CHAPTER 2

Running the Setup Program

This chapter provides information about how to use the Setup program to configure your host system for Cisco Configuration Engine 3.5.3.

This chapter contains the following sections:

Tip The Encryption and Authentication settings in the Setup program allow you to enable security so that communication between the Cisco Configuration Engine and CNS Agents is secure. We strongly recommend that you enable security by answering **y** to the Encryption and Authentication setup prompts. For details, see Encryption Settings, page 2-7 and Authentication Settings, page 2-8. To enable security in the CNS agent devices, see Chapter 4, "Setting Up CNS Agent Devices for Secure Communication."

Running Setup

System configuration for Cisco Configuration Engine 3.5.3 is accomplished using the Setup program. You must run the Setup program when you start the system for the first time. Before running the Setup program, make sure you're in BASH shell mode. At the prompt, enter:
/bin/bash, SHELL=/bin/bash, export SHELL

Then, from the directory where Cisco Configuration Engine 3.5.3 software files are located, use the **./setup** command.

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 the Setup program must contain alphanumeric characters *only*. Special characters have different meanings in the UNIX shell and should *not* be used for passwords.
- Device Name values can contain the following characters only: period (.), underscore (_), hyphen (-), and alphanumeric characters.
- Group Name values can contain the following characters only: underscore (_) and alphanumeric characters.

Internal Directory Mode Setup Prompts

The following example 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.

Note To understand the internal mode setup prompts, see Understanding the Internal Mode Setup Parameters, page 2-6.

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

Enter country code: us
Enter company code: cisco

Do you want to authenticate Configuration Engine GUI users externally?
(y/n) [n] y
Enter IP Address of external directory server: 17x.xx.xxx.xxx
Enter port number of external directory server: [389]
Enter prefix for user name in external directory server: [cn]
Enter suffix for user name in external directory server: o=myorg,c=us
Do you want to enable authorization? (y/n) [n] y
Enter UserDN for external directory server: cn=simpleuser,o=myorg,c=us
Enter password for the above user: *****
Re-enter password for the above user: *****
Enter role attribute name in user objectclass which defines the role:
[description]
Enter role attribute value which defines the role of an administrator:
[administrator]

        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 port number: [389]
Enter internal LDAP server password: *****
Re-enter internal LDAP server password: *****
```

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

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

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

Enable cryptographic (crypto) operation between Event Gateway(s)/Config
server and device(s) (y/n)? [n] y
Enter absolute pathname of server key file: [/user/server.key]
Enter absolute pathname of server certificate file: [/user/server.crt]

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] y

The default bootstrap password should be the same as the "cns password" specified in your
bootstrap file. If you are not sure what it is and would like to finish the setup now, you
could enter a default password of your choice and then change it by using "update" option
through the Security Manager bootstrap GUI.

Enter the default bootstrap password:*****
Re-enter the default bootstrap password: *****

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]

The event gateway ports 11011 and 11012 are reserved for port
        automatic allocation. If you want to zero touch deploy your devices
        or have devices currently configured to use to these 2 ports, then
        you should enable this feature and enter the current "cns event"
        commands in the later part of this setup. For details please refer
        to the CE installation and configuration guide.

Enable Event Gateways port automatic allocation (y/n)? [y]

        Each Event Gateway process serves 500 devices. Maximum number of
        Event Gateways allowed is 10.

Enter number of Event Gateways that will be started with crypto operation:
[0] 10
Is this a primary CE (y/n)? [y]
```

```
The CNS Event command configures how the managed devices should connect to this particular
CE. The command entered in the following line should match what's configured on the
devices WITHOUT the "cns event imgw-test35" and port number portion of the CLI.

For example, if "cns event imgw-test35 11011 source Vlan1 keepalive 120 2 reconnect 10" is
configured on devices, then the command "source Vlan1 keepalive 120 2 reconnect 10" should
be entered in the following line.
If this is a backup CE and CLI  "cns event imgw-test35 11011 source Vlan1 backup" is
configured on devices, then the command "source Vlan1 backup" should be entered in the
following line.

Unable to enter a correct CLI could cause the managed devices not be able to connect to
this CE.

Enter CNS Event command: cns event imgw-test35 11011 source Vlan1 keepalive 120 2
reconnect 10
Enter Cisco-CE Event Bus Network Parameter: [imgw-test35]
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]

Current settings of IMGW:
-------------------------
Gateway ID: imgw-test35
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]

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

Enter CE Monitor timer (seconds): [1800]

Web Services 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]
```

```
Multi-Zone Settings:
--------------------

Your box has multiple IP Addresses assigned: 17x.xx.xxx.xx 17x.xx.xxx.xxx
You can create http zones so that http traffic can be limited on the IP Address
17x.xx.xxx.xx. Only selected URLs can be accessed using IP Address 17x.xx.xxx.xx. For
details, you can check the CE Installation and Configuration Guide.

Do you want to create zones to have limited access to CE from public
network (y/n)?  [n] y
Do you want to allow plain-text http access to CE from public network
(y/n)?  [y] y

Please review the following parameters:
country code: us
company code: cisco
Do you want to authenticate Configuration Engine GUI users externally? (y/n) y
IP Address of external directory server: 172.xx.xxx.1xx
port number of external directory server: 389
prefix for user name in external directory server: cn
suffix for user name in external directory server: o=myorg,c=us
Do you want to enable authorization? (y/n) y
UserDN for external directory server: cn=simpleuser,o=myorg,c=us
password for the above user: *****
role attribute name in user objectclass which defines the role: description
role attribute value which defines the role of an administrator: administrator
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)? y
absolute pathname of server key file: [/user/server.key]
absolute pathname of server certificate file: [/user/server.crt]
Enable plaintext operation between Config Server and devices/GUI administration (y/n)? y
Enable plaintext operation between Event Gateway and devices (y/n)? y
port number for http web access: 80
port number for https web access: 443
Tomcat internal port number: 8009
Tomcat shutdown port number: 8005
Enable authentication (y/n)? y
the default bootstrap password: *****
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 crypto operation: 10
Is this a primary CE (y/n)? y
CNS Event command: cns event imgw-test35 11011 source Vlan1 keepalive 120 2 reconnect 10
Cisco-CE Event Bus Network Parameter: imgw-test35
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
```

```
Do you want to create zones to have limited access to CE from public network (y/n)? y
Do you want to allow plain-text http access to CE from public network (y/n)? y

Warning: setup cannot be aborted while committing changes.
```

Understanding the Internal Mode Setup Parameters

The following sections describe the setup parameters:

- Login Name, LDAP Password, LDAP Port Number Settings, page 2-6
- Email Service Setting, page 2-6
- Encryption Settings, page 2-7
- Authentication Settings, page 2-8
- Event Services Settings, page 2-9
- Web Services Settings, page 2-11

Login Name, LDAP Password, LDAP Port Number Settings

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

Enter internal LDAP server port number: Define the port number that should be used by the Lightweight Directory Access Protocol (LDAP) server. Default value is 389.

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

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 port number	Port number	0 – 65535
Internal LDAP server password	Password	1 – 20

- 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

Note The Encryption and Authentication settings in the Setup program allow you to enable security so that communication between the Cisco Configuration Engine server and CNS agent devices is secure. We strongly recommend that you enable security by answering **y** to the Encryption and Authentication setup prompts. To enable security in the CNS agent devices, see Chapter 4, "Setting Up CNS Agent Devices for Secure Communication."

Note For scalability, we recommend that you distribute devices evenly among Event Gateway ports. See Chapter 6, "Scalability Among Event Gateway Ports."

Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s) (y/n): This option enables crypto Secure Socket Layer (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 "Configuring SSL Certificates" section on page 2-20 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 Services Settings" section on page 2-9).

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 key file	Alphanumeric	1 – 255
Absolute pathname of certificate file	Alphanumeric	1 – 255

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

Parameter	Type	Length/Range
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

Note The Encryption and Authentication settings in the Setup program allow you to enable security so that communication between the Cisco Configuration Engine server and CNS agent devices is secure. We strongly recommend that you enable security by answering **y** to the Encryption and Authentication setup prompts. To enable security in the CNS agent devices, see Chapter 4, "Setting Up CNS Agent Devices for Secure Communication."

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**.

Enter the default bootsrap password: Define the default bootstrap password for accessing the Cisco Configuration Engine GUI. The password should be same as the **cns password** specified in your bootstrap file. If you are not sure what it is and would like to finish the setup now, you could enter a default password of your choice and then change it by using "update" option through the Security Manager bootstrap GUI.

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	—
Enter the default bootstarp password	Alphanumeric	—

External Authentication

The Cisco Configuration Engine can authenticate a user by using external authentication application. When a user logs into the Cisco Configuration Engine, instead of authenticating the user by using the Cisco Configuration Engine LDAP server, the Cisco Configuration Engine forwards the authentication request to an external authentication application. The Cisco Configuration Engine can support the LDAP based authentication and integrate with the MS Active Directory.

The Cisco Configuration Engine can authenticate the user both internally and externally based on the user selection during the Cisco Configuration Engine setup.

During the Cisco Configuration Engine setup, the administrator can select the authentication mode. The Cisco Configuration Engine prompts for IP address and user credentials for the remote LDAP server.

Choose the authentication mode of the system *0=internal mode, 1=external mode*.

This example shows how to set the external authentication settings.

```
Enter IP Address of external directory server: 10.1.2.3
Enter port number of external directory server: [389]
Enter prefix for user name in external directory server: [cn]
Enter suffix for user name in external directory server: o=myorg,c=us
```

Authorization

The Cisco Configuration Engine does not support task or resource-based authorization. However, the Cisco Configuration Engine GUI have Admin and Operator user levels. Depending on the role of the user, the appropriate GUI screens are shown to the user.

Backup Authentication-Authorization

To support the existing Cisco Configuration Engine users, backup authentication and authorization is supported for the external authentication mechanism. The Cisco Configuration Engine user who logs in is authenticated against the external application. If the external authentication fails, the user is authenticated against the Cisco Configuration Engine LDAP Server. The fall-back server will be the LDAP directory used by the Cisco Configuration Engine (internal or external). If the user chooses internal authentication, the Cisco Configuration Engine LDAP is used for authentication and there will be no fall-back authentication server used.

Event Services 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 If crypto operation is disabled, this prompt is also disabled.

Is this a primary CE(y/n)? Specify the Cisco Configuration Engine as primary Cisco Configuration Engine.

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 For dual processor, 2GB RAM system, the number of Event Gateways should not exceed 20.

Event CNS Event Command: Specify the CNS event command to configure the network element to connect to this particular Cisco Configuration Engine. The command entered should match with what is configured on the network element without the event gateway port number. For example, if **cns event ce-host 11011 source Vlan1 keepalive 120 2 reconnect 10** is configured on the device, then the command **cns event <ce-host> source Vlan1 keepalive 120 2 reconnect 10** should be entered, where **<ce-host>** is the IP address or hostname of the Cisco Configuration Engine server.

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
Log backup (y/n)?	y, n	—
Number of Event Gateways that will be started with crypto operation	Integer	1-11 1-20 for dual processor, 2GB RAM

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

Parameter	Type	Range
Number of Event Gateways that will be started with plaintext operation	Integer	**crypto enabled:** 0-11 0-20 for dual processor, 2GB RAM **crypto disabled:**1-11 1-20 for dual processor, 2GB RAM
Is this a primary CE (y/n)	y, n	—
Event CNS Even Command	Command	—
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	—

Web Services 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 application programming interface (API) to resolve subjects.

Reconfigure IMGW Parameters

This section shows the set of prompts required for reconfiguring 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:
```

IMGW Parameter

Reconfigure 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 command-line interface (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.

Table 2-5 Valid Values for IMGW Parameters

Parameter	Type	Length/Range
Gateway ID	Alphanumeric	1 – 32
Run as daemon	y, n	
Timeout in seconds for a CLI command to complete	Integer	30 – 7200 (sec)
Timeout in seconds to get the next prompt in Telnet session	Integer	30 – 7200 (sec)
Remove temporary logs of Telnet sessions into devices	y, n	—
Location of temporary logs of Telnet sessions into devices	Full pathname	—
Concurrent Telnet Session Limit	Integer	1 – 25
Hoptest success retry interval (sec)	Integer	0 – 2147483647 (sec)
Hoptest failure retry interval (sec)	Integer	0 – 2147483647 (sec)
Logging level	verbose, error, silent	—
Log file prefix	Alphanumeric	1 – 32
Log file size (bytes)	Integer	5242880 – 4294967295 (bytes)
Log file rotation timer (minutes)	Integer	0 – 2147483647 (sec)
Log file rotation timer (seconds)	Integer	0 – 2147483647 (sec)
Logging mode	append, overwrite	—
Username prompt for device using TACACS/RADIUS	Printable ASCII characters	—
Password prompt for device using TACACS/RADIUS	Printable ASCII characters	—

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 the Setup program in Internal Directory Mode again to enable them.

The example 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.

Note To understand the external mode setup prompts, see Understanding the External Mode Setup Parameters, page 2-16.

```
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 key file: /a/b/c
Enter absolute pathname of 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 20.
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:
----------------------------
Do you want to authenticate Configuration Engine GUI users using external
Server ? (y/n) [n] y
Enter IP Address of external directory server: 10.1.2.3
Enter port number of external directory server: [389]
Enter prefix for user name in external directory server: [cn]
Enter suffix for user name in external directory server: o=myorg,c=us
Do you want to enable authorization? (y/n) [n] y
Enter UserDN for external directory server: cn=simpleuser,o=myorg,c=us
Enter password for the above user: *****
Re-enter password for the above user: *****
Enter role attribute name in user objectclass which defines the role: description
Enter role attribute value which defines the role of an administrator: admin

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]
```

Understanding the External Mode Setup Parameters

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 "Understanding the Internal Mode Setup Parameters" section on page 2-6.

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

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

Directory server login name: Directory user that has the administrative privileges for all objects under Cisco-CE context; for example, **admin**.

Directory server password: Directory user password.

User DN: The complete distinguished name for the 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: Choose **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 Directory Server	IP address	—
Port number of the Directory Server	Port number	0 – 65535
Directory server login name	Alphanumeric	1 – 32
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/Stop Components

Cisco Configuration Engine 3.5.3 supports start/stop for the following components:

- http/tomcat (webserver): **/etc/init.d/httpd {start|stop}**
- IMGW: **/etc/init.d/Imgw {start|stop}**
- Event gateway: **/etc/init.d/EvtGateway {start|stop} [port number]**
- Event gateway crypto: **/etc/init.d/EvtGatewayCrypto {start|stop} [port number]**

Cisco Configuration Engine 3.5.3 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 is **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 (CA) for signing.

Note The files *server.key* and *server.crt* must be present on your host system.

Verifying Software Installation

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

The Cisco Configuration Engine supports:

- Java SE Development Kit 6 update 5 and above
- Internet Explorer 6.0 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***>.**

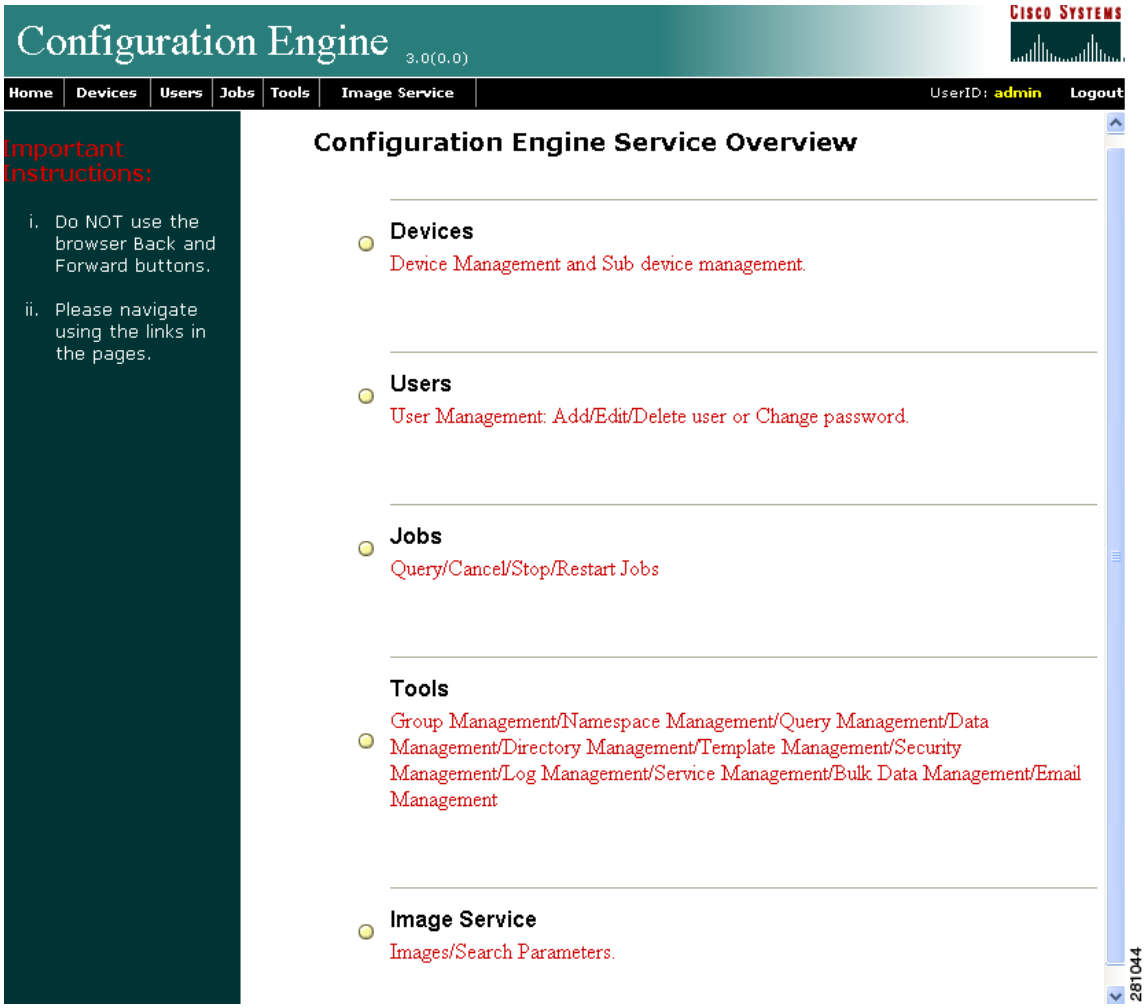
The Cisco Configuration Engine login page appears.

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



Reimaging System

If the image on your hard disk becomes corrupted, but the disk is operational (you can restart from the hard disk), you can reimage your system by uninstalling the Cisco Configuration Engine software, then reinstalling it.