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
- Client
- 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.
- Tomcat - Hosts Cisco UCS Director GUI web app.
- 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.
- Database (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                  Status        PID
 ----------           ----------      -----
 broker                  RUNNING      18718
 controller              RUNNING      18758
 eventmgr                RUNNING      18792
 client                  RUNNING      18891
 idaccessmgr             RUNNING      18938
 inframgr                RUNNING      18997
 TOMCAT                  RUNNING      19054
 websock                 RUNNING       19083

  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.

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 patch IP address and press Enter.

```
n
Applying Patch:
Patch URL: http://xxx.xxx.x.xxx/TestPkg.zip

Applying the Patch http://xxx.xxx.x.xxx/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.

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 number and size of files on the appliance. You can backup the appliance database to an FTP 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 3 about using the option.

You need the following information in order to execute the task:

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

Note After you provide the FTP credentials, the entire Cisco IMC Supervisor appliance database is backed up at 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 Backup Database.

Step 2 Press Enter.
Information similar to the following is displayed:

```
Backing database......
Backup will Upload file to an FTP server. Provide the necessary access credentials

   FTP Server IP Address: xxxx.xxxx.xxxx.xxxx
   FTP Server Login:
```

Step 3 Enter your FTP Server IP address and press Enter.

Step 4 Enter your FTP Server login name and press Enter.

Step 5 Enter your FTP Server password and press Enter.

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 ...
```