Cisco Configuration Engine Linux Installation & Configuration Guide, 2.0

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-7962-01

Cisco Configuration Engine Linux Installation & Configuration Guide, 2.0

Preface

This document describes how to install and configure Cisco Configuration Engine, 2.0, on a host system running on Linux. For a list of other documents related to this product, refer to the "Related Documentation" section.

Note For the latest information regarding this release, check online at: www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cce/rel2_0/index.htm.

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

Audience

This guide is intended primarily for:

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

Conventions

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

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

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

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

Related Documentation

Other documentation related to this product include:

- *Cisco Configuration Engine Administrator Guide, 2.0*
- *Release Notes for Cisco Configuration Engine, 2.0*
- *Cisco Configuration Engine Software Development Kit API Reference and Programmer Guide, 2.0*
- *Cisco Configuration Engine SDK Cookbook*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE RUNNING ON THE CISCO 2116 INTELLIGENCE ENGINE HARDWARE PLATFORM

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the Software License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the Software License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence. By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software. When used below, the term "server" refers to central processor unit.

1. **ADDITIONAL LICENSE RESTRICTIONS**

- **Installation and Use**

The Cisco Configuration Engine 1.5 Software component of the Cisco 2116 Intelligence Engine Hardware Platform is not preinstalled. A CD-ROM containing the Cisco Configuration Engine 1.5 Software for the Cisco 2116 Hardware Platform is provided to Customer for installation purposes only. Customer may only run the supported Cisco Configuration Engine 1.5 Software on the Cisco 2116 Hardware Platform designed for its use. No unsupported Software product or component may be installed on the Cisco 2116 Hardware Platform.

- **Software Upgrades, Major and Minor Releases**

Cisco may provide Cisco Configuration Engine Software updates and new version releases for the Cisco 2116 Hardware Platform. If the Software update and new version releases can be purchased through Cisco or a recognized partner or reseller, the Customer should purchase one Software update for each Cisco 2116 Hardware Platform. If the Customer is eligible to receive the Software update or new version release through a Cisco extended service program, the Customer should request to receive only one Software update or new version release per valid service contract.

- **Reproduction and Distribution.** Customer may not reproduce nor distribute software.

2. **DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS**

Please refer to the Cisco Systems, Inc. End User License Agreement.

Installing the Product Software

Cisco Configuration Engine, 2.0 is a Cisco product designed to configure large numbers of customer-premise network devices in a plug-and-play manner.

System Requirements

- Pentium III or equivalent and above.
- Red Hat Enterprise Linux Enterprise Server 3.0.
- 1 GB RAM.
- 40 GB disk space.

Cisco IOS Dependences

Table 1-1 lists Cisco IOS versions with corresponding versions of Cisco Configuration Engine, 2.0 including feature limitations associated with each version.

Table 1-1 Cisco Configuration Engine, 2.0 and Cisco IOS Dependencies

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

Installing the Software

The Cisco Configuration Engine, 2.0 software is contained on a CD-ROM that is in the accessory kit.

Step 1 Install the CD-ROM into the disk drive on the host system.

Step 2 Copy the tar file into a new folder where disk space is large enough:

tar xvf <*tarfilename***>**

Step 3 Enter the following commands:

cd RPMS

./ce_install.sh

Step 4 After installing the software, log out, then log back in again, or create a new window.

Step 5 Enter the following commands:

cd $CISCO_CE_INSTALL_ROOT/CSCOcnsie/bin/

./setup

Step 6 Go to Chapter 2, "System Configuration" for a description of how to configure your system.

Script Options

The Cisco Configuration Engine, 2.0 image is provided to the user in tar file format. Users should untar the image in a directory. Then, the user should go to that directory and run the **ce_install.sh** command.

In order to support different types of installations and setup, the scripts uses options to differentiate different requirements.

Because Cisco Configuration Engine, 2.0 must share the web infrastructure-related software with bundled Cisco software. The default behavior of the script is defined in the *installRule.<os>.xml* file. This file is located in the same directory where the Cisco Configuration Engine, 2.0 tar file is untarred. The *installRule.<os>.xml* file contains information about:

- Which package for which version should be installed.
- Can a package be shared.
- The behavior of the installation if the package exists or not.
- The methods to install and un-install the package.

The result of the installation is logged under */var/log/CNSCE/install.log*, lists what exactly is being installed into the system. For a successful install, it should be the same as the contents of *installRule.<os>.xml*.

The *installError.xml* file is generated if there is an error during installation. Other files such as those that contain all Cisco Configuration Engine, 2.0 related environmental variables are generated during installation stage including: *global.sh*, *global.csh*, *global.pm*, and *installdata.properties*.

Options for *ce_install.sh*

The installation script, *ce_install.sh*, has the following options:

Note No option indicates default behavior which is described above.

-batch: This option allows non-interactive installation. The installation script reads the default values from *installRule.<os>.xml* file and installs Cisco Configuration Engine, 2.0 based on these settings without query for user input.

-demo: Installs the package without checking system resources except for minimum disk space, which is 650MB.

-force: install/uninstall Cisco Configuration Engine, 2.0 without installation or un-installation status check.

Options for Setup Script

The setup script, *setup*, has the following options:

Default option is interactive mode, that prompts the user to provide inputs and store them in a data file. The default value is read from *setupRule.xml* under *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/*.

The result will put in log file: */var/log/CNSCE/appliance-setup.log*.

-s: batch mode which reads all the information it requires for setup without user interaction from the data file: *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/setupRule.xml*.

The result is put in a log file: */var/log/CNSCE/appliance-setup.log*.

Before running batch mode the first time, you must run the utility script:

$CISCO_CE_HOME/bin/passwdEncryption.pl

This creates encrypted passwords and loads them into **setupRule.xml**. The passwords in XML must be in encrypted text, not plain text.

Uninstall Script

The uninstall script, *ce_uninstall.sh*, is copied into */var/ciscoce/install* directory. This script reads the *installdata.xml* file to do package uninstall:

1. Stop all running Cisco Configuration Engine, 2.0 processes.
2. Remove all database data from BDB.
3. Remove installed database software if it is BDB.

Remove all presence of the installed packages.

Data Migration from Release 1.5 to 2.0

The Data Migration function allows you to upgrade your system to from Release 1.5 to Release 2.0, then populate your directory with the data you established for the prior release.

This is a three-step process:

1. Export data to a remote FTP site.
2. Install Release 2.0 software.
3. Retrieve data from the FTP site and setup the system.

Export Data to a Remote FTP Site

Before exporting the data, it is assumed that your host has already been setup and is up running.

Step 1 Insert the Release 2.0 CD-ROM into the CD drive of your host to be upgraded.

Step 2 To mount the CD-ROM, login as root, then enter the command:

mount /mnt/cdrom

Step 3 Copy and untar the image file, then go to: *RPMS/DataExport*.

Step 4 Issue the data export command:

./dataexport

Tip Make sure you type the period (**.**) prior to the command.

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

Following are the prompts of **dataexport**:

Notes

Sample user inputs are shown in **bold** text.

```
Entering Data Export
Type ctrl-c to exit

Enter FTP server (hostname.domainname or IP address): sername.cisco.com
Enter DNS server IP address: 171.69.226.120
Enter username used for FTP server: smith
Enter FTP password: *****
Re-enter FTP password: *****
Enter absolute pathname of data file on FTP server: /users/smith/migration.tar
```

Install Release 2.0 Software

Install the new Cisco Configuration Engine, 2.0 software on the target system.

Run *datamigrate* and Configure the System

Step 1 Log in as **root**.

Step 2 Start data migration with the command:

datamigrate

The script proceeds in three stages:

1. Acquire information of the FTP server that stores the migration data and retrieve the data.
2. Start Release 2.0 **Setup** prompts and configure the system.
3. Populate internal directory storage with retrieved data.

Following are the prompts of **datamigrate**:

Notes

Sample user inputs are shown in bold text.

```
Enter FTP server (hostname.domainname or IP address): sername.cisco.com
Enter username used for FTP server: smith
```

```
Enter FTP password: *****
Re-enter FTP password: *****
Enter absolute pathname of data file on FTP server: /users/smith/migration.tar
```

Synchronize Clocks

The clock (date and time) on your host and the clock on the PC you use to access the Cisco Configuration Engine, 2.0 user interface should be synchronized. This is particularly important when scheduling an update-image job for a future time (refer to the *Cisco Configuration Engine Administrator Guide, 2.0*).

For this operation, the client-side check to ensure you have entered a valid time value is done using the clock on the PC with the browser used to access the Cisco Configuration Engine, 2.0 user interface. Consequently, if your host clock is behind the PC clock, the user interface does not allow the job to be scheduled.

For example, if your host clock read 11:10 while the PC clock read 12:10, the user interface will not allow a job to be scheduled before 12:10. It will issue an error message: **Please input a future time**.

System Configuration

This chapter provides information about how to use the **Setup** program to configure your host system for Cisco Configuration Engine, 2.0.

Running Setup

System configuration for Cisco Configuration Engine, 2.0 is accomplished using the **Setup** program. You must run the **Setup** program when you start the system for the first time.

To get started, from the directory where Cisco Configuration Engine, 2.0 software files are located, use the command:
./setup

Limitations and Restrictions

- Once you have committed changes (`Commit changes (y/n): y`), it cannot be aborted by entering **Ctrl-c**.
- All password values in **Setup** must contain alphanumeric characters *only.* Special characters have different meanings in the UNIX shell and should *not* be used for passwords.
- Device Name values may contain only: period (.), underscore (_), hyphen (-), and alphanumeric characters.
- Group Name values may contain only: underscore (_) and alphanumeric characters.

Internal Directory Mode Setup Prompts

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

Notes

- Default values are shown within brackets: […]. To use a default value, simply press **Return**.
- Sample user inputs are shown in **bold** text.

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

        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: *****
Enter internal LDAP server port number: [389]

Email service settings:
-----------------------

Enter SMTP server (hostname.domainname or IP address):


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

Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s) (y/n)?
[y]
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
Enter port number for http web access: [80]
Enter port number for https web access: [443]
Enter Tomcat internal port number: [8009]
Enter Tomcat shutdown port number: [8005]

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

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

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

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

Enter Event Gateway application parameter(s) for NSM: [config]
Enable Event Gateway debug log (y/n)? [n]
Enter log file rotation timer (minutes, 0 = no rotation): [15]
Enter max log file size (Kbytes): [3072]
Enable log backup (y/n)? [y]

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]
Enter CNS Event Bus Daemon Parameter: [7500]
Enable CNS Event Bus routing daemon logging (y/n)? [n]
Enter http port for Event Bus Web Adminstration GUI: [7580]

Event Bus Web Admin port should always be closed unless the Web admin GUI is needed.
Keeping web admin port open is a security risk.
```

```
Would you like to open Event Bus Web Administration port (y/n)? [n]

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: 20
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 (seconds): 60
Logging mode (append, overwrite): append
Alternative username prompt for device using TACACS/RADIUS:
Alternative password prompt for device using TACACS/RADIUS:

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

CE Monitor Settings:
-----------------------

Enter CE Monitor timer (seconds): [1800]

Web Servicess settings:
----------------------

Enable CEConfigService web service (y/n)?  [y]
Enable CEImageService web service (y/n)?  [y]
Enable CEAdminService web service (y/n)?  [y]
Enable CEExecService web service (y/n)?  [y]
Enable CENSMService web service (y/n)?  [Y]
Please review the following parameters:
Configuration Engine login name: admin
Configuration Engine login password: *****
internal LDAP server port number: 389
internal LDAP server password: *****
SMTP server (hostname.domainname or IP address):
Enable cryptographic (crypto) operation between Event Gateway(s)/Config server and
device(s) (y/n)? n
port number for http web access: 80
Tomcat internal port number: 8009
Tomcat shutdown port number: 8005
Enable authentication (y/n)? n
Event Gateway application parameter(s) for NSM: config
Enable Event Gateway debug log (y/n)? n
log file rotation timer (minutes, 0 = no rotation): 15
max log file size (Kbytes): 3072
Enable log backup (y/n)? y
number of Event Gateways that will be started with plaintext operation: 5
Cisco-CE Event Bus Network Parameter: imgw-test7
Cisco-CE Event Bus Service Parameter: 7500
Cisco-CE Event Bus Daemon Parameter: 7500
Enable Cisco-CE Event Bus routing daemon logging (y/n)? n
http port for Event Bus Web Administration GUI: 7580
Would you like to open Event Bus Administration port (y/n)? n
Re-configure IMGW (y/n)? n
CE Monitor timer (seconds): 1800
Enable CEConfigService web service (y/n)?  y
Enable CEImageService web service (y/n)?  y
```

```
Enable CEAdminService web service (y/n)?  y
Enable CEExecService web service (y/n)?  y
Enable CENSMService web service (y/n)? Y


        Warning: setup cannot be aborted while committing changes.

Commit changes (y/n):
```

Parameter Descriptions

Configuration Engine login name/password: Define the administrator account and password for accessing Cisco Configuration Engine GUI.

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

Enter internal LDAP server port number: Define the port number that should be used by LDAP server. Default value is 389.

Table 2-1 Valid Values for General Parameters

Parameter	Type	Length/Range
Configuration Engine login name	Alphanumeric	1 – 30
Configuration Engine login password	Password	1 – 12
Internal LDAP server password	Password	1 – 20
Internal LDAP server port number	Port number	0 – 65535

- Password type refers to ASCII characters that are between the octal values 040 (space) and 176 (~) inclusive.
- Alphanumeric type refers to alphabetic and numeric characters plus the underscore (_) symbol.

Email Service Setting

Enter SMTP server (hostname.domainname or IP address): Specifies the SMTP server hostname or IP address to enable email notification service. The SMTP server is used to send out email. This parameter is optional. If you do not wish to provide email service, leave it blank.

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 (for example, *https://machine/config/login.html*). The event gateway listens to ports 11012, 11014, and so on (depending on the number of gateways started). All data between your host and the far end is encrypted. The SSL protocol (combined with valid certificates) ensures that your host is authenticated by the far end. In order to complete SSL configuration, valid certificates need to be placed on your host. See Section "Configuring SSL Certificates" section on page 2-16 for details. For testing, after configuration open an SSL connection to each port (**openssl s_client –connect hostname:port**). This should be done for both enable and disable cases.

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

Enable plaintext operation between Config Server and devices/GUI administration (y/n): This option enables plaintext config server operation. In addition to listening on TCP port 443 for crypto connections, the web server also listens on TCP port 80 for plaintext connections, responding to HTTP requests (for example, *http://machine/config/login.html*). **If crypto is disabled, plaintext between Config Server and devices/GUI administration 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 is in Event service settings (see "Event Service Settings" section on page 2-6).

Port number for http web access: Specify the port number to be used for http web access. The default is 80.

Enter port number for https web access: Specify the port number to be used for secure http web access. The default is 443.

Enter Tomcat internal port number: Specify the port number for internal communication between Apache and Tomcat. The default is 8009.

Enter Tomcat shutdown port number: Specify the shutdown port number for Tomcat. The default is 8005.

Table 2-2 Valid Values for Encryption Parameters

Parameter	Type	Length/Range
Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s)	y, n	
Absolute pathname of remote key file	Alphanumeric	1 – 255
Absolute pathname of remote certificate file	Alphanumeric	1 – 255
Enable plaintext between Config Server and devices/operators	y, n	
Enable plaintext operation between Event Gateway and devices	y, n	
port number for http web access	Port number	0 – 65535
port number for https web access	Port number	0 – 65535
Tomcat internal port number	Port number	0 – 65535
Tomcat shutdown port number	Port number	0 – 65535

Authentication Settings

Enable authentication (y/n): Enable IOS device authentication mechanism within your host. To test, attempt to connect an IOS device, with an incorrect password, to the Configuration Engine 1.6. The password can be changed on IOS with the hidden command **cns password newPassword**.

Note If disabling device authentication, connection to devices with pre 12.2(10)T IOS is implicitly allowed.

Table 2-3 Valid Values for Authentication Parameters

Parameter	Type	Length
Enable authentication	y, n	

Event Service Settings

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**.

Event Gateway debug log: Send Event Gateway **debug** output to the log file: */var/log/CNSCE/evtgateway.*

Log file rotation timer (minutes, 0 = no rotation): The time period to check whether event gateway log files should be log-rotated in current working directory. If the value is **0** then the event log files are not log-rotated. The default value is 2 minutes if event gateway debug logging is turned on and 5 minutes if event gateway debug logging is turned off. Valid values are 0 to 1440.

Max log file size (Kbytes): The file size above which log-rotation starts. The default is 3072 Kbytes. Valid values are 1 to 2097152 (Kbytes).

Log backup (y/n)? Indicates whether the event gateway log-rotated file should be copied to the backup directory */var/log/CNSCE/evt_gateway/backup*. Default is **y**; log files in */var/log/CNS* are tarred, time stamped and moved into the backup directory.

Number of Event Gateways that will be started with crypto operation: Specify the number of Event Gateway processes that should be started in crypto mode; for example, the number of Event Gateways that communicate with devices using SSL. **Note: that if crypto operation is disabled, this prompt is also disabled.**

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

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

Event CNS Bus Service Parameter: Specify the UDP port used for publishing and listening to events among Event Bus daemons. Dedicating a port for communication between a host system and its managing devices can reduce traffic caused by listening to other unrelated events. The default is 7500.

Enter CNS Event Bus Daemon Parameter: Specify the TCP port that should be used for the TCP connections between Event Bus daemon and its client applications. The default is 7500.

Enable CNS Event Bus routing daemon logging (y/n)? Enable or disable Event Bus logging. The default is disable. Log file can be found at */var/log/CNSCE/rvrd/rvrd.log*.

Enter http port for Event Bus Web Administration GUI: Specify the http port for accessing Event Bus Web Administration interface. The default is 7580.

Would you like to open Event Bus Web Administration port (y/n)? Enable or disable the http port for Event Bus Web interface access.

Table 2-4 Valid Values for Event Service Parameters

Parameter	Type	Range
Event Gateway application parameter(s) for NSM	Alphanumeric, dash, space	1 – unlimited
Event Gateway debug log	y, n	
Log file rotation timer (minutes, 0=no rotation)	Timer	0 – 1440
Max log file size	File size	1 – 2097152 (Kbytes

Table 2-4 Valid Values for Event Service Parameters (continued)

Parameter	Type	Range
Log backup (y/n)?	y, n	
Number of Event Gateways that will be started with crypto operation	Integer	1 – 11
Number of Event Gateways that will be started with plaintext operation	Integer	0 – 11 (if crypto enabled) 1 – 11 (if crypto disabled)
Event CNS bus network parameter	Network parameter	
Event CNS bus service parameter	Port number	0 – 65535
Event CNS bus daemon parameter	Port number	0 – 65535
Event CNS bus routing daemon logging (y/n)	y, n	
HTTP port for Event Bus Web Administration GUI	Port number	0 – 65535
Open Event Bus Web Administration port (y/n)	y, n	
Re-configure IMGW	y, n	

Web Service Settings

The following Web Service interfaces are provided:

- **Enable CEConfigService web service**: Enable web service to send/acquire configurations to/from devices.
- **Enable CEImageService web service**: Enable web service to delete files, obtain an inventory of the hardware, file system(s) & their content, distribute or activate image(s) on devices.
- **Enable CEExecService web service**: Enable web service to execute show commands or reboot on devices.
- **Enable CEAdminService web service**: Enable web service to create and manage the various system objects used by the Cisco Configuration Engine to manage devices (such as devices, line-cards, images, configurations (templates), users, conditions, groups, passwords).
- **Enable CENSMService web service**: Enable web service to create and manage namespace, subjects in namespace and subject mappings in Namespace. It also includes an operational API to resolve subjects.

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: [mainstreet]
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: [20]
```

```
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 (seconds): [60]
Enter logging mode (append, overwrite): [append]
Alternative username prompt for device using TACACS/RADIUS:
Alternative password prompt for device using TACACS/RADIUS:
```

Parameter Descriptions

Re-configure IMGW: This yes/no prompt determines whether setup should display the section of prompts for re-configuring IMGW related parameters. Regular user should always answer **n**.

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 purposes.

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.

Alternative username/password prompts for device using TACACS/RADIUS: When a device is authenticated by TACACS+ or RADIUS servers, the username/password prompts which are returned to the Telnet users are configurable. The **alternative username/password prompts** allow you to choose your own set of username/password prompts. If no inputs are entered, the default username/password prompts **Username:** and **Password:** are assumed.

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.

Note No prompts are issued to set up FTP and TFTP File Servers in External Directory Mode as these services are always disabled in this mode. If you had previously set up FTP and/or TFTP in Internal Directory Mode, after switching to External Directory Mode the services will have been disabled. You will need to rerun **Setup** in Internal Directory Mode again to re-enable them.

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

Notes

- Default values are shown within brackets: […]. To use a default value, simply press **Return**.
- Sample user inputs are shown in **bold** text.

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

Email service settings:
-----------------------

Enter SMTP server (hostname.domainname or IP address): abc.cisco.com

Encryption settings:

Enable cryptographic (crypto) operation between Event Gateway(s)/Config
Server and device(s) (y/n)? [n] y
Enter absolute pathname of remote key file: /a/b/c
Enter absolute pathname of remote certificate file: /a/b/c

        Enabling plaintext operation will increase security risk.

Enable plaintext operation between Config Server and devices/GUI
administration (y/n)? [y]
Enable plaintext operation between Event Gateway and devices (y/n)? [y]
Enter port number for http web access: [80]
Enter port number for https web access: [443]
Enter Tomcat internal port number: [8009]
Enter Tomcat shutdown port number: [8005]

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]

Event services settings:
```

```
------------------------

Enter Event Gateway application parameter(s) for NSM: [config]
Enable Event Gateway debug log (y/n)? [n]
Enter log file rotation timer (minutes, 0 = no rotation): [15]
Enter max log file size (Kbytes): [3072]
Enable log backup (y/n)? [y]

        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 plaintext
operation: [5] 4
Enter Cisco-CE Event Bus Network Parameter: [imgw-test7]
Enter Cisco-CE Event Bus Service Parameter: [7500]
Enter Cisco-CE Event Bus Daemon Parameter: [7500]
Enable Cisco-CE Event Bus routing daemon logging (y/n)? [n]
Enter http port for Event Bus Web Administration GUI: [7580]

        Event Bus Web Admin port should always be closed unless the Web
        admin GUI is needed. Keeping web admin port open is a security
        risk.

Would you like to open Event Bus Administration port (y/n)? [n]

External directory settings:
----------------------------
Enter IP address of remote directory server: 3.3.3.3
Can't ping remote directory server. The ip address you input is invalid.
Enter IP address of remote directory server: [3.3.3.3] 192.168.98.73
Enter port number of remote directory server: [389]
Enter external directory server login name: admin
Enter external directory server password: *****
Re-enter external directory server password: *****
Enter User DN: cn=admin,o=butterfly
Enter Cisco-CE context: ou=cns,o=butterfly
Use sample schema (y/n)? [y]

Current settings of IMGW:
-------------------------
Gateway ID: imgw-test7
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: 25
Hoptest success retry interval (sec): 0
Hoptest failure retry interval (sec): 0
Logging level (verbose, error, silent): error
Log file Prefix: IMGW-LOG
Log file size (bytes): 50331648
Log file rotation timer (seconds): 60
Logging mode (append, overwrite): append
Alternative username prompt for device using TACACS/RADIUS:
Alternative password prompt for device using TACACS/RADIUS:
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 Cisco-CE context; for example, **admin**.

Remote directory server password: Directory user password.

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

Cisco-CE context: Directory context (DN) under which all Cisco Configuration Engine objects are created. This includes device objects, group objects, application objects, and event objects. These objects can be created inside containers under Cisco-CE 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 2-6 Valid Values for General External Directory Mode Parameters

Parameter	Type	Length/Range
IP address of the remote Directory Server	IP address	
Port number of the remote Directory Server	Port number	0 – 65535
Remote directory server login name	Alphanumeric	1 – 32
Remote directory server password	Alphanumeric	1 – 20
User DN	Name-value pair with space	3 – unlimited
Cisco-CE context	Name-value pair with space	3 – unlimited

Sample Schema

If you answer the first prompt (Use sample schema (y/n):) with **y** indicating that you want to use the sample schema, the default values shown in brackets in the sample below are used for all sample schema attributes and they do not appear.

If you answer the first prompt with **n** indicating you do not want to use the sample schema as is, the attributes of the sample schema appear along with their default values in brackets. You can overwrite any of these default values to create your own schema:

```
Use sample schema (y/n): n
Enter container name under which device objects are stored: [ou=CNSDevices]
Enter container name under which generic device objects are stored:
[ou=GenericDevices]
Enter container name under which PIX device objects are stored:
[ou=PIXDevices]
Enter container name under which linecard objects are stored:
[ou=LinecardDevices]
Enter container name under which application objects are stored:
[ou=CNSApplications]
Enter container name under which IMGW objects are stored: [ou=imgw]
Enter container name under which CIS objects are stored: [ou=CISObjects]
Enter container name under which image objects are stored: [ou=Images]
Enter container name under which CIS device objects are stored:
[ou=CISDevices]
Enter container name under which distribution objects for Image are stored:
[ou=Distributions]
Enter container name under which Query objects are stored: [ou=Query]
Enter objectclass for device object: [IOSConfigClass]
```

```
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 device category attribute name in device objectclass: [AdminDevType]

        Enabling Modular Router feature allows you to configure linecards
        independently of the slot numbers.

Would you like to use Modular Router Feature (y/n)? [y] y
Enter IOS device type attribute name in device objectclass: [IOSlinecardtype]
Enter IOS sub devices attribute name in device objectclass: [IOSsubdevices]
Enter IOS main device attribute name in device objectclass: [IOSmaindevice]
Enter IOS slot attribute name in device objectclass: [IOSslot]
Enter interfaces info attribute name in device objectclass: [IOSinterfacesinfo]
Enter controllers info attribute name in device objectclass: [IOScontrollerinfo]
Enter voiceports info attribute name in device objectclass: [IOSvoiceportinfo]
Enter Cisco-CE group attribute name in device: [parent]
Enter Cisco-CE 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]
```

Definitions

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

Generic device objects container name: The container in the directory under which generic 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.

IMGW objects container name: The container in the directory under which IMGW 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. Note 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.

Would you like to use Modular Router Feature (y/n)?: Enable/Disable the next seven modular router related schema prompts from IOS-device-type attribute name to voiceports-info attribute name.

IOS device type attribute name: Single-value string attribute which will be used to store device type information in the directory.

IOS sub devices attribute name: Attribute that stores sub-device list associated with main device in the directory. Note this has to be a multi-valued attribute.

IOS main device attribute name: Attribute that stores the name of the main device of a sub-device in the directory.

IOS slot device attribute name: Attribute that stores the inventory details related to slot numbering.

Interfaces info attribute name: Attribute that stores the inventory details related to interfaces.

Controllers info attribute name: Attribute that stores the inventory details related to controllers.

Voiceports info attribute name: Attribute that stores the inventory details related to voice-ports.

Cisco-CE 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 only required when NSM directive is set to http mode**.

Cisco-CE password attribute name in device object class: The attribute of the device class that stores the value that the host system expects as the CNS password from the IOS device. **If bypass authentication is "y", this prompt is disabled.**

objectclass for bootstrap password object: The name of the user defined object class for the bootstrap password object. **If bypass authentication is "y", 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 host system uses as the bootstrap password. **If bypass authentication is "y", this prompt is disabled.**

Table 2-7 Valid Values for Sample Schema Parameters

Parameter	Type	Length
Device object container name	Name-value pair with space	3 – unlimited
Generic device object container name	Name-value pair with space	3 – unlimited
Group object container name	Name-value pair with space	3 – unlimited
Application container name	Name-value pair with space	3 – unlimited
Object class	Alphanumeric	1 – 80
Template attribute name	Alphanumeric	1 – 80
Config ID attribute name	Alphanumeric	1 – 80
Device ID attribute name	Alphanumeric	1 – 80
Event ID attribute name	Alphanumeric	1 – 80
IOS device type attribute name	Alphanumeric	1 – 80
IOS sub device type attribute name	Alphanumeric	1 – 80
IOS main device type attribute name	Alphanumeric	1 – 80
IOS slot attribute name	Alphanumeric	1 – 80
Interfaces info attribute name	Alphanumeric	1 – 80
Controllers info attribute name	Alphanumeric	1 – 80
Voiceports info attribute name	Alphanumeric	1 – 80
Cisco-CE group attribute	Alphanumeric	1 – 80
Cisco-CE password attribute name	Alphanumeric	1 – 80
Objectclass for bootstrap password object	Alphanumeric	1 – 80
Bootstrap password attribute name	Alphanumeric	1 – 80

Command Line Support for Start/StopComponents

Cisco Configuration Engine, 2.0 supports start/stop for the following components:

- http/tomcat (webserver): **/etc/rc.d/init.d/httpd {start|stop}**

- IMGW: **/etc/rc.d/init.d/Imgw {start|stop}**
- Event gateway: **/etc/rc.d/init.d/EvtGateway {start|stop} [port number]**
- Event gateway crypto: **/etc/rc.d/init.d/EvtGatewayCrypto {start|stop} [port number]**

Cisco Configuration Engine, 2.0 includes two new scripts to handle start and stop components. Some servers have dependency to other servers, therefore the shutdown and startup script is not provided for these types of servers. For example, Tibco has to be up for http/tomcat, if Tibco is shutdown, and brought up again, the webservers, httpd and tomcat, that rely on Tibco will have connection problem, therefore Tibco restart is not supported.

- **ce_startup** – a script to combine all the start up scripts for different components.

  This script is located in: *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/*

  -all: default option that bring up all the services.

  -http: includes Apache, Tomcat, config server, image server, web service.

  -imgw: start imgw server.

  -eventgw: event gateway including event gateway crypto. This script should read the setup data file, *varsetup.dat*, for the user input *enable_ssl*, if the answer if **y** (yes), this script should run EvtGatewayCrypto; otherwise run EvetGateway.

  -monitor: Configuration Engine Monitor scripts.

- **ce_shutdown** – a script to combine all the stop scripts for different components.

  This script is located in: *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/*

  -all: default option that bring down all the services.

  -http: includes Apache, Tomcat, config server, image server, webservice

  -imgw: imgw server.

  -evtgw: event gateway including event gateway crypto.

  -monitor: Configuration Engine Monitor scripts.

Registering 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 can occur.

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

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 your host, 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 *server.crt* are transferred (FTP) into your host as part of its setup process.

Verifying Software Installation

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

The Cisco Configuration Engine supports:

- Netscape 5.0 and above.
- Internet Explorer 6.0 and above.
- FireFox 1.0 and above.

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

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

where: <*ip_address*> is the IP address you entered during host system configuration. 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***>.**

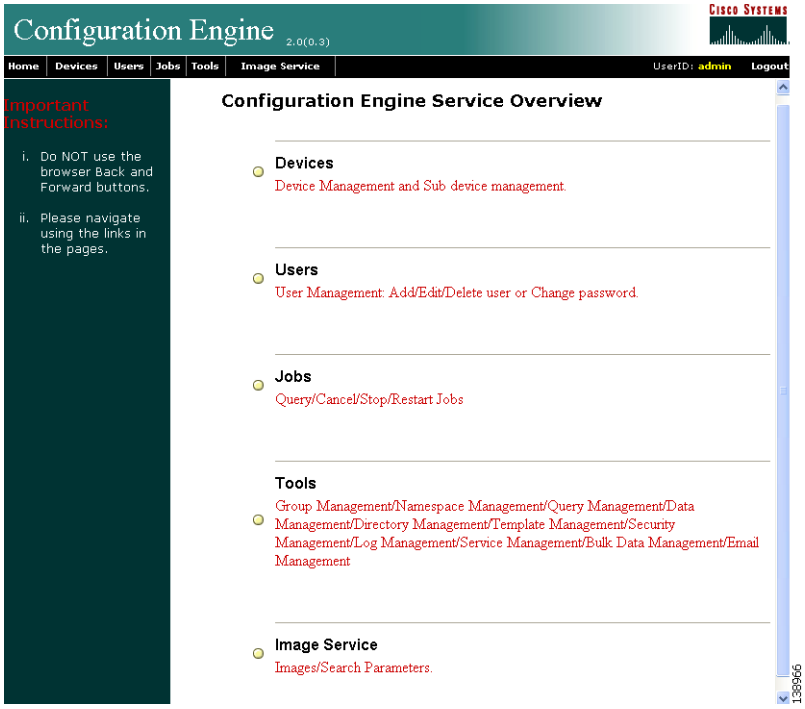
The Cisco Configuration Engine login page appears.

Step 3 Enter the ConfigService AdminID and Password that you entered during host system configuration.

The Home page appears.

If you have reached the Cisco Configuration Engine Home page (Figure 2-1), you have verified the successful installation on the Cisco Configuration Engine.

Figure 2-1 Internal Directory Mode Home Page



Re-imaging 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 uninstalling the Cisco Configuration Engine software, then reinstall the Cisco Configuration Engine, 2.0 software.

R

S

U