



Cisco Media Delivery Engine Administration Guide

September 2012

Americas 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: 408 527-0883

Text Part Number: OL-24528-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Media Delivery Engine Administration Guide
© 2011-2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface	iii
What's in This Guide	iii
Document Revision History	iii
Document Organization	iv
Conventions	iv
Related Documentation	v
Obtaining Documentation and Submitting a Service Request	v
Managing the Media Delivery Engine Appliance	1-1
CIMC Prerequisites	1-1
Configure CIMC Network Settings and Password	1-2
Logging Into the CIMC Web Interface	1-3
Logging Out of the CIMC Web Interface	1-3
Logging Into the CIMC CLI Interface	1-3
Configure CIMC Remote Access Settings	1-4
Accessing the Cisco ECDS CLI Interface through the CIMC Interface	1-5
Managing the Server	1-5
Powering On the Server	1-6
Powering Off the Server	1-6
Power Cycling the Server	1-6
Resetting the Server	1-6
Shutting Down the Server	1-7
Enabling the Virtual KVM	1-7
Enabling Virtual Media	1-7
MDE Software and System Recovery	2-1
Software Recovery	2-1
System Recovery	2-4
Mount the Recovery Image as a Virtual Drive	2-5
Install the Recovery Image	2-6
Configure Basic Settings	2-9
Managing Spares	2-10



Preface

Created: March 2011

This chapter contains the following sections:

- [What's in This Guide, page iii](#)
- [Document Revision History, page iii](#)
- [Document Organization, page iv](#)
- [Conventions, page iv](#)
- [Related Documentation, page v](#)
- [Obtaining Documentation and Submitting a Service Request, page v](#)

What's in This Guide

The Cisco Media Delivery Engine (Cisco MDE) is the hardware platform upon which the Cisco Enterprise Content Delivery System (Cisco ECDS) software runs. This guide describes how to use the Cisco Integrated Management Controller (Cisco CIMC), an integrated appliance management interface, to remotely manage the Cisco MDE hardware and to perform system and software recovery.



Note

This guide does not describe how to configure software features on your system. For software configuration information, see the software configuration guide and the command reference.

For hardware specifications and installation information, see the hardware installation guide for your MDE.

To manage spares on your system, see the Cisco MDE 1100 Series and Cisco MDE 3100 Series hardware installation guides.

Find a link to all related documentation in the [“Related Documentation” section on page v](#).

Document Revision History

[Table 1](#) describes document update history.

Table 1 Document Revision History

Date	Change Summary
March 2011	This is the first version of this document.

Document Organization

Table 2 lists the chapters in this guide.

Table 2 Document Organization

Chapter	Description
Chapter 1, “Managing the Media Delivery Engine Appliance”	How to use the Cisco Integrated Management Controller to manage the MDE appliance.
Chapter 2, “MDE Software and System Recovery”	How to perform software and system recovery on the Cisco MDE appliance.

Conventions

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

Convention	Description
boldface font	Commands, keywords, and button names are in boldface .
<i>italic font</i>	Variables for which you supply values are in <i>italics</i> . Directory names and filenames are also in italics.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Variables you enter are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
string	Defined as a nonquoted set of characters. For example, when setting a community string for SNMP to “public,” do not use quotation marks around the string, or the string will include the quotation marks.
vertical bars ()	Vertical bars separate alternative, mutually exclusive, elements.
{ }	Elements in braces are required elements.
[]	Elements in square brackets are optional.
{ x y z }	Required keywords are grouped in braces and separated by vertical bars.

Convention	Description
[x y z]	Optional keywords are grouped in brackets and separated by vertical bars.
[[{ }]]	Braces within square brackets indicate a required choice within an optional element.

**Note**

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

Related Documentation

For complete document support for the Cisco Media Delivery Engine appliances and the Cisco Enterprise Content Delivery System, see the [Documentation for the Enterprise Content Delivery System \(Cisco Cisco ECDS\)](#) document roadmap at the following link:

[http://www.cisco.com/en/US/docs/video/Cisco ECDS/documentation.html](http://www.cisco.com/en/US/docs/video/Cisco_ECDS/documentation.html)

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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.





CHAPTER 1

Managing the Media Delivery Engine Appliance

Use the Cisco Integrated Management Controller (CIMC) to remotely control and manage your MDE appliance. CIMC is a separate management module that is built into the appliance. It has its own network configuration and processor, which runs the CIMC software separately from the Cisco ECDS software. This allows you to access and monitor the appliance even when the Cisco ECDS software is not running. You can access CIMC through a web-based or command-line interface (CLI).

This chapter describes the most common CIMC features you will use:

- [CIMC Prerequisites, page 1-1](#)
- [Configure CIMC Network Settings and Password, page 1-2](#)
- [Logging Into the CIMC Web Interface, page 1-3](#)
- [Logging Out of the CIMC Web Interface, page 1-3](#)
- [Logging Into the CIMC CLI Interface, page 1-3](#)
- [Configure CIMC Remote Access Settings, page 1-4](#)
- [Accessing the Cisco ECDS CLI Interface through the CIMC Interface, page 1-5](#)
- [Managing the Server, page 1-5](#)
- [Enabling the Virtual KVM, page 1-7](#)
- [Enabling Virtual Media, page 1-7](#)

CIMC Prerequisites

To use the CIMC web-based interface, you need a remote host with a web browser and the following minimum requirements:

- Java 1.6 or later
- HTTP and HTTPS enabled
- Adobe Flash Player 10 or later

To use the CLI interface, you need a remote host with an SSH client.

Configure CIMC Network Settings and Password


Caution

DO NOT change the network interface controller (NIC) mode or NIC redundancy settings. Changing these settings may cause severe performance degradation. The supported NIC mode is “Dedicated” and the supported NIC redundancy setting is “None.”

Step 1

Power on the Cisco MDE appliance.

Step 2

During the boot process, press **F8** when prompted to open the CIMC Configuration Utility. This utility allows you to make changes to the network settings and to reset the default CIMC password. See [Figure 1-1](#).


Note

You can use DHCP on the device management interface. Allow the appliance to boot and to obtain network settings from your DHCP server. The new IP and MAC addresses are displayed on the Cisco logo screen during subsequent boots. However, we recommend using static IP settings.

Figure 1-1 CIMC Configuration Utility

```

CIMC Configuration Utility  Version 1.5  Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                   None:           [X]
Shared LOM:     [ ]                   Active-standby:[ ]
Cisco Card:     [ ]                   Active-active:  [ ]
IPV4 (Basic)   Factory Defaults
DHCP enabled:   [ ]                   CIMC Factory Default:[ ]
CIMC IP:        10.194.51.91           Default User (Basic)
Subnetmask:     255.255.255.240        Default password:
Gateway:        10.194.51.81          Reenter password:
VLAN (Advanced)
VLAN enabled:   [ ]
VLAN ID:        1
Priority:        0
*****
<Up/Down arrow> Select items    <F10> Save    <Space bar> Enable/Disable
<F5> Refresh                    <ESC> Exit

```

Step 3

Define static network settings by entering values in the following fields:

- DHCP Enabled—Remove the check mark from this box to use static settings.
- CIMC IP—Enter the IP address for the appliance in this field.
- Subnet Mask—Enter the subnet mask for the appliance in this field.
- Gateway—Enter the gateway for the appliance in this field.

- Step 4** Change the default CIMC password:
- Use the Up/Down arrow keys to move the insertion point to Default password under Default User.
 - Type the new password.
 - Type the password again in the Reenter password field.
- Step 5** Press **F10** to save your changes and reboot the appliance.



Note Changes to the settings take effect after approximately 45 seconds. Refresh the view with **F5** to verify the new settings.

After the appliance has been assigned an IP address, you can use that address in a browser to access the CIMC GUI management system.

Logging Into the CIMC Web Interface

The default username for the appliance is **admin**. The default password for the appliance is **password** (unless you changed it in the [“Configure CIMC Network Settings and Password”](#) section on page 1-2).

- Step 1** In your web browser, type or select the web link for CIMC:
- ```
http://cimc_addr/
```
- Step 2** If a security dialog box displays, do the following:
- (Optional) Check the check box to accept all content from Cisco.
  - Click **Yes** to accept the certificate and continue.
- Step 3** In the log in window, enter your username and password.
- Step 4** Click **Log In**.

## Logging Out of the CIMC Web Interface

- Step 1** In the upper right of CIMC, click Log Out.  
Logging out returns you to the CIMC log in page.
- Step 2** (Optional) Log back in or close your web browser.

## Logging Into the CIMC CLI Interface

The default username for the appliance is **admin**. The default password for the appliance is **password** (unless you changed it in the [“Configure CIMC Network Settings and Password”](#) section on page 1-2).

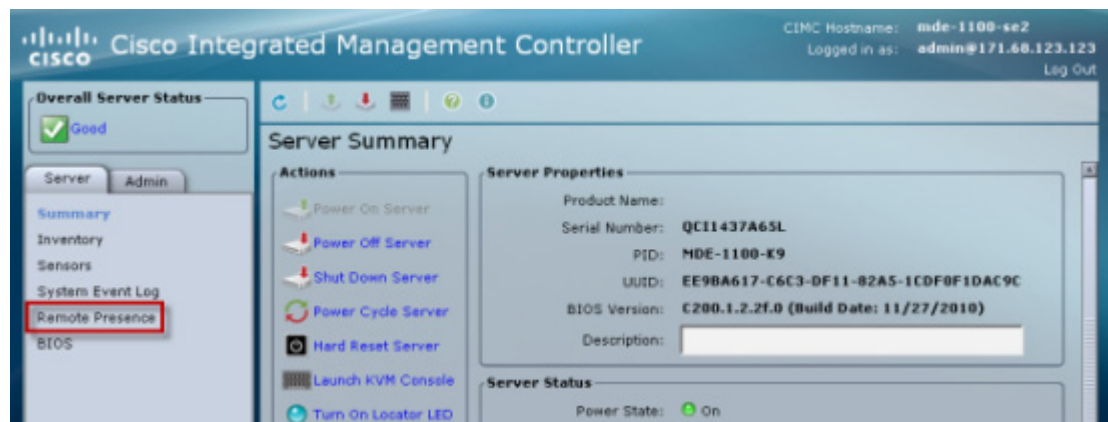
Point your SSH client to the CIMC IP address using port 22.

## Configure CIMC Remote Access Settings

Enabling the Serial over LAN remote access setting allows the input and output of the serial port of the Cisco ECDS software to be redirected over IP. Configure and use Serial over LAN on your server when you want to reach the Cisco ECDS console through CIMC.

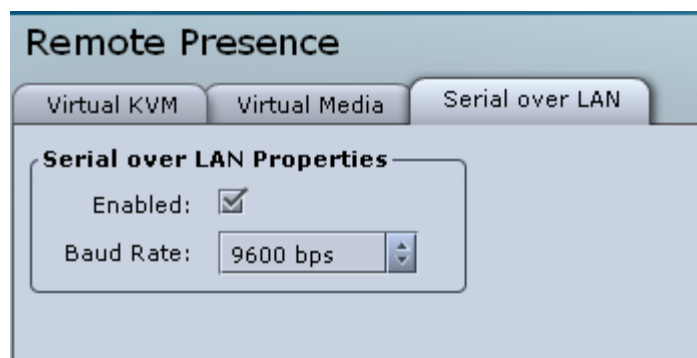
- 
- Step 1** Log into the CIMC GUI.
  - Step 2** On the Server tab, click **Remote Presence**, as shown in [Figure 1-2](#).

**Figure 1-2** Server Summary



- Step 3** Click the Serial over LAN tab ([Figure 1-3](#)).

**Figure 1-3** Remote Presence Window - Serial over LAN Tab



- Step 4** Check the Enabled checkbox and choose **9600** bps from the Baud Rate list.
  - Step 5** Click **Save Changes**.
  - Step 6** Proceed to [Accessing the Cisco ECDS CLI Interface through the CIMC Interface](#).
-

# Accessing the Cisco ECDS CLI Interface through the CIMC Interface

You can log into the Cisco ECDS console interface through the CIMC console interface. You need to supply your Cisco ECDS username and password when logging into the Cisco ECDS console. The default Cisco ECDS username is **admin** and the default password is **default**.

## Prerequisites

You must have the Serial over LAN setting enabled. Go back to [Configure CIMC Remote Access Settings, page 1-4](#) for more information.

## Procedure

- 
- |               |                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Log into the CIMC CLI interface using SSH. See <a href="#">Logging Into the CIMC CLI Interface, page 1-3</a> . |
| <b>Step 2</b> | Enter <b>connect host</b> .<br>The Cisco ECDS login prompt appears.                                            |
| <b>Step 3</b> | Enter your Cisco ECDS username and press <b>Enter</b> .                                                        |
| <b>Step 4</b> | Enter your Cisco ECDS password and press <b>Enter</b> .                                                        |
- 

## Managing the Server

This section contains the following server management topics:

- [Powering On the Server, page 1-6](#)
- [Powering Off the Server, page 1-6](#)
- [Power Cycling the Server, page 1-6](#)
- [Resetting the Server, page 1-6](#)
- [Shutting Down the Server, page 1-7](#)

## Powering On the Server

**Note**

If the server was powered off by any means other than through CIMC, it will not become active immediately when powered on. The server will remain in standby mode until CIMC completes initialization.

- 
- Step 1** In the Navigation pane, click the **Server** tab.
  - Step 2** On the Server tab, click **Summary**.
  - Step 3** In the Actions area, click **Power On Server**.  
A dialog box with the following message appears: “Power on the server?”
  - Step 4** Click **OK**.
- 

## Powering Off the Server

- 
- Step 1** In the Navigation pane, click the **Server** tab.
  - Step 2** On the Server tab, click **Summary**.
  - Step 3** In the Actions area, click **Power Off Server**.  
A dialog box with the following message appears: “Power Off the Server?”
  - Step 4** Click **OK**.
- 

## Power Cycling the Server

- 
- Step 1** In the Navigation pane, click the **Server** tab.
  - Step 2** On the Server tab, click **Summary**.
  - Step 3** In the Actions area, click **Power Cycle Server**.  
A dialog box with the following message appears: “Power Cycle the Server?”
  - Step 4** Click **OK**.
- 

## Resetting the Server

- 
- Step 1** In the Navigation pane, click the **Server** tab.
  - Step 2** On the Server tab, click **Summary**.
  - Step 3** In the Actions area, click **Hard Reset Server**.

A dialog box with the following message appears: “Hard Reset the Server?”

**Step 4** Click **OK**.

---

## Shutting Down the Server

The Shut Down Server function in CIMC is not supported in this release. Follow the instruction in [Powering Off the Server, page 1-6](#), instead.

## Enabling the Virtual KVM

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location.

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives.

- 
- Step 1** In the Navigation pane, click the **Server** tab.
- Step 2** On the Server tab, click **Remote Presence**.
- Step 3** In the Remote Presence pane, click the **Virtual KVM** tab.
- Step 4** On the Virtual KVM tab, check the **Enabled** checkbox.
- 

## Enabling Virtual Media

- 
- Step 1** In the Navigation pane, click the **Server** tab.
- Step 2** On the Server tab, click **Remote Presence**.
- Step 3** In the Remote Presence pane, click the **Virtual Media** tab.
- Step 4** Check the **Enabled** checkbox.
- Step 5** (Optional) Check the **Enable Virtual Media Encryption** checkbox. If checked, all virtual media communications are encrypted.
- Step 6** Click **Save Changes**.
-







## CHAPTER 2

# MDE Software and System Recovery

---

There are two recovery procedures for the Cisco MDE:

- [Software Recovery, page 2-1](#)
- [System Recovery, page 2-4](#)

## Software Recovery

Software recovery recovers the software stored in Flash memory if it has become corrupted. System configuration and content is retained.

A corrupted system image can result from a power failure that occurs while a system image is being written to Flash memory. The rescue image can download a system image to the main memory of the device and write it to Flash memory.



### Caution

---

Only perform this procedure when instructed to by Cisco TAC.

---

### Prerequisites

- Log into the CIMC web interface. See [Logging Into the CIMC Web Interface, page 1-3](#).
- Log into the Cisco ECDS console interface using an SSH session through the CIMC interface. See [Accessing the Cisco ECDS CLI Interface through the CIMC Interface, page 1-5](#).
- Obtain the software recovery image from Cisco TAC. Host the software image on an FTP server that is accessible from the MDE.

### Procedure

To install a new system image using the rescue image:

- 
- Step 1** Reboot the server by choosing **Power Cycle Server** from the CIMC Server Summary page. Monitor your SSH session to the Cisco ECDS console. As the MDE reboots, boot messages appear in the console. Look for the following message:
- ```
[BOOT-PHASE3]: enter `***' for rescue image: ***[BOOT-PHASE3]: rescue image: 58 sectors
```
- Step 2** Enter *** (three asterisks) when the “enter `***’” prompt appears. The system boots to the software recovery interface. The example below walks you through the software recovery process. The values you enter may differ from those shown below.

This is the rescue image. The purpose of this software is to let you install a new system image onto your system's boot flash device. This software has been invoked either manually (if you entered `***` to the bootloader prompt) or has been invoked by the bootloader if it discovered that your system image in flash had been corrupted.

To download an image from network, this software will request the following information from you:

- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- FTP server IP address
- username and password on FTP server
- path to system image on server

System Recovery Menu:

1. Configure Network
2. Download and install system image
3. Exit (and reboot)

Choice [1]: **1**

Network Configuration Menu:

1. Configure ethernet interface
2. Configure portchannel interface
3. Exit to main menu

Choice [1]: **1**

Please enter an interface from the following list:

- 0: GigabitEthernet 1/0
- 1: GigabitEthernet 2/0

enter choice: Choice [0]: **0**

Using interface GigabitEthernet 1/0

Please enter the local IP address to use for this interface:

[Enter IP Address]: **10.194.52.1.92**

Please enter the netmask for this interface:

[Enter Netmask]: **255.255.255.240**

Please enter the IP address for the default gateway:

[Enter Gateway IP Address]: **10.194.51.81**

Network Configuration Menu:

1. Configure ethernet interface (done)
2. Configure portchannel interface
3. Exit to main menu

Choice [3]: **3**

System Recovery Menu:

1. Configure Network (done)
2. Download and install system image
3. Exit (and reboot)

Choice [2]: **2**

Please enter the IP address for the FTP server where you wish to obtain the new system image:

[Enter Server IP Address]: **171.68.123.123**

Please enter your username on the FTP server (or 'anonymous'):

[Enter Username on server (e.g. anonymous)]: **beaugus**

Please enter the password for username 'beaugus' on FTP server:

```
Please enter the directory containing the image file on the FTP server:  
[Enter Directory on server (e.g. /)]: /
```

```
Please enter the file name of the system image file on the FTP server:  
[Enter Filename on server]: cds52.sysimg
```

Here is the configuration you have entered:

```
Current config:  
    IP Address: 10.194.51.92  
    Netmask: 255.255.255.240  
Gateway Address: 10.194.51.81  
    Server Address: 171.68.123.123  
    Username: beaugus  
    Password: *****  
Image directory: /  
Image filename: cds52.sysimg
```

```
Attempting download...  
Downloaded 39111680 byte image file  
A new system image has been downloaded.  
You should write it to flash at this time.  
Please enter 'yes' below to indicate that this is what you want to do:  
[Enter confirmation ('yes' or 'no')]: yes  
Ok, writing new image to flash  
done.  
Finished writing image to flash.
```

```
System Recovery Menu:  
  1. Configure Network (done)  
  2. Download and install system image (done)  
  3. Exit (and reboot)  
Choice [3]: 3  
Restarting system.
```

Step 3 Log into the EDCS command line interface and verify the software version by running the **show version** command.

```
hcl-sr1#sh ver
```

```
Content Delivery System Software (CDS)  
Copyright (c) 1999-2011 by Cisco Systems, Inc.  
Content Delivery System Software Release 2.5.3 (build b360 Jan 25 2012)  
Version: MDE1100-2.5.3.360
```

```
Compiled 11:34:33 Jan 25 2011 by ipvbuild  
Compile Time Options: KQ SS
```

```
System was restarted on Wed Mar 9 19:37:00 2011.  
The system has been up for 4 minutes, 10 seconds.
```

Step 4 This completes the process of installing a new system image using the rescue image.

System Recovery

Cisco Cisco ECDS system recovery reimages the entire system (Flash and disk).

Use the Cisco Cisco ECDS system recovery procedure to recover an Cisco ECDS system that must be completely reimaged. This is the last resort procedure for installing the software. It will erase existing configurations and content.

**Caution**

Only perform this procedure when instructed to by the Cisco TA C.

**Note**

This process does not reimage the CIMC software.

Prerequisites

Before you begin:

- Enable the Serial over LAN in CIMC. See [Configure CIMC Remote Access Settings, page 1-4](#).
- Enable the Virtual KVM. See [Enabling the Virtual KVM, page 1-7](#).
- Enable Virtual Media. See [Enabling Virtual Media, page 1-7](#).
- Unregister the appliance in the Enterprise CDSM (if it is not the CDSM itself that you are reimaging).
- Obtain the system recovery image from the Cisco TAC and save it to your local drive.

Procedure

1. [Mount the Recovery Image as a Virtual Drive, page 2-5](#).
2. [Install the Recovery Image, page 2-6](#).
3. [Configure Basic Settings, page 2-9](#) (optional).

Mount the Recovery Image as a Virtual Drive

Before you can install the software, you must mount the recovery image as a virtual drive on the box. To mount the recovery image as a virtual drive:

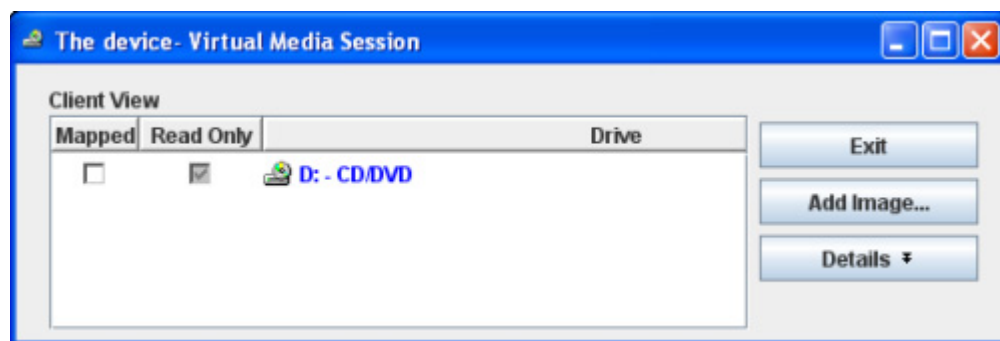
- Step 1** Log into the CIMC web interface:
http://cimc_addr/
- Step 2** Launch the KVM console. Click **Launch KVM Console** on the Server Summary page (Figure 2-1). You might have to approve the download and running of a Java component.

Figure 2-1 KVM Console Actions



- Step 3** In the KVM Console window, choose **Tools > Launch Virtual Media** (Figure 2-2).

Figure 2-2 Virtual Media Session



- Step 4** Click **Add Image**, browse to the system recovery image, and click **Open**.
- Step 5** Check the Mapped checkbox next to the entry that you added.



Tip Do not close the Virtual Media Session or KVM Console windows. You need to leave the windows open during the recovery procedure.

- Step 6** Proceed to [Install the Recovery Image, page 2-6](#).
-

Install the Recovery Image

During the system recovery image installation, you will have the CIMC web interface, CIMC KVM Console window, the Virtual Media Session window open, plus an SSH session open to perform and monitor the installation.

**Tip**

Follow each step carefully to verify which window to monitor for a given step.

Prerequisites

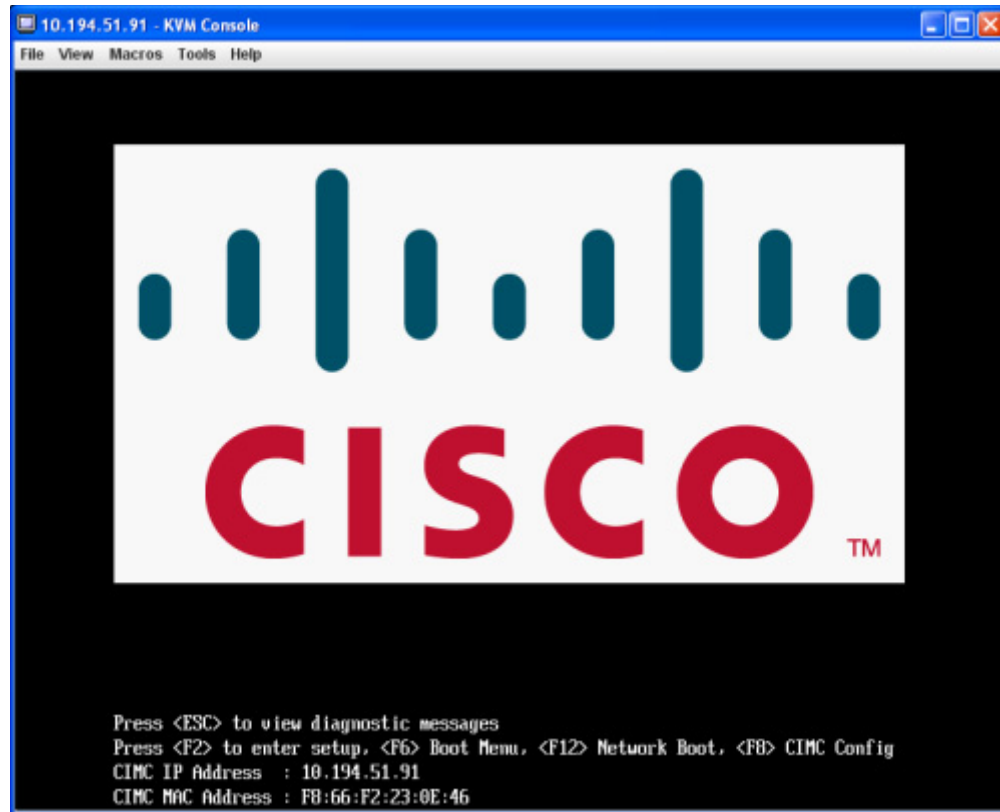
You must have mounted the system recovery image as a virtual drive before performing this procedure. See [Mount the Recovery Image as a Virtual Drive, page 2-5](#).

Procedure

To perform a remote install of the system recovery image:

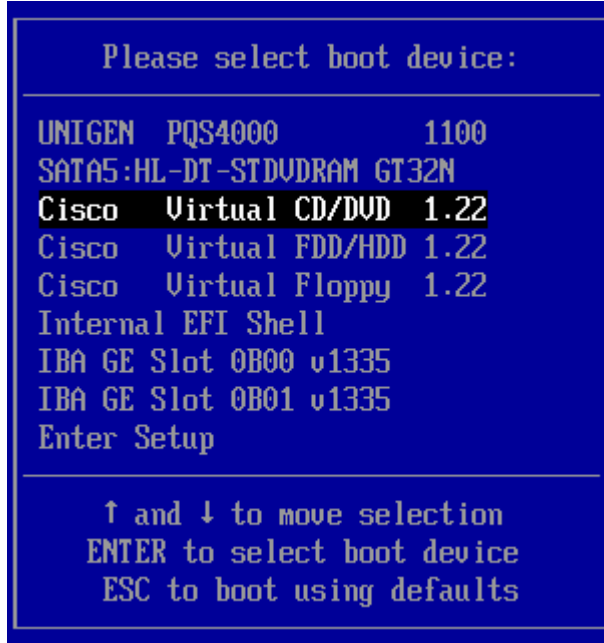
- Step 1** Start an SSH session to the Cisco ECDS console through the CIMC interface:
- a. Start the SSH session to the CIMC IP address. Use the CIMC username and password to connect.
 - b. Enter **connect host**.
- Step 2** From the CIMC web interface, click **Power Cycle Server**.
Monitor the KVM Console window. Make sure it is the active window.
- Step 3** Wait for the BIOS menu to appear in the KVM Console window ([Figure 2-3](#)).

Figure 2-3 KVM Console Window



Step 4 Press **F6** to enter the boot menu (Figure 2-4).

Figure 2-4 Boot Menu



- Step 5** From the boot menu, choose **Cisco Virtual CD/DVD** as the boot device. After you select the boot device, the system boots with the system recovery image. Monitor your SSH session to the Cisco ECDS console. After booting, the Installer Main Menu appears.

Installer Main Menu:

1. Configure Network
2. Manufacture flash
3. Install flash cookie
4. Install flash image from network
5. Install flash image from cdrom
6. Install flash image from disk
7. Wipe out disks and install .bin image
8. Exit (and reboot)
9. Force manufacturing flash

- Step 6** Type **9** and press **Enter**. This reformats the Flash. Type **y** and press **Enter** to confirm your choice.

- Step 7** Type **5** and press **Enter**.

Please select an image from the following list:

1. CDS25.sysimg
2. Return to Main Menu

- Step 8** Type **1** and press **Enter** to select the Flash image file. Type **y** and press **Enter** to proceed with writing the image to Flash.

Once the Flash is done being written, the Installer Main Menu appears.

- Step 9** Type **7** and press **Enter**. This installs the disk component of the software.
- You are prompted to provide a URL to the image. By default, the URL to the system recovery image on the virtual drive is provided.
- ```
Enter full URL of .bin image to install.
 ftp://[user:pass@]ip_addr/path/to/file
 http://[user:pass@]ip_addr/path/to/file
 file:/local/path/to/to/file
URL for .bin image [file:/cdrom/images/CDS25.bin]:
```
- Step 10** Press **Enter** to accept the default URL for the .bin image. Type **y** and press **Enter** to confirm that you want to install the image. Installing this image will overwrite all disks.
- When the image is done installing, the Installer Main Menu appears.
- Step 11** Type **8** and press **Enter** to reboot the system.
- Step 12** Type **y** and press **Enter** to confirm the reboot.
- When the system is done rebooting, you are prompted to configure basic settings.
- Step 13** Do one of the following:
- Ignore the prompt and configure the settings later using the **setup** command.
  - Press **Enter** to enter the setup mode. See [Configure Basic Settings, page 2-9](#).
- Step 14** Close the Virtual Media Session and KVM Console windows.
- 

## Configure Basic Settings

The example below walks you through the basic settings configuration. The interface you configure becomes the primary interface for the MDE.

```
What is the mode of the device (SE/SR/CDSM) [SE]:SE
Press the ESC key at any time to quit this session
```

```
Is this SE going to be managed by a
CDSM (Content Delivery System Manager) (y/n) [y]: y
Press the ESC key at any time to quit this session
Please choose an interface to configure from the following list:
1: GigabitEthernet 1/0
2: GigabitEthernet 2/0
```

```
Enter choice: 1
```

```
Do you want to enable DHCP on this interface (y/n) [y]: n
```

```
Please enter the IP address of this interface: 10.194.51.92
```

```
Please enter the netmask of this interface: 255.255.255.240
```

```
Please enter the default gateway: 10.194.51.81
```

```
Please enter the domain name server ip: 10.194.50.157
```

```
Please enter the domain name: Cisco ECDS.com
```

```
Please enter the hostname: hcl-se1
```

```
Please enter CDSM (Content Delivery System Manager) IP or Host name: 10.194.51.90
```

Configurations generated in the setup session will be applied after the device boots up fully.

You can redo this configuration, if needed, by issuing the CLI 'setup' any time after the device boots up.

For your reference, configuration generated during this setup session is available at /local1/setup\_gen\_config.txt. You can view this file with the command, "type /local1/setup\_gen\_config.txt".

Press any key to continue..

If you receive the error " cms: unable to register node " after rebooting, it is likely caused by the MDE still being registered with the CDSM. You can fix this by issuing the following commands:

```
cms deregister force
cms enable
```

## Managing Spares

To manage spare disks on your Cisco MDE, see the Cisco MDE 1100 Series and Cisco MDE 3100 Series hardware installation guides.



## INDEX

---

### C

#### CIMC

- accessing [1-1](#)
- CLI login [1-3](#)
- configuring network settings [1-2](#)
- prerequisites [1-1](#)
- standby mode [1-6](#)

#### CIMC Configuration Utility [1-2](#)

#### CIMC server

- power cycle [1-6](#)
- powering off [1-6](#)
- powering on [1-6](#)
- resetting [1-6](#)
- shutting down [1-7](#)

#### CLI

- accessing [1-5](#)

#### CMIC

- configuring
  - remote access [1-4](#)

---

### D

- default password [1-3](#)
- default username [1-3](#)

---

### M

- managing spare disks [i-iii](#)

#### MDE [2-10](#)

- configure basic settings [2-9](#)
- install new system image [2-1](#)
- recovery image

- remote install [2-6](#)
- virtual drive [2-5](#)
- registration [2-10](#)
- software recovery [2-1](#)
- system recovery [2-4](#)

---

### N

- network interface controller (NIC) mode [1-2](#)

---

### P

- password
  - default [1-3](#)

---

### U

- username, default [1-3](#)

---

### V

- virtual KVM
  - enabling [1-7](#)
- virtual media
  - enabling [1-7](#)

