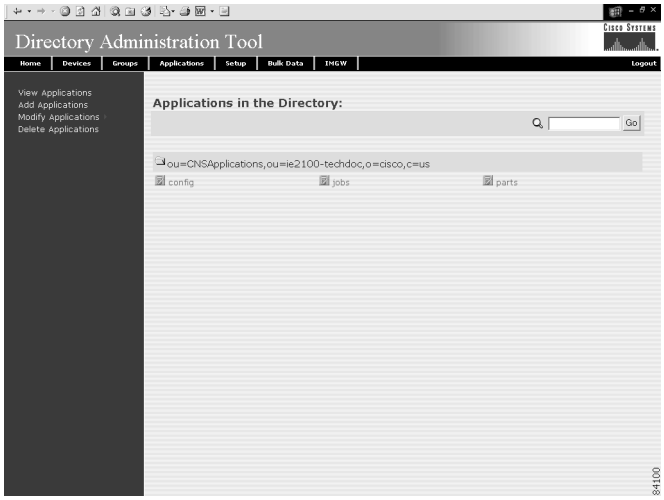

# How to View Applications on the System

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 5-24).

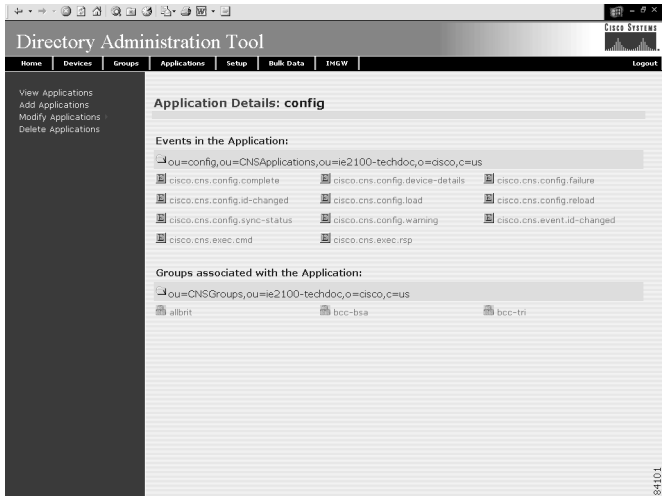
*Figure 5-24 Applications List*




**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 5-25) listing the events in the application and group currently associated with this application.

*Figure 5-25 Application Details*




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

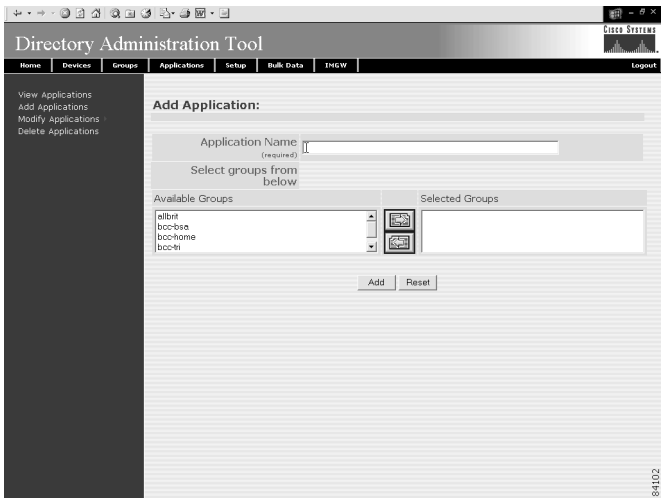
# How to Add Applications

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 5-26).

*Figure 5-26 Add Applications*




**Step 2** Enter a value in the **Application Name** field.

**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 5-24).

**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 5-24).

**Step 2** Click on the icon associated with the application you want to modify.

The application details appear (see Figure 5-25).

**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 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 5-32.)

**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**.

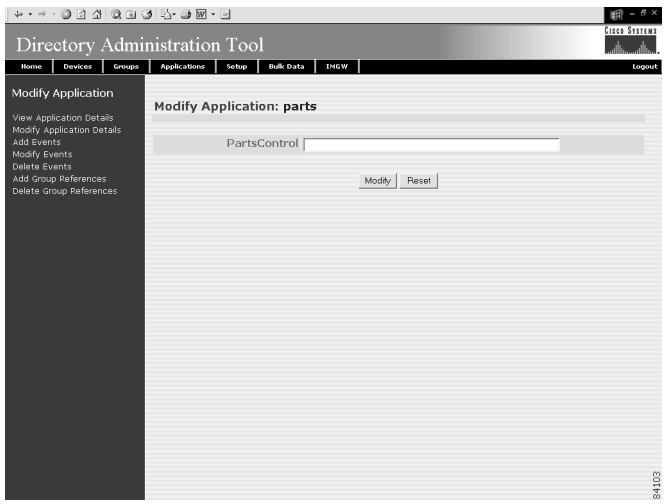
## How to Modify Application Details

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 5-27 Modify Application Details***




**Note** The attribute shown in Figure 5-27 is a sample value used only for illustration purposes. For more information about adding attributes to the directory, see "How to Populate an Application Attribute" section on page 5-23.

**Step 2** Modify all appropriate attributes.

**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.

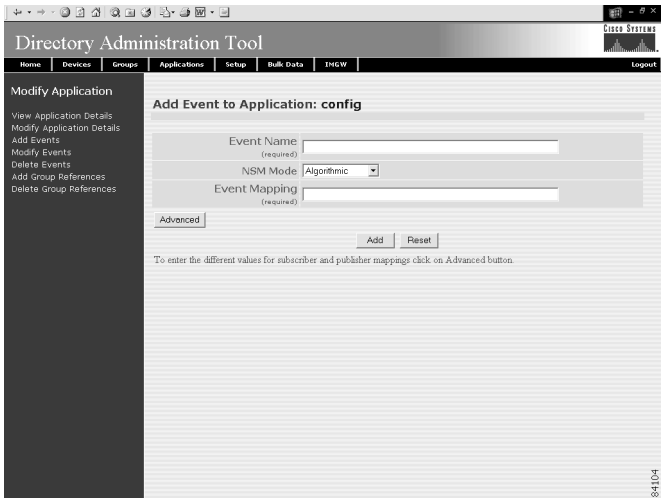
## How to Add Events to an Application

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 5-28).

***Figure 5-28 Add Events to an Application***




**Step 2** Enter a value in the **Event Name** field.

All the events that are added in the internal directory for **config** application are as follows:

```
cisco.cns.config.load
cisco.cns.config.complete
cisco.cns.config.warning
cisco.cns.config.failure
cisco.cns.config.sync-status
cisco.cns.exec.cmd
cisco.cns.exec.rsp
cisco.cns.config.id-changed
cisco.cns.config.reload
cisco.cns.config.device-details
cisco.cns.event.id-changed
```

**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

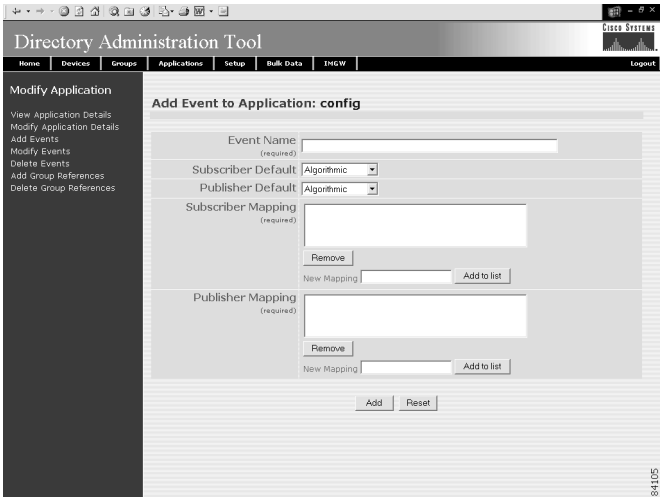
**Step 4** Enter the event mapping in the **Event Mapping** field.

For more information about naming events, see "NameSpace Mapper" section on page 1-4.

**Step 5** To change Subscriber and Publisher parameters from default, click **Advanced**.

The Advanced Event page appears (see Figure 5-29).

***Figure 5-29 Advanced Event Add***




**Step 6** Select the Subscriber Default mode from the pull down menu.

**Step 7** Select the Publisher Default mode from the pull down menu.

**Step 8** To add a new subscriber mapping, enter the subscriber mapping in the **New Mapping** field, the click **Add to list**.

**Step 9** To remove a subscriber mapping, in the **Subscriber Mapping** list, select the desired mapping, then click **Remove**.

**Step 10** To add a new publisher mapping, enter the publisher mapping in the **New Mapping** field, the click **Add to list**.

**Step 11** To remove a publisher mapping, in the **Publisher Mapping** list, select the desired mapping, then click **Remove**.

**Step 12** To add this event to the system, click **Add**.

**Step 13** To clear your entries and start over, click **Reset**.

**Step 14** 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 5-24).

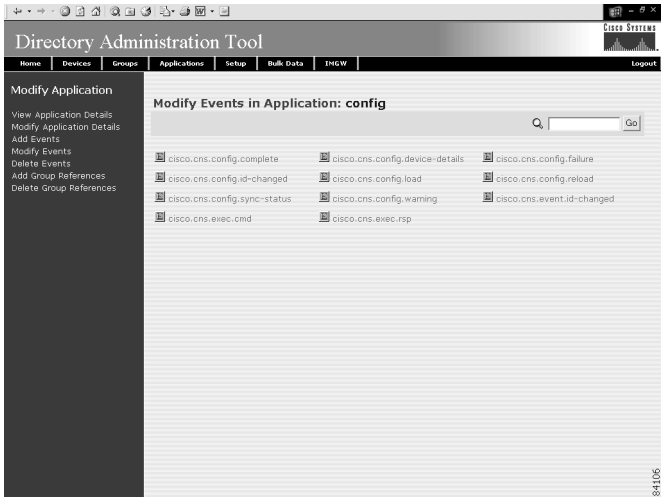
**Step 2** Click on the icon associated with the application for which you want to modify events.

The Application Details page appears (see Figure 5-25).

**Step 3** From the left side-bar menu, click **Modify Events**.

The events list for this application appears (see Figure 5-30).

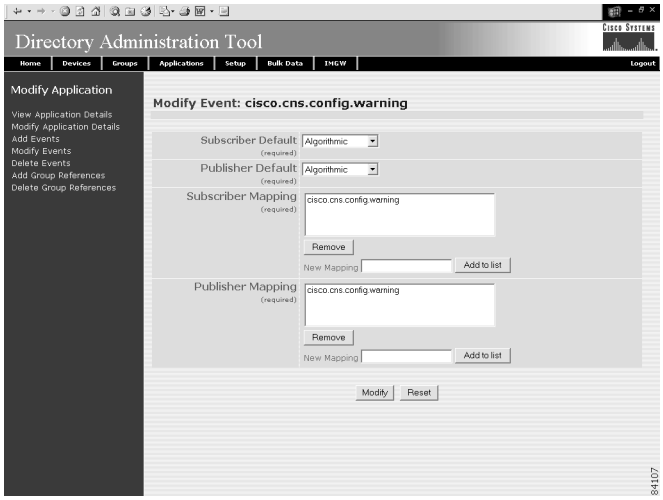
*Figure 5-30 Modify Events in Application*




**Step 4** Click on the icon associated with the event you want to modify.

The Modify Event page appears (see Figure 5-31).

*Figure 5-31 Modify Event*




**Step 5** Modify all appropriate fields.

**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 5-24).

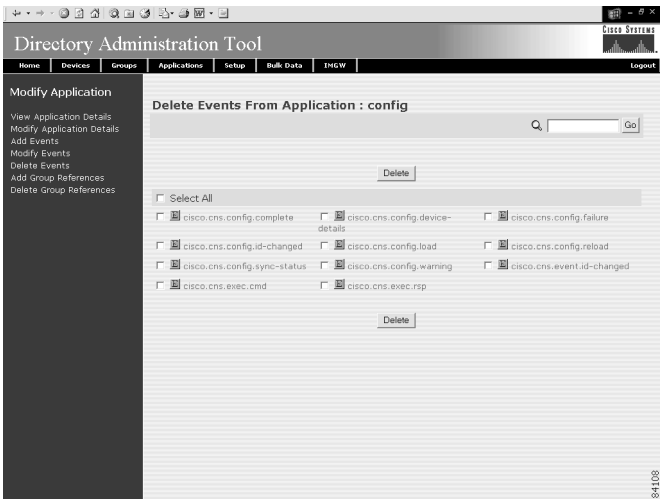
**Step 2** Click on the icon associated with the application from which you want to delete events.

The Application Details page appears (see Figure 5-25).

**Step 3** From the left side-bar menu, click **Delete Events**.

The delete events list for this application appears (see Figure 5-32).

***Figure 5-32 Delete Events from Application***




**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 5-24).

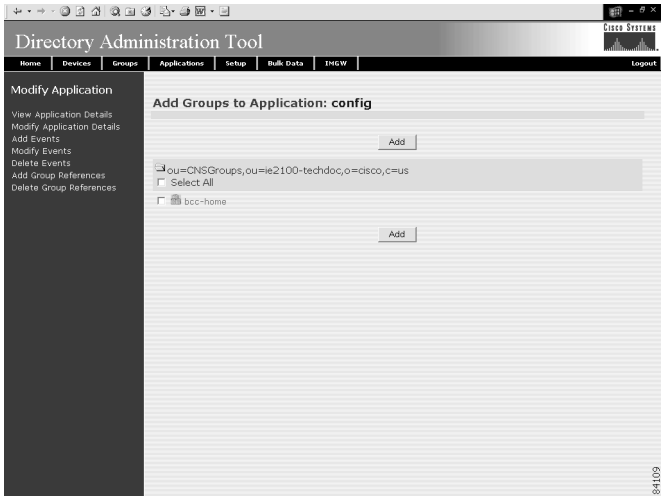
**Step 2** Click on the icon associated with the application from which you want to add groups.

The Application Details page appears (see Figure 5-25).

**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 5-33).

*Figure 5-33 Add Groups to an Application*




**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 5-24).

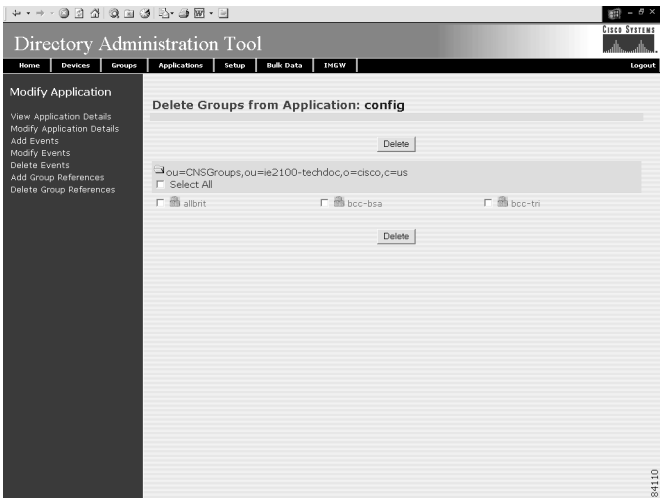
**Step 2** Click on the icon associated with the application from which you want to delete groups.

The Application Details page appears (see Figure 5-25).

**Step 3** From the left side-bar menu, click **Delete Group References**.

A list of groups currently associated with this application appears (see Figure 5-34).

*Figure 5-34 Delete Groups from an Application*




**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 5-24).

**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

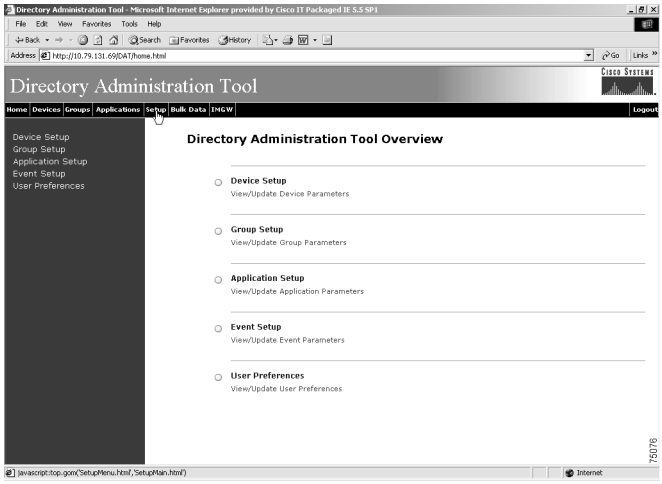
When the Cisco CNS Configuration Engine is setup, DAT also gets configured with the values as entered by the user during setup. If you have extended the schema, then you have to provide the information about the new attributes (name of the attribute, whether the attribute is mandatory or not, and whether 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 5-35).

***Figure 5-35 Setup Page***



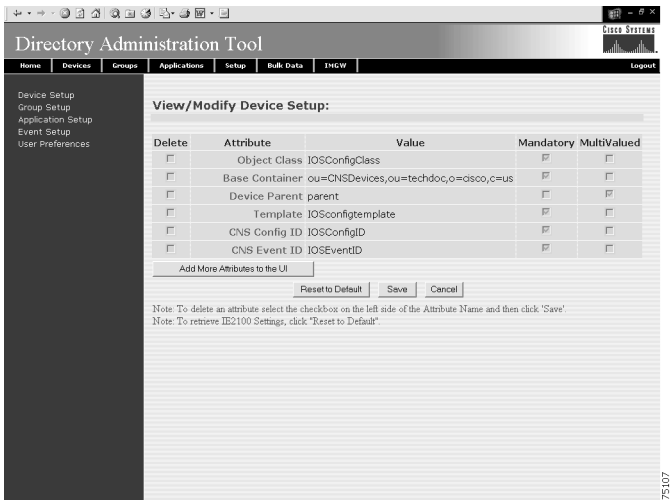

# How to View and Modify Device Setup

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 5-36).

***Figure 5-36 View and Modify Device Setup***




**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 setup. These attributes are made mandatory. To change any of these values, the Cisco CNS Configuration Engine 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 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.

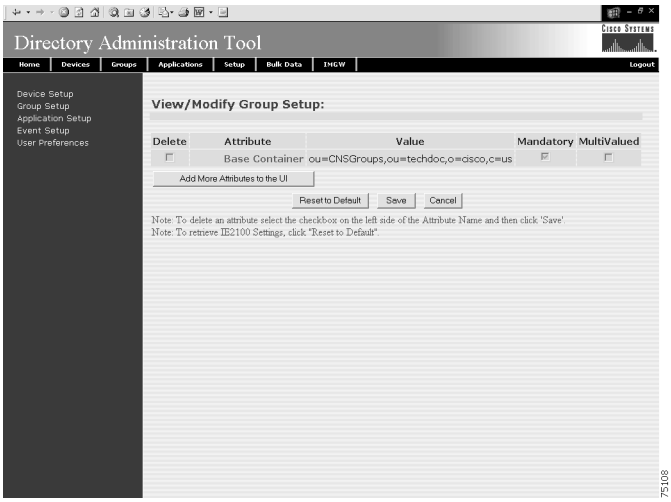
# How to View and Modify Group Setup

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 5-37).

***Figure 5-37 View and Modify Group Setup***



**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 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.

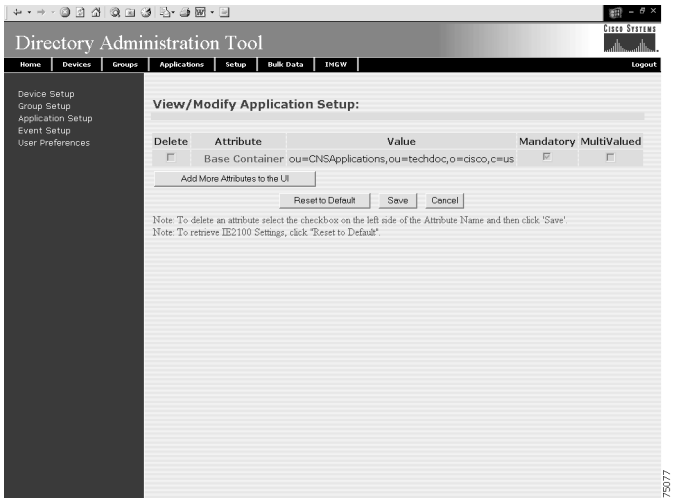
# How to View and Modify Application Setup

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 5-38).

***Figure 5-38 View and Modify Application Setup***




**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 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.

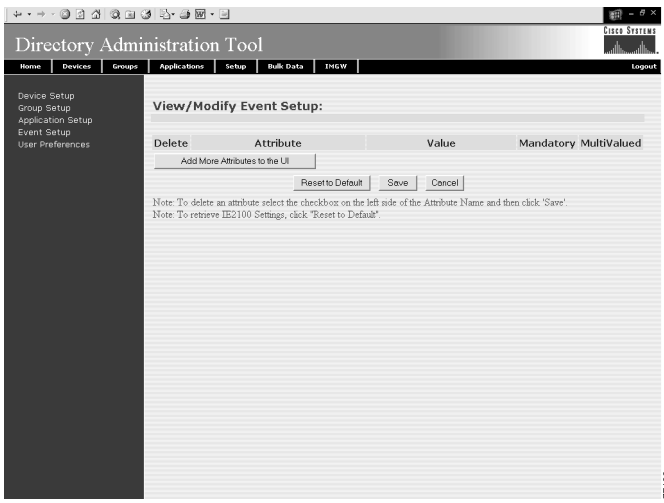
# How to View and Modify Event Setup

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 5-39).

***Figure 5-39 View and Modify Event Setup***




**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.

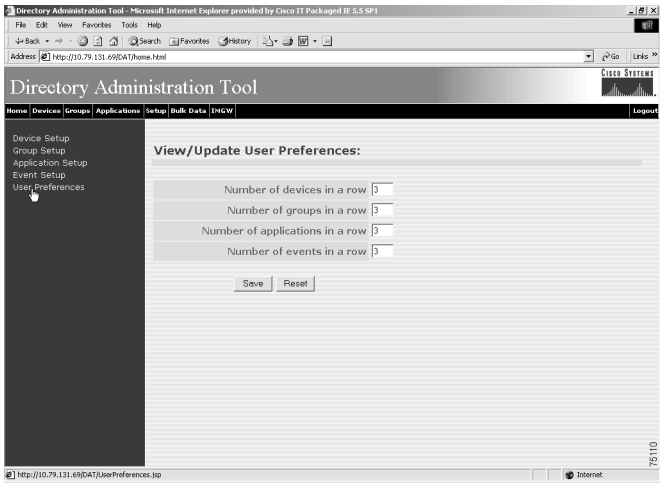
# How to View and Modify User Preferences

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 5-40).

***Figure 5-40 View and Modify User Preferences***




**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**.

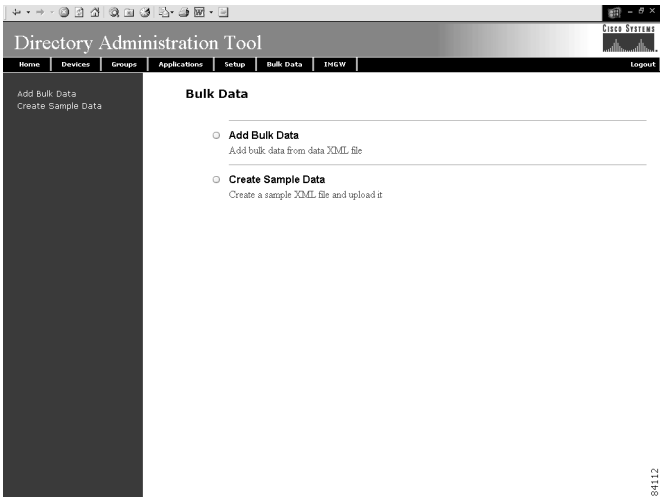
**Step 5** To return to the main menu, click the **Home** tab.

# 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 5-41).

***Figure 5-41 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)>
<!ELEMENT IMGW-DATA (imgw-device*)>
<!ATTLIST IMGW-DATA
    op-type (add) #REQUIRED
>
<!ELEMENT imgw-device (device-id, gateway-id?, hop-information*)>
<!ELEMENT device-id (#PCDATA)>
<!ELEMENT gateway-id (#PCDATA)>
<!ELEMENT hop-information (device-type, ip-address?, port?, username?, password?)>
<!ELEMENT device-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?)>
<!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 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
>
```

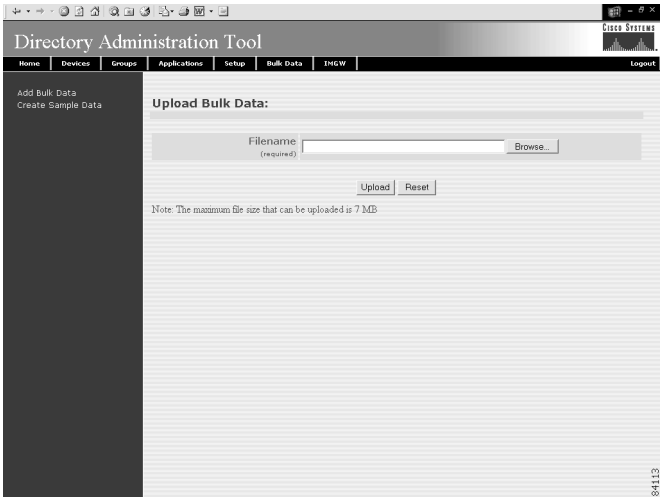
# How to Upload Bulk Data

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 5-42).

***Figure 5-42 Upload Bulk Data***




**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.

**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 5-35) 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.

## 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>
```

## IMGW Data Sample

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>SampleIMGWDevice1</device-id>
                <gateway-id>SampleIMGWGatewayID1</gateway-id>
            </imgw-device>
            <imgw-device>
                <device-id>SampleIMGWDevice2</device-id>
                <gateway-id>SampleIMGWGatewayID2</gateway-id>
                <hop-information>
                    <device-type>IOS_LOGIN</device-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>Sampleusr2</username>
                    <password>Samplepwd2</password>
                </hop-information>
            </imgw-device>
            <imgw-device>
                <device-id>SampleIMGWDevice3</device-id>
                <gateway-id>SampleIMGWGatewayID3</gateway-id>
                <hop-information>
                    <device-type>IOS_LOGIN</device-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>Sampleusr3</username>
                    <password>Samplepwd3</password>
                </hop-information>
                <hop-information>
                    <device-type>IOS_LOGIN</device-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>Sampleuser3</username>
                    <password>Samplepasswd3</password>
                </hop-information>
            </imgw-device>
            <imgw-device>
                <device-id>SampleIMGWDevice4</device-id>
                <gateway-id>SampleIMGWGatewayID4</gateway-id>
                <hop-information>
                    <device-type>IOS_LOGIN</device-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>Sampleusr4</username>
                    <password>Samplepwd4</password>
                </hop-information>
                <hop-information>
                    <device-type>IOS_LOGIN</device-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>Sampleuser4</username>
                    <password>Samplepasswd4</password>
                </hop-information>
            </imgw-device>
            <imgw-device>
                <device-id>SampleIMGWDevice5</device-id>
                <gateway-id>SampleIMGWGatewayID5</gateway-id>
```

```
                <hop-information>
                    <device-type>IOS_LOGIN</device-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>Sampleusr5</username>
                    <password>Samplepwd5</password>
                </hop-information>
                <hop-information>
                    <device-type>IOS_LOGIN</device-type>
                    <ip-address>0.0.0.0</ip-address>
                    <port>0000</port>
                    <username>Sampleuser5</username>
                    <password>Samplepasswd5</password>
                </hop-information>
            </imgw-device>
        </IMGW-DATA>
    </cns-element-data>
</cns-bulk-upload>
```

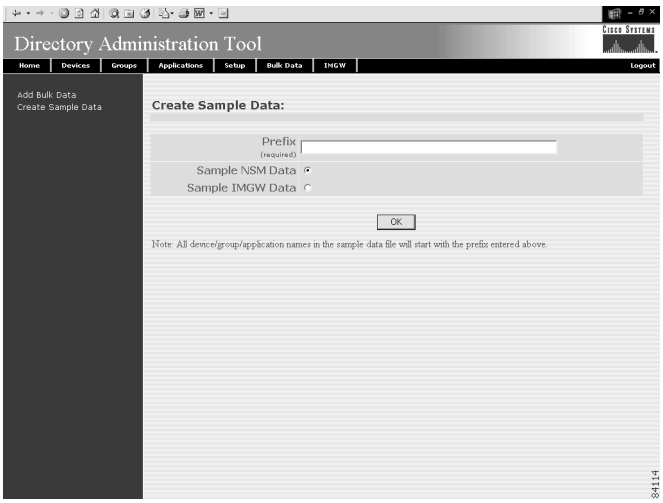
## How to Create Sample Data for Bulk Upload

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 5-43).

***Figure 5-43 Create Sample Data***




**Step 2** Enter the prefix name for this sample in the **Prefix** field.

**Step 3** Select whether this is for NSM or IMGW device.

**Step 4** To create this sample, click **OK**.

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

# 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 3-12).

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 3-42).

**Step 3** Edit template parameters for the device (see "How to Edit Device Templates" section on page 3-14).

**Step 4** Preview the configuration for the device (see "How to View Device Configuration" section on page 3-11).

**Step 5** Update the device configuration (see "How to Update a Device Configuration" section on page 3-16).

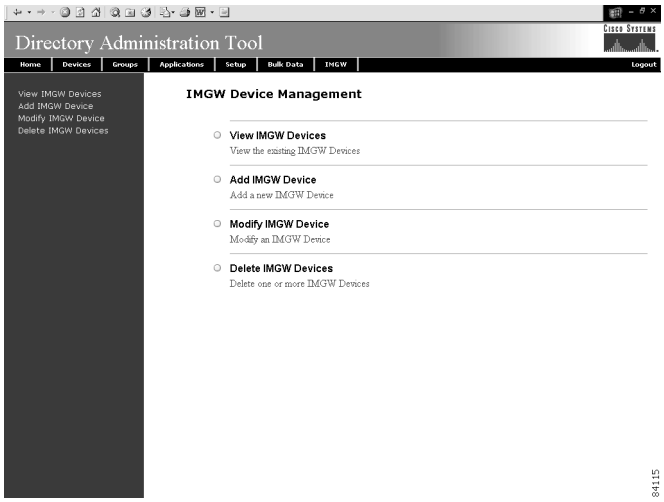
Check the response message returned by IMGW (see "How to View Log Files" section on page 3-36).

# Managing IMGW Parameters

To manage IMGW parameters, from the main menu, click the **IMGW** tab.

The IMGW main menu appears (see Figure 5-44).

***Figure 5-44 IMGW Device Management***



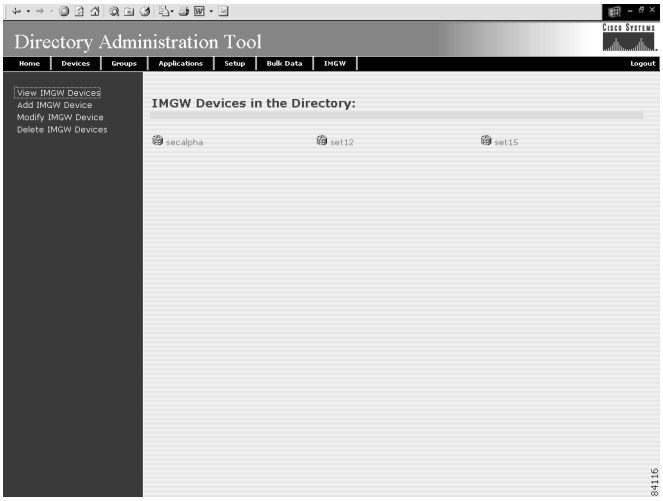
# How to View IMGW Devices

To view IMGW devices in the system, click **View IMGW Devices**.

The IMGW Devices page appears (see Figure 5-45).

You can see the details of a particular device by clicking on the device icon.

***Figure 5-45 IMGW Devices in the System***




# 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 5-46). 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 log in 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 5-1 shows the fields in the HopInfo structure:

*Table 5-1 HopInfo Structure*

| Field | Purpose |
|---|---|
| device_type | String indicating type of device. |
| ip_address | IP address of device (string) |
| port | TCP port on which to access device (integer) |
| username | Username with which to log in to device (string) |
| password | Password with which to log in to device (string) |

## Currently Supported Device Types

Table 5-2 through Table 5-9 on page 5-45 provide the HopInfo list for devices that are directly accessible on the network by IMGW. For accessing devices by way of Commserver, see Table 5-10 on page 5-45.

All the rows in these tables are mandatory. Also, the device_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 5-2 Cisco IOS Device Directly Connected*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| IOS_LOGIN | X | | X | X |
| IOS_EN | | | X | X |

*Table 5-3 Cisco IOS Device Directly Connected Supporting SSH*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| IOS_LOGIN:SSH | X | | X | X |
| IOS_EN | | | X | X |

*Table 5-4 Catalyst Device Directly Connected*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| CATALYST_LOGIN | X | | X | X |
| CATALYST_EN | | | X | X |

*Table 5-5 Catalyst IOS MSFC Blade Directly Connected*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| CATALYST_LOGIN | X | | X | X |
| IOS_CAT_BLADE | | X | X | X |
| IOS_EN | | | X | X |

*Table 5-6 Catalyst IOS Device Directly Connected*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| CATIOS_LOGIN | X | | X | X |
| CATIOS_EN | | | X | X |

*Table 5-7 CSS Device Directly Connected*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| CSS_LOGIN | X | | X | X |
| CSS_EN | | | X | X |

*Table 5-8 CE Device Directly Connected*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| CE_LOGIN | X | | X | X |
| CE_EN | | | X | X |

*Table 5-9 PIX Device Directly Connected*

| device_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 5-10 Partial HopInfo List For Commserver Access*

| device_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 5-11 Cisco IOS Device Directly Connected*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| IOS_LOGIN | 172.28.6.90 | | Johndoe | Passnow |
| IOS_EN | | | dummy | compass |

*Table 5-12 Cisco IOS Device Directly Connected Supporting SSH*

| device_type | ip_address | port | username | password |
|---|---|---|---|---|
| IOS_LOGIN:SSH | 172.28.6.90 | | Johndoe | Passnow |
| IOS_EN | | | dummy | compass |

*Table 5-13 Cisco IOS Device Connected With Commserver*

| device_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 5-14 Catalyst IOS MFSC Blade Directly Connected*

| device_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 5-15 Catalyst IOS MFSC Blade Accessed With Commserver*

| device_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 |

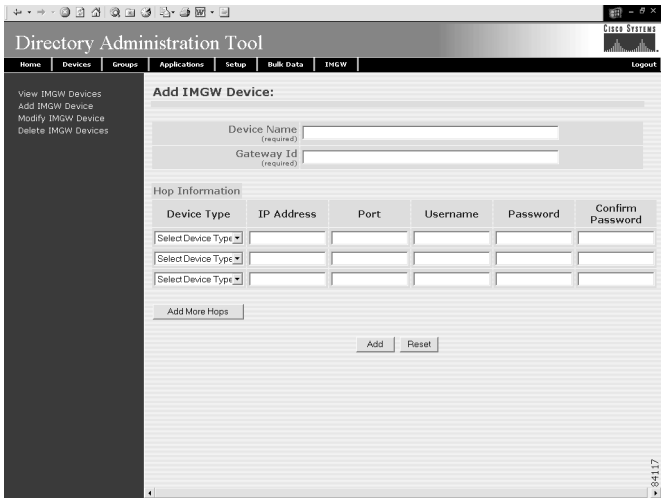
## How to Add an IMGW Device

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 5-46).

***Figure 5-46 Add IMGW Devices***




**Step 2** Enter the name of the device in the **Device Name** field.

**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** Enter parameters about each hop in the **Hop Information** fields.

For more information, see "Hop Tables" section on page 5-43.

**Step 5** To add more hops, click **Add More Hops**.

**Step 6** To clear your entries and start over, click **Reset**.

**Step 7** To add this IMGW device to the system, click **Add**.

**Step 8** To return to the main menu, click the **Home** tab.

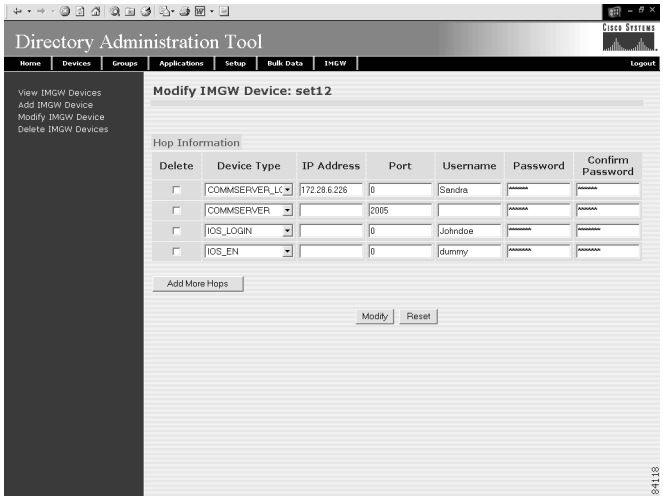
# How to Modify IMGW Devices

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 5-47).

***Figure 5-47 Add IMGW Devices***




**Step 2** Modify all required fields.

**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.

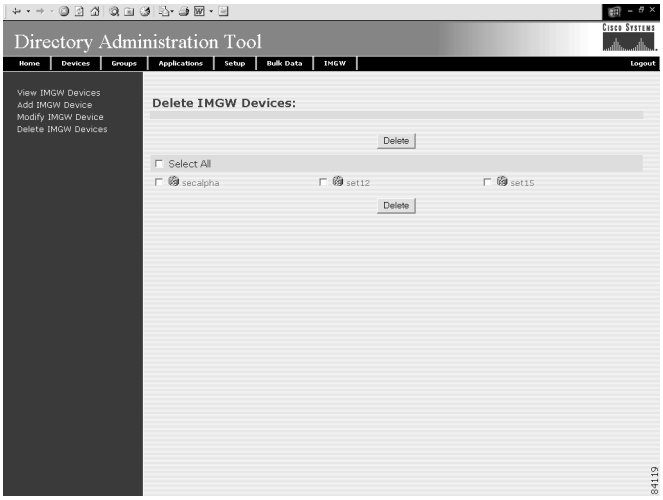
# How to Delete IMGW Devices

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 5-48).

***Figure 5-48 Delete IMGW Devices***




**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.


# 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 Telnet or Telnet 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 3-6 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 **show interfaces** 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 Telnet or Telnet Interaction is Slow

**Problem:** You cannot connect to the system using Telnet or Telnet 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. Telnet 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 Telnet.

**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 Telnet or Telnet interaction with the system is extremely slow, contact the Cisco TAC.

# 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 Telnet.

**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.

**Example1:**

Using command: **showversion**

```
[root@ie2100-techdoc /root]# showversion
Cisco Intelligence Engine 2110
Cisco Configuration Registrar (tm) Software, Version 1.3(0.1) CRYPTO [pvgarde-re
naming]
Copyright (c) 2001, 2002 by cisco Systems, Inc.
Compiled Mon 01-Jul-2002 14:55 by pvgarde


Internal directory mode.

apache
  Version: 1.3.19
  Release: 5

IBMJava2-SDK
  Version: 1.3
  Release: 10.0

ACE
  Version: 5.2
  Release: 0

DCL
  Version: 2.4
  Release: 1

Tibco
  Version: 6.48
  Release: 0

tomcat
  Version: 3.2.3
  Release: 0

CSCOPerl500503
  Version: 1
  Release: 0

CSCOcnscommon
  Version: 1.0
  Release: 1

zCSCOcnssetup
  Version: 1.2
  Release: 2

CSCOImgwConfig
  Version: 1.2
  Release: 2

CSCOcnsnsm
  Version: 1.2
  Release: 1
```

```
CSCOImgwDeviceServer
  Version: 1.2
  Release: 2

CSCOdat
  Version: 1.0
  Release: 1

CSCOcda
  Version: 0.0
  Release: 1

CSCOcnscfgs
  Version: 1.3
  Release: 0

CSCOTools
  Version: 1.0
  Release: 0

CSCOcnses
  Version: 1.5
  Release: 1

CSCOimgw
  Version: 1.2
  Release: 2
```

### Example2:

Using command: **showversion -m CSCOcnses**

```
[root@ie2100-techdoc /root]# showversion -m CSCOcnses
Cisco Intelligence Engine 2110
Cisco Configuration Registrar (tm) Software, Version 1.3(0.1) CRYPTO [pvgarde-re
naming ]
Copyright (c) 2001, 2002 by cisco Systems, Inc.
Compiled Mon 01-Jul-2002 14:55 by pvgarde


Internal directory mode.

Name        : CSCOcnses                    Relocations: (not relocateable)
Version     : 1.5                               Vendor: Cisco Systems, Inc.
Release     : 1                             Build Date: Mon Jul  1 14:25:50 2002
Install date: Tue Jul  2 07:06:08 2002      Build Host: rm-build7.cisco.com
Group       : Event Services                Source RPM: CSCOcnses-1.5-1.src.rpm
Size        : 537126                           License: Copyright (c) 1999, 2000
, 2001, 2002 by Cisco Systems, Inc.  All Rights Reserved.
Summary     : CNS Event Services
Description :
CNS Event Services
```

# 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. 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**.


# Country Codes

This appendix lists the two-letter IOS codes for country identification (ISO 3166). These are used in the **Setup** program.

***Table B-1 Country Codes***

| | | | | | |
|---|---|---|---|---|---|
| Afghanistan | af | Georgia | ge | Northern Mariana Islands | mp |
| Albania | al | Germany | de | Norway | no |
| Algeria | dz | Ghana | gh | Oman | om |
| American Samoa | as | Gibraltar | gi | Pakistan | pk |
| Andorra | ad | Greece | gr | Palau | pw |
| Angola | ao | Greenland | gl | Palestinian Territory, Occupied | ps |
| Anguilla | ai | Grenada | gd | Panama | pa |
| Antarctica | aq | Guadeloupe | gp | Papua New Guinea | pg |
| Antigua and Barbuda | ag | Guam | gu | Paraguay | py |
| Argentina | ar | Guatemala | gt | Peru | pe |
| Armenia | am | Guinea | gn | Philippines | ph |
| Aruba | aw | Guinea-Bissau | gw | Pitcairn | pn |
| Australia | au | Guyana | gy | Poland | pl |
| Austria | at | Haiti | ht | Portugal | pt |
| Azerbaijan | az | Heard Island and McDonald Islands | hm | Puerto Rico | pr |
| Bahamas | bs | Holy See (Vatican City State) | va | Qatar | qa |
| Bahrain | bh | Honduras | hn | Reunion | re |
| Bangladesh | bd | Hong Kong | hk | Romania | ro |

*Table B-1 Country Codes (continued)*

| | | | | | |
|---|---|---|---|---|---|
| Barbados | bb | Hungary | hu | Russian Federation | ru |
| Belarus | by | Iceland | is | Rwanda | rw |
| Belgium | be | India | in | Saint Helena | sh |
| Belize | bz | Indonesia | id | Saint Kitts and Nevis | kn |
| Benin | bj | Iran, Islamic Republic of | ir | Saint Lucia | lc |
| Bermuda | bm | Iraq | iq | Saint Pierre and Miquelon | pm |
| Bhutan | bt | Ireland | ie | Saint Vincent and the Grenadines | vc |
| Bolivia | bo | Israel | il | Samoa | ws |
| Bosnia and Herzegovina | ba | Italy | it | San Marino | sm |
| Botswana | bw | Jamaica | jm | Sao Tome and Principe | st |
| Bouvet Island | bv | Japan | jp | Saudi Arabia | sa |
| Brazil | br | Jordan | jo | Senegal | sn |
| British Indian Ocean Territory | io | Kazakstan | kz | Seychelles | sc |
| Brunei Darussalam | bn | Kenya | ke | Sierra Leone | sl |
| Bulgaria | bg | Kiribati | ki | Singapore | sg |
| Burkina Faso | bf | Korea, Democratic People's Republic of | kp | Slovakia | sk |
| Burundi | bi | Korea, Republic of | kr | Slovenia | si |
| Cambodia | kh | Kuwait | kw | Solomon Islands | sb |
| Cameroon | cm | Kyrgyzstan | kg | Somalia | so |
| Canada | ca | Lao People's Democratic Republic | la | South Africa | za |
| Cape Verde | cv | Latvia | lv | South Georgia and the South Sandwich Islands | gs |
| Cayman Islands | ky | Lebanon | lb | Spain | es |
| Central African Republic | cf | Lesotho | ls | Sri Lanka | lk |
| Chad | td | Liberia | lr | Sudan | sd |
| Chile | cl | Libyan Arab Jamahiriya | ly | Suriname | sr |
| China | cn | Liechtenstein | li | Svalbard and Jan Mayen | sj |

*Table B-1 Country Codes (continued)*

| | | | | | |
|---|---|---|---|---|---|
| Christmas Island | cx | Lithuania | lt | Swaziland | sz |
| Cocos (Keeling) Islands | cc | Luxembourg | lu | Sweden | se |
| Colombia | co | Macau | mo | Switzerland | ch |
| Comoros | km | Macedonia, the Former Yugoslav Republic of | mk | Syrian Arab Republic | sy |
| Congo, The Democratic Republic of the | cd | Madagascar | mg | Taiwan, Province of China | tw |
| Congo | cg | Malawi | mw | Tajikistan | tj |
| Cook Islands | ck | Malaysia | my | Tanzania, United Republic of | tz |
| Costa Rica | cr | Maldives | mv | Thailand | th |
| Cote D'Ivoire | ci | Mali | ml | Togo | tg |
| Croatia | hr | Malta | mt | Tokelau | tk |
| Cuba | cu | Marshall Islands | mh | Tonga | to |
| Cyprus | cy | Martinique | mq | Trinidad and Tobago | tt |
| Czech Republic | cz | Mauritania | mr | Tunisia | tn |
| Denmark | dk | Mauritius | mu | Turkey | tr |
| Djibouti | dj | Mayotte | yt | Turkmenistan | tm |
| Dominica | dm | Mexico | mx | Turks and Caicos Islands | tc |
| Dominican Republic | do | Micronesia, Federated States of | fm | Tuvalu | tv |
| East Timor | tp | Moldova, Republic of | md | Uganda | ug |
| Ecuador | ec | Monaco | mc | Ukraine | ua |
| Egypt | eg | Mongolia | mn | United Arab Emirates | ae |
| El Salvador | sv | Montserrat | ms | United Kingdom | gb |
| Equatorial Guinea | gq | Morocco | ma | United States Minor Outlying Islands | um |
| Eritrea | er | Mozambique | mz | United States | us |
| Estonia | ee | Myanmar | mm | Uruguay | uy |
| Ethiopia | et | Namibia | na | Uzbekistan | uz |
| Falkland Islands (Malvinas) | fk | Nauru | nr | Vanuatu | vu |

*Table B-1 Country Codes (continued)*

| | | | | | |
|---|---|---|---|---|---|
| Faroe Islands | fo | Nepal | np | Venezuela | ve |
| Fiji | fj | Netherlands Antilles | an | Vietnam | vn |
| Finland | fi | Netherlands | nl | Virgin Islands, British | vg |
| France, Metropolitan | fx | New Caledonia | nc | Virgin Islands, U.S. | vi |
| France | fr | New Zealand | nz | Wallis and Futuna | wf |
| French Guiana | gf | Nicaragua | ni | Western Sahara | eh |
| French Polynesia | pf | Niger | ne | Yemen | ye |
| French Southern Territories | tf | Nigeria | ng | Yugoslavia | yu |
| Gabon | ga | Niue | nu | Zaire | zr |
| Gambia | gm | Norfolk Island | nf | Zambia | zm |
| | | | | Zimbabwe | zw |


# 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



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



This package is a SSLv3/TLS protocol analyzer written by Eric Rescorla <ekr@rtfm.com> and licensed by RTFM, Inc.

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 acknowledgement: This product includes software developed by Eric Rescorla for RTFM, Inc.

4. Neither the name of RTFM, Inc. nor the name of Eric Rescorla may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ERIC RESCORLA AND RTFM, INC. “AS IS” AND ANY EXPRESS 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 REGENTS OR 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 SUCH DAMAGE.

# Mozilla Public License

The contents of this file are subject to the Mozilla Public License Version 1.1 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is RHINO v 1.5.3.

# GNU General Public License

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991



59 Temple Place, Suite 330, Boston, MA 02111-1307 USA



### 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



59 Temple Place, Suite 330, Boston, MA 02111-1307 USA



[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


## Symbols



## A



## B



## C

## D

## E



## G



## H



## I

## L



## M



## N



## O



## P

## R



## S



## T



## U

## V



## X