Cisco IMC Supervisor Shell Guide, Release 2.2

First Published: 2017-07-11

Last Modified: 2018-06-06

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

CONTENTS

Preface

Audience

This guide is intended primarily for data center administrators who use Cisco IMC Supervisor and who have responsibilities and expertise in server administration.

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Text Type	Indication
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

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.

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.

Related Documentation

Cisco IMC Supervisor Documentation Set

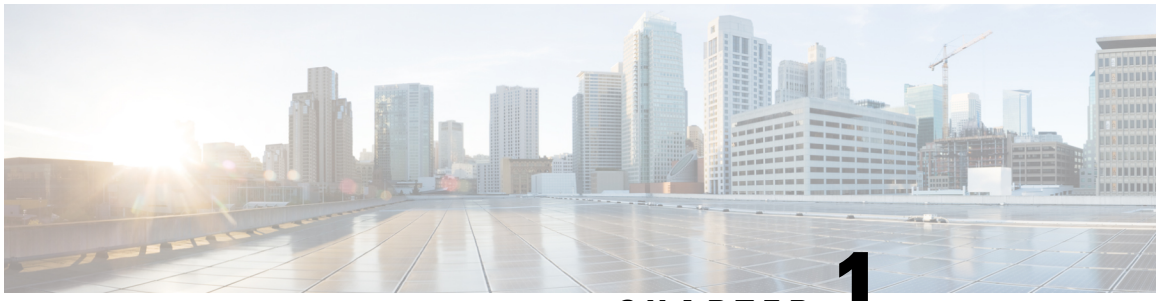
Following are the documents that are available for Cisco IMC Supervisor:

- Cisco IMC Supervisor Release Notes
- Cisco IMC Supervisor Installation and Upgrade on VMware Vsphere Guide
- Cisco IMC Supervisor Rack-Mount Servers Management Guide
- Cisco IMC Supervisor Shell Guide
- Cisco IMC Supervisor REST API Getting Started Guide
- Cisco IMC Supervisor REST API Cook Book

Other Documentation

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.



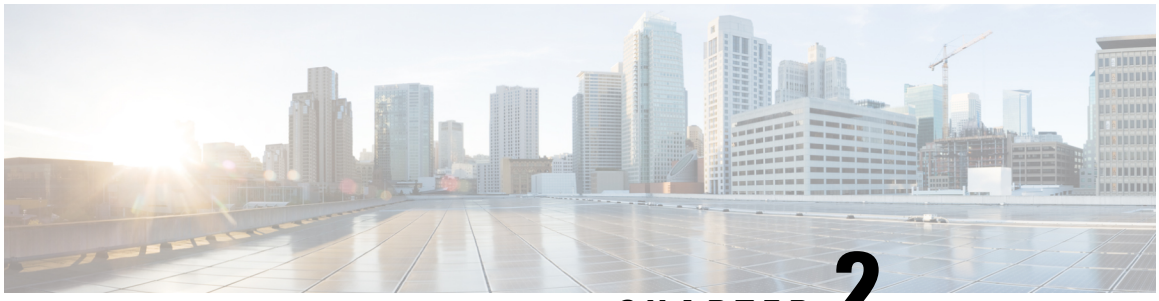
CHAPTER 1

New and Changed Information in this Release

New and Changed Information in Release 2.2(0.3)

The following table provides an overview of the significant changes to this guide for the release 2.2(0.3). The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Feature	Description	Where Documented
Shell options output updated to display additional details	This release introduces support for enabling and disabling HTTP in Cisco IMC Supervisor.	Enabling or Disabling HTTP, on page 19
	The Grant/Deny client access to MySQL port 3306 option allows you to allow or deny the external clients to access the MYSQL port.	Granting Client Access to MySQL Port, on page 18 Denying Client Access to MySQL Port, on page 19



CHAPTER 2

Overview

This chapter contains the following sections:

About Cisco IMC Supervisor

Cisco IMC Supervisor is a management system that allows you to manage rack mount servers on a large scale. It allows you to create groups of rack mount servers for monitoring and inventory purposes.

You can use Cisco IMC Supervisor to perform the following tasks for a rack mount server:

- Support for logical grouping of servers and summary views per group
- Collect inventory for the servers
- Provide monitoring capabilities for servers and groups
- Firmware management including firmware download, upgrade, and activation
- Manage standalone server actions including power control, LED control, log collection, KVM launch, CIMC UI launch and e-mail alerts
- Role Based Access Control (RBAC) to restrict access
- Policy driven configuration

About Cisco IMC Supervisor Shell Commands

This guide describes all of the commands available to you when logging into the Cisco IMC Supervisor shell. You can use these commands to perform the following administrative tasks:

- Changing ShellAdmin password
- Display Service Status
- Stopping/starting all Cisco services

- Stopping/starting the MySQL database
- Backing up/restoring the appliance database
- Synching up time
- Pinging hostname/IP address
- Version (Cisco IMC Supervisor appliance version)
- Generating Self-Signed Certificate and Certificate Signing Request
- Importing CA (JKS) file
- Configuring network interface
- Displaying network details
- Troubleshooting by using Tail Inframgr logs
- Applying a patch to the appliance
- Shutting down the Appliance
- Rebooting the Appliance
- Manage Root Access
- Login as Root
- Clean Up Patch Files
- Enabling or disabling the debug logging information
- Resetting MySQL user password
- Terminating active GUI user sessions
- Quitting the shell

For additional system administration information refer to the *Cisco IMC Supervisor Rack-Mount Servers Management Guide*.

Prerequisite

To successfully execute the commands described in this guide, Cisco IMC Supervisor should be up and running (and reachable).

Note The information in this guide is based on Cisco IMC Supervisor, release 1.0 and later releases.

Logging into the Shell

The login procedure requires the use of a Secure Shell (SSH) client and the correct login credentials. After gaining access to the Cisco IMC Supervisor appliance you can perform a wide variety of system administration tasks.

Before you begin

Obtain proper access to a Cisco IMC Supervisor appliance and a secure shell (SSH) application.

Step 1 Open your SSH application.

Step 2 Enter the Cisco IMC Supervisor appliance IP address.

Step 3 In the **Port** field, enter **22**.

The shell window displays the introductory **Cisco UCS Director Platform - Cisco IMC Supervisor Shell Menu**.

Step 4 In the **User** field, enter **shelladmin**.

Step 5 In the **Password** field, enter the default password, **changeme**.

You can modify the default password.

Step 6 Press **Enter**.

The following services are available for selection:

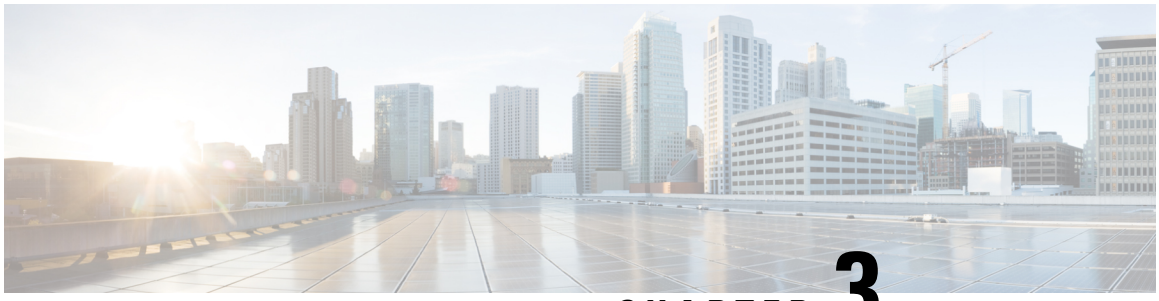
```
Cisco IMC Supervisor Shell Menu

         Select a number from the menu below

             1)  Change ShellAdmin password
             2)  Display Services Status
             3)  Stop Services
             4)  Start Services
             5)  Stop Database
             6)  Start Database
             7)  Backup Database
             8)  Restore Database
             9)  Time Sync
             10) Ping Hostname/IP Address
             11) Show version
             12) Generate Self-Signed Certificate and Certificate Signing Request
             13) Import CA/Self-Signed Certificate
             14) Configure Network Interface
             15) Display Network Details
             16) Tail Inframgr logs
             17) Apply Patch
             18) Shutdown Appliance
             19) Reboot Appliance
             20) Manage Root Access
             21) Login as Root
             22) Clean-up Patch Files
             23) Collect Diagnostics
             24) Enable/Disable Debug Logging
             25) Reset MySQL User Password
             26) Terminating active GUI session(s) for user
             27) Quit
```

```
SELECT>
```

Step 7 Enter the option number at the **SELECT>** prompt.



CHAPTER 3

Using Shell Commands

This chapter contains the following sections:

General Administration

This section describes how to execute common administration tasks such as changing your password, stopping and starting services, generating log and report data, as well as other common system administration tasks.

Changing ShellAdmin Password

Choose **Change ShellAdmin Password** to change the Cisco IMC Supervisor user's password.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Change ShellAdmin Password** and press **Enter**.

Information similar to the following is displayed:

```
 Changing password for user shelladmin.
New UNIX password:
```

Step 2 Enter the password and press **Enter**.

Displaying the Status of Your Services

The **Display Services** option displays all executed services. The **Display Services** option also displays the status of any associated databases and disks.

- Broker - An ActiveMQ JMS broker used for inter-process communication using JMS messages. All infra services use the broker to communicate between them.
- Controller
- Eventmgr

- Idaccessmgr - Provides authentication service for Cisco IMC Supervisor users (local, AD imported through LDAP). When you log in through the GUI, tomcat receives the login request and queries idaccessmgr to authenticate the user.
- Inframgr - The back-end server that proves APIs over JMS and REST. Tomcat (GUI) uses these back-end APIs.
- Websock (VNC interface) - VNC proxy. Cisco UCS Director provides browser based VNC access to the VM console. The websock service acts as a VNC proxy to the VM console.
- Tomcat - Hosts Cisco UCS Director GUI web app.
- Flashpolicyd
- Mysqld

Note Ensure that all of the above services are up and operating. If a service is not executed on Cisco IMC Supervisor, restart the service through the shell client.

From the **Cisco IMC Supervisor Shell Menu**, choose **`Display Services Status`**.

The following list of services appears:

```
Service                  State        PID
----------            ----------      -----
broker                   RUNNING      18718
controller               RUNNING      18758
eventmgr                 RUNNING      18792
idaccessmgr              RUNNING      18938
inframgr                 RUNNING      18997
websock                  RUNNING      9548
TOMCAT                   RUNNING      9515
flashpolicyd             RUNNING      9545
mysqld                   RUNNING      8069
 2693 ?        00:00:00 mysqld_safe
3170 ?        01:10:16 mysqld

Press return to continue ...
```

Note The corresponding status and process ID (PID) of each service is also displayed in the menu.

Stopping Cisco Services

You can stop all Cisco services that are part of the Cisco IMC Supervisor appliance by choosing **`Stop Services`**. You can verify that all services are stopped by choosing **`Display Services Status`**.

SUMMARY STEPS

1. From the **Cisco IMC Supervisor Shell Menu**, choose **`Stop Services`**.
2. Press **`Enter`**.

3. Press **Enter** to complete the procedure.

DETAILED STEPS

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Stop Services**.

Step 2 Press **Enter**.

Information similar to the following is displayed:

```
Do you want to stop services [y/n]? : y
Stopping service broker... [ OK ]
Stopping service controller... [ OK ]
Stopping service eventmgr... [ OK ]
Stopping service client... [ OK ]
Stopping service idaccessmgr... [ OK ]
Stopping service inframgr... [ OK ]
Stopping service websock... [ OK ]
Stopping service tomcat... [ OK ]
Stopping service flashpolicyd... [ OK ]
Press return to continue ...
```

Step 3 Press **Enter** to complete the procedure.

Starting Cisco Services

You can execute all services that are part of Cisco IMC Supervisor by choosing **Start Services**.

After using this option, you can choose **Display Services Status** to verify that all services have started and are running.

Note Services started in the background are not displayed.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Start Services**.

Information similar to the following is displayed:

```
Services are being started. Use "Display Services Status" option to check the status
Press return to continue ...
```

Step 2 Press **Enter** to complete the process.

Step 3 Choose **Display Service Status** to verify that the services are executed.

Synchronizing the System Time

You can synchronize the system time to the hardware time as well as the NTP server by choosing **Time Sync**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Time Sync**.

Step 2 Press **Enter**.

Information similar to the following is displayed:

```
Time Sync......
System time is Tue Sep 17 15:57:34 UTC 2013
Hardware time is Tue Sep 17 15:57:35 2013  -0.849104 seconds
Do you want to sync systemtime [y/n]? y
NTP Server IP Address: 172.25.168.203
5 Dec 03:24:02 ntpdate[5017]: step time server 172.25.168.203 offset 25510.954857 sec
Sync'ed with NTP SERVER 172.25.168.203
Press return to continue ...
```

Step 3 Press **y** and press **Enter** to synchronize to system time.

Step 4 Press **y** and press **Enter** to synchronize to the NTP server.

Step 5 Press **Enter** to complete the process.

Pinging the Hostname and IP Address

You can ping a hostname or IP address to test your connectivity by choosing **Ping Hostname/IP address**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Ping Hostname/IP addres** and press **Enter**.

Step 2 Enter the IP address to ping and press **Enter**.

Information similar to the following is displayed:

```
 Enter IP Address : 209.165.200.224
PING 209.165.200.224 (209.165.200.224) 56(84) bytes of data.
64 bytes from 209.165.200.224: icmp_seq=1 ttl=64 time=9.90 ms
64 bytes from 209.165.200.224: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 209.165.200.224: icmp_seq=3 ttl=64 time=0.254 ms
64 bytes from 209.165.200.224: icmp_seq=4 ttl=64 time=0.198 ms
64 bytes from 209.165.200.224: icmp_seq=5 ttl=64 time=0.267 ms

--- 209.165.200.224 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.198/2.187/9.901/3.857 ms
Press return to continue ...
```

Step 3 Press **Enter** to exit out of the operation.

Examining the Version Information

You can verify the Cisco IMC Supervisor version and build number by choosing **Show Version**. This information is required for debugging purposes.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Show Version** and press **Enter**.

Information similar to the following is displayed:

```
Cisco UCS Director Platform
------------------
Platform Version      : 5.1.0.1
Platform build Number : 51143
Product Name : Cisco IMC Supervisor
Product Version : 1.1.0.0
Press return to continue ...
```

Step 2 Press **Enter** to complete the process.

Configuring a Network Interface

You can configure a network interface for the Cisco IMC Supervisor appliance by choosing **Configure Network Interface**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Configure Network Interface** and press **Enter**.

Information similar to the following is displayed:

```
Do you want to Configure DHCP/STATIC IP  [D/S] ? : S
```

Step 2 Choose one of the following configuration selections:

- Choose **D** to configure a DHCP IP address.
- Choose **S** to configure a static IP address.

Step 3 Enter **s** to configure a static IP address and press **Enter**.

Information similar to the following is displayed:

```
Configuring STATIC configuration..
Enter the ethernet interface that you want configure E.g. eth0 or eth1:
```

Step 4 Enter the Ethernet interface to configure (for example, eth1) and press **Enter**.

Information similar to the following is displayed:

```
Configuring STATIC IP for eth1...
   IP Address: 209.165.200.224
   Netmask: 255.255.255.0
   Gateway: 209.187.108.1
   DNS Server1: 198.51.100.1
   DNS Server2: 203.0.113.1
Configuring Network with : INTERACE(eth1), IP(209.165.200.224), Netmask(255.255.255.0),
Gateway(209.187.108.1),
DNS Server1(198.51.100.1), DNS Serverx 2(203.0.113.1)

Do you want to continue  [y/n]? :
```

Step 5 Enter **n** to discontinue the configuration process.

Step 6 Press **y** to return to complete the process.

Displaying Appliance Network Details

You can display the Cisco IMC Supervisor appliance network details by choosing **Display Network Details**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose option **Display Network Details** and press **Enter**.

Information similar to the following is displayed:

```
Network details....
eth0      Link encap:Ethernet  HWaddr 00:50:56:97:1E:2D
          inet addr:192.0.2.23  Bcast:192.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::230:56gg:fe97:1e2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:189818223 errors:14832 dropped:17343 overruns:0 frame:0
          TX packets:71520969 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:105749301003 (98.4 GiB)  TX bytes:27590555706 (25.6 GiB)
          Interrupt:59 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1821636581 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1821636581 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:327846827946 (305.3 GiB)  TX bytes:327846827946 (305.3 GiB)

Press return to continue ...
```

Step 2 Press **Enter** to complete the process.

Viewing Tail Inframgr Logs

The **Tail Inframgr Logs** option enables you to see inframgr (Infrastructure Manager) log data, which are generated behind the scenes by using the Unix tail command. When you are debugging, you can trace problems by using this log data. Use the **Tail Inframgr Logs** option to immediately tail the most recent inframgr logs. The results are displayed on your screen directly after you select this option.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Tail Inframgr Logs** and press **Enter**.

Following are a few sample lines, typical of the results displayed immediately after you use the **Tail Inframgr Logs** option:

```
2015-05-04 09:51:31,569 [pool-15-thread-16] INFO  run(SystemTaskExecutor.java:55) - Preparing to
execute task: LeafAgentConnectivityCheckPeriodicTask; frequency=5 minutes; Priority=5
2015-05-04 09:51:31,577 [pool-15-thread-16] INFO  isSystemTaskRemotable(SystemTaskExecutor.java:282)
 - Task remoting is not allowed per policy: LeafAgentConnectivityCheckPeriodicTask
2015-05-04 09:51:31,581 [pool-15-thread-16] INFO  updateStatus(SystemTaskStatusProvider.java:181) -
 Task: task.LeafAgentConnectivityCheckPeriodicTask changed state to OK
```

```
2015-05-04 09:51:31,592 [pool-15-thread-16] INFO  executeLocally(SystemTaskExecutor.java:133) -
Executing task locally: LeafAgentConnectivityCheckPeriodicTask
2015-05-04 09:51:31,592 [pool-15-thread-16] INFO  getClusterLeaf(ClusterPersistenceUtil.java:81) -
Leaf name LocalHost
2015-05-04 09:51:31,598 [pool-15-thread-16] INFO  updateStatus(SystemTaskStatusProvider.java:181) -
 Task: task.LeafAgentConnectivityCheckPeriodicTask changed state to In Progress
2015-05-04 09:51:31,604 [pool-15-thread-16] INFO  executeLocally(SystemTaskExecutor.java:149) - Start
 executing task. name=LeafAgentConnectivityCheckPeriodicTask; status=OK; lastExecuted=1430732791586
2015-05-04 09:51:31,608 [pool-15-thread-16] INFO
execute(LeafAgentConnectivityCheckPeriodicTask.java:33) - Retry : 0
2015-05-04 09:51:31,611 [pool-15-thread-16] INFO  executeLocally(SystemTaskExecutor.java:154) - Done
 executing task. name=LeafAgentConnectivityCheckPeriodicTask; status=OK; lastExecuted=1430733091611
2015-05-04 09:51:31,613 [pool-15-thread-16] INFO  updateStatus(SystemTaskStatusProvider.java:181) -
 Task: task.LeafAgentConnectivityCheckPeriodicTask changed state to OK
```

Step 2 To exit from the log file display, type **Ctrl + C**, then press **Enter**.

Applying a Patch to Cisco IMC Supervisor

Choose this option to apply a patch to the appliance.

Note The patch file (zip file) is provided by Cisco IMC Supervisor. Before applying a patch:

- Review the patch release notes and the Readme file.
- Take a snapshot of your VM.
- Make a backup of your database prior to taking the patch. The **Apply Patch** option enables you to make a backup as part of the **Apply Patch** procedure; but the best practice is to create a backup immediately before using the **Apply Patch** option.
- Stop the appliance services.

Before you begin

- Download the patch file.
- Place the file in a web server or an FTP server.
- Choose **Apply Patch** from the Cisco IMC Supervisor Shell menu.
- Provide patch URL (http://WebServer/TestPkg.zip)

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Apply Patch** and press **Enter**.

Information similar to the following is displayed:

```
Applying Patch...
Do you want to take database backup before applying patch (y/n)?
```

Step 2 If you entered **y**, enter the requested FTP server IP address and login data, then press **Enter**.

```
y
Backup will upload file to an FTP server.
Provide the necessary access credentials.
   FTP Server IP Address:
   FTP Server Login:
```

Step 3 If you entered **n**, enter the mode of transfer, and press **Enter** and provide the required information, as follows:

- SFTP—Enter the SFTP server IP address, server login name and password, and the path to the location where you have stored the upgrade file.
- SCP—Enter the SCP server IP address, server login name and password, and the path to the location where you have stored the upgrade file.
- FTP—Enter the FTP server IP address, server login name and password, and the path to the location where you have stored the upgrade file. For example,

  ftp://username:password@hostname\IP_address/software_location_and_name.
- HTTP—Enter the URL for the location where you stored the upgrade file.
- FILE—Enter the path to the local directory where you have stored the upgrade file.

```
n
User selected option not to take backup, proceeding with applying patch
Specify the Transfer mode [SFTP/SCP/FTP/HTTP/FILE]: SFTP
Server IP Address: XXX.XX.XXX.XXX
Server Username: XXXXX
Server Password:
SFTP Path to Patch Zip file:TestPkg.zip
Applying the Patch TestPkg.zip [y/n]? y
```

Note Refer to the Readme file for information about the patches.

Step 4 If you are prompted to confirm that you want to apply the patch, enter **y**, then press **Enter**.

Step 5 Follow the onscreen prompts to complete the process.

What to do next

After the patch is applied, choose **Stop Services** and **Start Services**.

Note Refer to the *Cisco IMC Supervisor Installation and Upgrade on VMware vSphere Guide* for additional information on upgrading to a patch.

Shutting Down the Appliance

Choose **Shutdown Appliance** to shut down the Cisco IMC Supervisor appliance.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Shutdown Appliance** and press the **Enter** key.

The following information is displayed:

```
Do you want to Shutdown appliance [y/n] ?:
```

Step 2 Enter **y** to shutdown the appliance.

Information similar to the following is displayed:

```
Broadcast message from root (pts/0) (Thu Sep 15 13:34:33 2013)

The system is shutting down NOW!
```

Step 3 Press **Enter** to return to the main menu.

Rebooting the Appliance

Choose **Reboot Appliance** to reboot the Cisco IMC Supervisor appliance.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Reboot Appliance** and press **Enter**.

The following information is displayed:

```
Do you want to Reboot appliance [y/n] ?:
```

Step 2 Enter **y** to reboot the appliance.

Information similar to the following is displayed:

```
Broadcast message from root (pts/0) (Mon May  4 10:34:14 2015):

The system is going down for reboot NOW!
Rebooting sucessful
Press return to continue ...
```

Step 3 Press **Enter** to return to the main menu.

Cleaning Patch Files

Choose **Clean-up Patch Files** to delete patch files from the appliance.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Clean-up Patch Files** and press **Enter**.

Information similar to the following is displayed:

```
Do you want to delete old patch files [y/n]?
```

Step 2 If you enter **y**, select a directory that you want to delete and then press **Enter**.

```
1) infra-04-20-2015-08-48-29
Select a directory to be deleted OR to exit press (x):
```

Step 3 Enter **n** and press **Enter** to go back to the main menu.

Collecting Diagnostics

The **Collect Diagnostics** option generates a summary report (SummaryReport.txt) and a detail report (DiagOutput.txt) and stores these files under `/opt/diagnostics`.

From the **Cisco IMC Supervisor Shell Menu**, choose **Collect Diagnostics**.

Information similar to the following appears, advising you that the diagnostic files have been created:

```
***************
Diagnostic Tool
***************

 Please find the below files under /opt/diagnostics :
 Summary Report: SummaryReport.txt
 Diagnostics report: DiagOutput.txt

/opt/diagnostics/rules

Press return to continue...
```

Enabling or Disabling Debug Logging

You can enable or disable the debug logging information by choosing **Enable/Disable Debug Logging**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Enable/Disable Debug Logging**.

Step 2 Press **Enter**.

Information similar to the following is displayed:

```
 Current Log Level = INFO

        Do you want to enable/disable debug logging [e/d]? :
```

Step 3 Press **e** to enable or press **d** to disable debug logging.

Step 4 Press **Enter**

Information similar to the following is displayed if you enable:

```
  Enabling debug logging...
        Enabled debug logging
        Current Log Level = DEBUG
Press return to continue...
```

Information similar to the following is displayed if you disable:

```
  Disabled debug logging
        Current Log Level = INFO
Press return to continue...
```

Step 5 Press **Enter** to complete the process.

Quitting the Shell

Choose **Quit** to exit the Cisco IMC Supervisor shell.

From the **Cisco IMC Supervisor Shell Menu**, choose **Quit** and press **Enter**.

The client application closes.

Resetting MySQL User Password

You can reset your MySQL admin and root password by choosing the **Reset MySQL User Password** option.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Reset MySQL User Password**.
Step 2 Press Enter.
Step 3 Enter **y** to confirm if you want to continue with changing the MySQL password.

Note If you confirm, the services will restart.

Step 4 Press Enter.
Step 5 Enter **y** to confirm if you want to change the password for MySQL admin user.
Step 6 Press Enter.
Step 7 Enter **y** to confirm if you want the system to generate a random password or **n** to specify a new admin password.
Step 8 Press Enter.
Step 9 Specify the new admin password and confirm the password again.
Step 10 Press Enter.
Step 11 Enter **y** to confirm if you want to change the password for MySQL root user.
Step 12 Press Enter.
Step 13 Enter **y** to confirm if you want the system to generate a random password or **n** to specify a new root password.
Step 14 Specify the new root password and confirm the password again.
Step 15 Press **Enter** to complete the procedure.

Terminating Active GUI Sesisons

Choose **Terminate active GUI session(s) for user** to terminate the active user sessions.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Terminate active GUI session(s) for user** and press **Enter**.

Information similar to the following is displayed:

```
 On a subsequent login, all active session(s) for the user will be terminated.

This utility is for terminating the GUI sessions after the specified maximum concurrent sessions for
 a user is reached. Do you want to proceed [y/n]?:
```

Step 2 Enter **y** and press **Enter** to terminate the active GUI sessions.

Granting Client Access to MySQL Port

Choose this option to allow the external clients to access the MYSQL port.

Step 1 From the Shell menu, choose the **Grant/Deny client access to MySQL port 3306** option and press **Enter**.

The following information displays:

```
Grant provide external clients access to MySQL port 3306. Deny blocks external clients access to
MySQL port 3306 for the granted ip address.

Source IP's configured
----------------------
10.197.110.92
----------------------

Do you want to grant/deny external clients access to MySQL port 3306 [g/d]? :
```

Step 2 Enter **g** and press **Enter**.

The following information is displayed:

```
Enter the ip address you want to grant access to MySQL port 3306 :
```

Step 3 Enter the IP address and press **Enter**.

The following information is displayed:

```
Enabling firewall rules for ip 10.197.110.92
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Press return to continue...
```

Note You can enter 0.0.0.0 (IP address) if you want to grant access to all the clients.

Step 4 Press **Enter** to return to complete the process.

Denying Client Access to MySQL Port

Step 1 From the Shell menu, choose the **Grant/Deny client access to MySQL port 3306** option and press **Enter**.

The following information displays:

```
Grant provide external clients access to MySQL port 3306. Deny blocks external clients access to
MySQL port 3306 for the granted ip address.

Source IP's configured
----------------------
10.197.110.92
----------------------

Do you want to grant/deny external clients access to MySQL port 3306 [g/d]? :
```

Step 2 Enter **d** and press **Enter**.

The following information is displayed:

```
Enter the ip address you want to deny access to MySQL port 3306 :
```

Step 3 Enter the IP address and press **Enter**.

The following information is displayed:

```
Successfully denied ipaddress 10.197.110.92 provided...
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Press return to continue...
```

Step 4 Press **Enter** to return to complete the process.

Enabling or Disabling HTTP

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Enable/Disable HTTP**.

Step 2 Press **Enter**.

Information similar to the following is displayed:

```
 Do you want to enable/disable HTTP [e/d]? :
```

Step 3 Press **e** to enable or press **d** to disable HTTP.

Step 4 Press **Enter**.

The Shell menu will indicate if HTTP is enabled or disabled.

Step 5 Press **Enter** to complete the process.

Working with Databases

This section describes how to enable, start and stop, as well as backup and restore a database.

Stopping the Database

You can halt the mysql daemon (mysqld) by choosing **Stop Database**. This option stops all of the following Cisco services:

- Broker
- Controller
- Eventmgr
- Client
- Idaccessmgr
- Inframgr
- Tomcat
- Websock

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Stop Database**.

Information similar to the following is displayed:

```
Do you want to stop the database [y/n]?  y
Stopping database....
Database stopped....
     Stopping broker [PID=21921]/[Child=21923]
     Stopping controller [PID=21959]/[Child=21961]
     Stopping eventmgr [PID=21993]/[Child=21995]
     Stopping client [PID=22052]/[Child=22054
22101
22160]
     Stopping idaccessmgr [PID=22099]/[Child=]
     Stopping inframgr [PID=22158]/[Child=]
     Tomcat is running with [PID=22213]. Stoping it and its child process
  Flashpolicyd is running with [PID=22237]. Stopping it
Stopping websock[PID=22242]
Press return to continue ...
```

Step 2 Press **Enter** to return to the main menu.

Starting the Database

You can start the mysql daemon (mysqld) by choosing **Start Database**.

Note This option starts the appliance database only.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Start Database**.

Step 2 Press **Enter**.

Information similar to the following is displayed:

```
Starting database.....
directory (/var/lib/mysql/data/confmgr_production) exists
directory (/var/lib/mysql/data/db_private_admin) exists
the file (/var/lib/mysql/data/ib_logfile1) exists
the file (/var/lib/mysql/data/ib_logfile0) exists
the file (/var/lib/mysql/data/ibdata1) exists
Database started
Press return to continue ...130917 10:10:54 mysqld_safe Logging to '/var/log/mysqld.log'.
130917 10:10:54 mysqld_safe Starting mysqld daemon with databaes from /var/lib/mysql/data
```

Note The Cisco services are not started automatically when you start the appliance database. Choose **Start Services** to start the Cisco services.

Backing Up the Database

Backing up the database triggers a full backup of the Cisco IMC Supervisor appliance. The process may take time to complete based on the number of files and the size of these files on the appliance. You can backup the appliance database to an FTP server, SFTP server or SCP server. Before you begin the backup process, you must first stop the Cisco services. To stop the services, choose **Stop Services**. Refer to Stopping Cisco Services, on page 8 about using the option.

You need the following information in order to complete this task:

- Server IP address (where you want to backup the database)
- Server login credentials

Note After you provide the login credentials, the entire Cisco IMC Supervisor appliance database is backed up at the specified location in the server. You can then start the Cisco services by choosing **Start Services**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Backup Database**.

Step 2 Press **Enter**.

Step 3 Enter **y** to confirm that you want to continue with the database back up and that the services on the appliances can be stopped.

Step 4 Enter the transfer mode for the backup.

You can enter one of the following options:

- **ftp**
- **sftp**
- **scp**

Step 5 Enter the server IP address and press **Enter**.

Step 6 Enter the server login name and press **Enter**.

Step 7 Enter the server password and press **Enter**.

Step 8 Enter the directory in which the file created during the backup process must be stored in.

Messages will appear to confirm the progress of your backup.

Restoring the Database

Before restoring the database, stop the Cisco services. To stop the services, choose **Stop Services**. Provide the following information in order to execute the task:

- FTP server's IP address (where you want the database restored from)
- FTP server's login credentials
- Restore filename
- Confirm to restore

Note After you provide the FTP credentials, the entire Cisco IMC Supervisor appliance database is restored from the specified FTP location. You can then start the Cisco services by choosing **Start Services**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Restore Database**.

Step 2 Press **Enter**.

Information similar to the following is displayed:

```
Restore database......
Restore will recover file from an FTP server. Provide the necessary access credentials

   FTP Server IP Address:
   FTP Server Login: root
   FTP Server Password:
```

Step 3 Enter your FTP server IP address and press **Enter**.

Step 4 Enter your FTP server login and press **Enter**.

Step 5 Enter your FTP server password and press Enter.

Step 6 Follow the onscreen prompts to complete the process.

Step 7 Choose **Start Services** to restart the Cisco services.

Importing Certificates

This section describes how to import certification authority (CA) certificates such as the Java KeyStore (JKS). A JKS certificate is a repository of security certificates used in SSL encryption. This certificate is required for a secure connection through HTTPS. Importing a JKS certificate allows you to connect securely to Cisco IMC Supervisor through HTTPS.

Generating Self-Signed Certificates and Certificate Signing Requests

When you generate a self-signed certificate, a new self-signed certificate in PEM format and a Certificate Signing Request (CSR) file are created in the `opt/certs/` directory. When generating a self-signed certificate, clicking enter will select the default option. For example, if you do not specify a domain name, the shell admin by default chooses the domain name of the appliance that is configured.

You can generate a self-signed certificate and a CSR using the **`Generate Self-Signed Certificate and Certificate Signing Request`** option.

Step 1 From the Cisco IMC Supervisor Shell menu, choose the **`Generate Self-Signed Certificate and Certificate Signing Request`** and press Enter.

The following information is displayed:

```
Domain Name [localdom]:
```

Step 2 Enter the domain name and press **`Enter`**.

By default the shell menu selects the domain name of the local appliance that is configured.

The following information is displayed:

```
How many days is self-signed certificate valid for? [365]:
```

Step 3 Enter the number of days that you want the self-signed certificate to be valid for and press **`Enter`**.

The following information is displayed:

```
Generating a 2048 bit RSA private key
writing new private key to 'opt/certs/localdom.key'
------
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
------
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
```

Step 4 Enter the country name, state or province name, locality name, organization name, organizational unit name, common name, and email address, and press **`Enter`**.

The following information is displayed:

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name:
```

Step 5 (Optional) Enter a challenge password and an optional company name, and press **Enter**.

The following information is displayed:

```
Writing new CSR (Certificate Signing Request) to /opt/certs/localdom.csr.
Use the CSR to obtain a certificate in PEM format from a CA (Certificate Authority).

Writing new self-signed certificate in PEM format to opt/certs/localdom.pem.

Press return to continue ...
```

Importing a Certification Authority or Self Signed Certificates

You can either import the generated self-signed certificate or import a certificate generated by another system or third party by copying .pem and .key (private key) files to the `/opt/certs/` directory. The shell admin will automatically discover the .pem and .key files for the given domain in the `/opt/certs/` directory. The .pem file provided is exported into PKCS12 format, and then converted to JKS format. The JKS file can be imported into Tomcat.

You can import a CA signed certificate or self-signed certificate using the **Import CA/Self-Signed Certificate** option.

Step 1 From the Cisco IMC Supervisor Shell menu, choose the **Importing CA/Self-Signed Certificate** option and press Enter.

The following information is displayed:

```
Domain Name [localdom]:
```

Step 2 Enter the domain name and press **Enter**.

By default the shell menu selects the domain name of the local appliance that is configured.

The following information is displayed:

```
Enter CA/self-signed certificate [/opt/certs/localdom.pem]:
```

Step 3 Enter the path to the CA signed certificate or self-signed certificate, and press **Enter**.

The following information is displayed:

```
Enter private key [/opt/certs/localdom.key]:
```

Step 4 Enter the path to the private key and press **Enter**.

The following information is displayed:

```
Enter keystore password:
```

Step 5 Enter the Java KeyStore (JKS) password and press **Enter**.

Information similar to the following is displayed

```
Exporting /opt/certs/localdom.pem to PKCS12 format....

Converting PKCS12 to JKS format...

Importing /opt/certs/keystore.jks into tomcat for secured access to UCSD UI using HTTPS.

Certificate /opt/certs/keystore.jks imported to tomcat succesfully.

Do you want to import the certificate file:///opt/certs/localdom.pem into WebProxy for secured access
 to VM console through VNC [y/n]?:
```

Step 6 Enter **y** and press **Enter** to import the certificate file into WebProxy for secured access to the VM console through VNC.

The following information is displayed:

```
Certificate file:///opt/certs/localdom.pem imported to WebProxy succesfully.
Press return to continue ...
```

Accessing Root Privileges

This section describes how to access root. Tasks that require root privileges include moving directories or files into other directories, providing or revoking user privileges, general system repairs, and occasionally installing applications.

Note Compiling software as root is not recommended for security reasons.

Configuring Root Access

You can enable root privileges by choosing **Manage Root Access**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Manage Root Access** and press **Enter**.

The following information is displayed:

```
 Enable/Disable/Configure (root privalege) [e/d/c]:
```

Step 2 Enter **c** and press **Enter**.

The following information is displayed:

```
Do you want to Configure/Set Root Privilege/Password [y/n]? :
```

Step 3 Enter **y** and press **Enter**.

The following information is displayed:

```
Changing root password...
         Changing password for user root.
         New UNIX password:
```

Step 4 Enter a new UNIX password and press **Enter**.

The following information is displayed:

```
 Retype new UNIX password:
```

Step 5 Enter your new UNIX password and press **Enter**.

Information similar to the following is displayed:

```
passswd: all authentication tokens updated successfully.
         Root passwd changed successfully
         Press return to continue...
```

Step 6 Press **Enter** to complete the process.

Logging in as Root

You can login in as root by choosing **Login As Root**.

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **Login As Root** and press **Enter**.

The following information is displayed:

```
 Do you want to  Login As Root [y/n]? :
```

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Logging in as root
         password:
```

Step 3 Enter your root password and press **Enter**.

The following information is displayed:

```
 Logging as root
Password:
[root@localhost shelladmin]#
```

Step 4 Enter your password and press **Enter**.

Step 5 Enter **exit** to return to the shelladmin.

The following information is displayed:

```
[root@localhost shelladmin]# cd /opt
[root@localhost opt]# exit
exit
Sucessful login
Press return to continue ...
```