



CHAPTER 2

Installing, Upgrading, and Uninstalling HCM Service Assurance

This chapter explains how to install HCM 1.2 or upgrade from HCM 1.1 to HCM 1.2, and uninstall HCM Service Assurance. It includes:

- [HCM Service Assurance Server Requirements, page 2-2](#)
- [HCM Service Assurance Client Requirements, page 2-3](#)
- [HCM Service Assurance Default Ports, page 2-4](#)
- [HCM Service Assurance Pre-Installation Steps, page 2-5](#)
- [Installing/Upgrading and Starting HCM Service Assurance in a Non-Cluster Setup, page 2-6](#)
- [Installing HCM Service Assurance in a Cluster Setup, page 2-11](#)
- [HCM Service Assurance Post-Installation Tasks, page 2-12](#)
- [HCM Service Assurance Log Files, page 2-14](#)
- [Starting and Stopping HCM Service Assurance Server, page 2-14](#)
- [Modifying Database User Password in HCM Service Assurance Configuration File, page 2-15](#)
- [Configuring a New Client and New User in ACS 5.1, page 2-16](#)
- [Configuring LDAP for Authentication, page 2-19](#)
- [Installing MySQL Database Server 5.1, page 2-24](#)
- [Uninstalling HCM Service Assurance, page 2-24](#)

HCM Service Assurance Server Requirements

Table 2-1 lists the server requirements for the HCM Service Assurance component.

Table 2-1 HCM Service Assurance Server Requirements

Requirement	Notes
Operating System	Red Hat Enterprise Linux 5.3 (64-bit). See Installing Linux 5.3—Guidelines, page 2-22 .
CPU	2.33 vCPU
DRAM	8 GB RAM
CPU Cache	2 x 6 MB L2 cache
Disk Space	200 GB hard drive
Network Interface Card (NIC)	One 1-Gigabit Ethernet, low-latency NIC with dedicated connectivity to all supported domain managers.
Structured Query Language (SQL) Server	MySQL 5.1. This is not installed as a part of the HCM application package. MySQL Server is installed by default on the Red Hat Enterprise Linux operating system. If MySQL is not installed, you must install it. See Installing MySQL Database Server 5.1, page 2-24 .
Java Development Kit (JDK)	JDK 1.5—available as part of the HCM application package.
Web Server	JBoss 4.2.3 GA. This is available as part of the HCM application package.
Domain Managers	<ul style="list-style-type: none"> • CUOM 8.6 • UCSM 1.4 • vCenter 4.1.0 • DCNM-LAN 5.2 • DCNM-SAN 5.2

HCM Service Assurance Client Requirements

The following are the client requirements to view HCM Service Assurance:

- Mozilla 3.6.3
- IE 8.0

**Note**

The language setting of your system must be set to English. If you changed the language to a language other than English, be sure to follow the procedure outlined below to be able to view HCM without distortions.

Follow the procedure given below to arrive at the appropriate setting.

First, you need to set the language preference specific to your browser. Next, you need to set the language preference at system level.

For Mozilla Firefox:

-
- Step 1** Open a Mozilla Firefox browse window and go to **Tools > Options**.
 - Step 2** Go to **Content** tab, and then click **Languages**.
The Languages dialog box opens and the languages are listed in order of preference.
 - Step 3** Choose **English [en]**, and click **Move Up**.
The language is set as your first choice in order of preference.
 - Step 4** Click **OK**.

For Internet Explorer:

-
- Step 1** Open an Internet Explorer window, and go to **Tools > Internet Options**.
 - Step 2** Under the **General** tab, click **Languages**.
The Language Preferences dialog box opens. The languages are listed in the order of your preference.
 - Step 3** Choose **English (United States) [en-us]** and click **OK**. If there are other options listed, choose **English (United States) [en-us]** and click **Move Up** to make it your first choice.
 - Step 4** Click **OK**.

Setting the OS Language to English

To set the language for your system, follow the steps mentioned below:

-
- Step 1** Go to **Windows Start > Control Panel > Regional and Language Options**.
The Regional and Language Options Setting dialog box opens.
 - Step 2** Under the **Regional Options** tab, in the **Standards and Formats** pane, choose **English (United States)** and click **OK**.
 - Step 3** Under the **Languages** tab, click **Details**.

Text Services and Input Languages dialog box opens.

Step 4 Click **Add**, and then add the language **English (United States)**.

Step 5 Click **OK**.

HCM Service Assurance Default Ports

This section lists the default ports of HCM Service Assurance and domain managers. You must make sure that HCM Service Assurance can communicate with the domain managers. It includes:

- [Default Ports of HCM Service Assurance, page 2-4](#)
- [Default Ports of Domain Managers, page 2-4](#)

Default Ports of HCM Service Assurance

[Table 2-2](#) lists the default ports of HCM Service Assurance. You can modify the default ports during installation.

Table 2-2 *Default Ports of HCM Service Assurance*

Protocol	Port Number
HTTP	8090
HTTPS	8443
HTTP	8080—For receiving notifications from CUOM.
ODBC	3306

Default Ports of Domain Managers

[Table 2-3](#) lists the default ports of Cisco Secure Access Control Server (ACS) and the domain managers.

Table 2-3 *Default Ports of Domain Managers*

Authentication and Domain Managers	Protocol	Port Number
Authentication		
ACS	TACACS	49
LDAP	LDAP	389
Domain Managers		
CUOM	NBI	44442
CUOM (Cross-launch)	HTTP	1741
	HTTPS	443
DCNM-LAN	HTTP	8080
DCNM-SAN	HTTP	80

Table 2-3 Default Ports of Domain Managers (continued)

Authentication and Domain Managers	Protocol	Port Number
UCSM	HTTP	80
vCenter	HTTPS	443

HCM Service Assurance Pre-Installation Steps



Caution

This procedure is *not* applicable if you are upgrading to HCM 1.2. The following procedure might result in loss of data, if you are upgrading to HCM 1.2.

Before you install HCM 1.2, do the following:

Step 1 Enter the following command to check whether MySQL server is running:

```
ps -ef | grep -i mysql
```

If MySQL server is not running, enter the following command:

```
/etc/init.d/mysql start
```

Step 2 Go to the /usr/bin directory.

Step 3 Enter the following command to invoke mysql_secure_installation:

```
./mysql_secure_installation
```

A set of options is displayed.

Step 4 Enter **y** for all options.

For example:

```
Set root password (y/n):y
```

```
Remove anonymous users (y/n):y
```

```
Disallow root login remotely (y/n):y
```

```
Remove test database and access to it (y/n):y
```

```
Reload privileges table now(y/n):y
```

Step 5 Enter the following command to log into MySQL with root credentials:

```
mysql -u root -p
```

Step 6 In the MySQL console window, enter the following command to grant remote access permission for root:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'root_password'  
WITH GRANT OPTION;
```

Installing/Upgrading and Starting HCM Service Assurance in a Non-Cluster Setup

This section explains how to install and upgrade to HCM Service Assurance 1.2. During installation, you are prompted to select either ACS or LDAP as an authentication server. The procedure varies, depending on the server that you choose.

Choosing ACS

If you choose ACS, you need to configure ACS. See [Configuring a New Client and New User in ACS 5.1, page 2-16](#).

If MySQL is not installed, you must install MySQL. See [Installing MySQL Database Server 5.1, page 2-24](#).

Choosing LDAP

If you choose LDAP, see [Configuring LDAP for Authentication, page 2-19](#).

For details on installing and upgrading to HCM Service Assurance see:

- [Installing and Starting HCM Service Assurance, page 2-6](#)
- [Upgrading to HCM 1.2, page 2-10](#)

Installing and Starting HCM Service Assurance

To install and start HCM Service Assurance in a non-cluster setup:

-
- Step 1** Copy hcm12.bin to the installation server and then rename it as hcm.bin.
- Step 2** Enter the following command:
- ```
./hcm.bin
```
- The Hosted Collaboration Mediation InstallAnywhere Wizard appears.
- Step 3** In the Introduction screen, click **Next**.
- Step 4** In the License Agreement screen, select the **I accept the terms of the license agreement** radio button and click **Next**.
- If a previous version of HCM Service Assurance has been installed on the server, the Detect Previous Version screen appears. You can view the following details on this screen:
- Version that has been installed.
  - Install directory path.
- You must uninstall the installed version before continuing with the new installation. To do this, see [Uninstalling HCM Service Assurance, page 2-24](#):
- Step 5** In the Select Cisco Hosted Collaboration Mediation Component screen, select the **Assurance** radio button and click **Next**.
- The Choose Install Folder screen appears. The Default Destination Folder path is set to /opt/hcm/dashboard.

If you want to install HCM Service Assurance in a different directory:

- a. Click **Choose**.
- b. Select the install directory path.
- c. Click **Next**.

**Step 6** In the Database Configuration screen (See [Figure 2-1](#)), enter the:

- a. IP address in the Server Address field.
- b. Port number in the Port Number field.  
The default database port is 3306, but you can change it, if needed.
- c. Username in the System User Name field.
- d. Password in the System User Password field.
- e. Click **Next**.

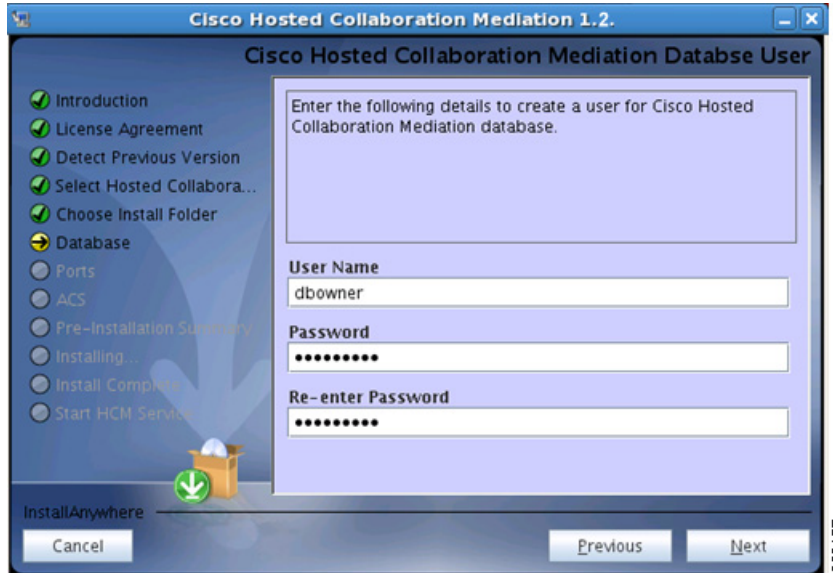
**Figure 2-1 Database Configuration Details**



**Step 7** In the Cisco Hosted Collaboration Mediation Database User screen (See [Figure 2-2](#)), enter the following details to create a user for Cisco Hosted Collaboration Mediation database:

- a. Username in the User Name field.
- b. Password in the Password field.
- c. Re-enter the password in the Re-enter Password field.
- d. Click **Next**.

Figure 2-2 Database User Details



- Step 8** In the Select Authentication Server screen, choose either **LDAP** or **ACS** as an authentication mechanism
- If you choose ACS, see [Installing HCM 1.2 with ACS, page 2-8](#)
  - If you choose LDAP, see [Installing HCM 1.2 with LDAP, page 2-9](#).
- Step 9** In the HTTP Port Configuration screen, enter the HTTP port number in the HTTP Port field and click **Next**.
- The default HTTP port is 8090, but you can change it if needed.
- Step 10** In the HTTPS Port Configuration screen, enter the HTTPS port number in the HTTPS Port field and click **Next**.
- The default HTTPS port is 8443, but you can change it if needed.
- Step 11** Click **Install**.
- The Installing HCM 1.2 screen appears and shows the progress of the installation.
- Step 12** In the Install Complete screen, click **Next**.
- Step 13** In the Start HCM Service Assurance screen, check the **Yes** check box if you want to start the HCM Service Assurance server and click **Done**.
- Wait a few minutes for HCM Service Assurance to start.
- After the installation completes, see [HCM Service Assurance Post-Installation Tasks, page 2-12](#) for further tasks.

### Installing HCM 1.2 with ACS

This procedure is a continuation of the section [Installing and Starting HCM Service Assurance, page 2-6](#). Read both the procedures together if you choose ACS as your authentication mechanism.



**Step 1** In the ACS Credentials screen (see [Figure 2-3](#)), enter the:

- a. IP address in the IP Address field.
- b. Port number in the Port field.
- c. Secret key in the Secret Key field.

If you want to change the ACS secret key after installation, follow the procedure in section [Modifying ACS Password in HCM Service Assurance Configuration File](#), page 2-18.

- d. Click **Next**.

The Pre-Installation Summary screen shows the items that will be installed.

**Figure 2-3 ACS Details**



**Step 2** Continue with [Step 9](#) in the procedure in the section [Installing and Starting HCM Service Assurance](#), page 2-6

### Installing HCM 1.2 with LDAP

This procedure is a continuation of the section [Installing and Starting HCM Service Assurance](#), page 2-6. Read both the procedures together if you choose LDAP as your authentication mechanism.

- Step 1** In the Choose LDAP Operational Mode screen, choose the location as either **Internal** or **External**.
- If you choose **External**, the data is fetched from an existing LDAP server in your network. Continue with [Step 9](#) in the procedure in the section [Installing and Starting HCM Service Assurance](#), page 2-6
  - If you choose **Internal**, HCM installs an embedded LDAP server on a local machine, continue with this procedure

- Step 2** Enter a password for LDAP authentication in the **Credentials** field, and then click **Next**.  
The following fields are populated, by default:
- LDAP Server Port
  - Base DN
  - Group
  - Principal
- Step 3** Continue with [Step 9](#) in the procedure in section [Installing and Starting HCM Service Assurance, page 2-6](#).
- 

## Upgrading to HCM 1.2

This section explains how to upgrade from HCM 1.1 to HCM 1.2. You cannot directly upgrade from HCM 1.0 to HCM 1.2. If you are running HCM 1.0, and you wish to upgrade to HCM 1.2, you must first upgrade to HCM 1.1, and then to HCM 1.2. See the *Installation Guide for Cisco Hosted Collaboration Mediation, 1.1*.

---

- Step 1** Copy hcm12.bin to the installation server and then rename it as hcm.bin.
- Step 2** Enter the following command:
- ```
./hcm.bin
```
- The Hosted Collaboration Mediation InstallAnywhere Wizard appears.
- Step 3** In the Introduction screen, click **Next**.
- Step 4** In the Confirm Upgrade screen, choose **Upgrade**, and then click **Next**.
- Step 5** In the Hosted Collaboration Mediation Database User screen, enter the:
- IP address in the Server Address field.
 - Port number in the Port Number field.
 - The default database port is 3306, but you can change it, if needed.
 - Username in the HCM User Name field. This username is the one you specified in the Cisco Hosted Collaboration Mediation Database User screen at the time of installation.
 - Password in the HCM User Password field. This password is the one you specified in the Cisco Hosted Collaboration Mediation Database User screen at the time of installation.
- Step 6** In the Select Authentication Server screen, choose an authentication mechanism between **LDAP** and **ACS**. Click **Next**.
- If you choose ACS, the system automatically fetches the credentials from your previous installation. Go to [Step 10](#).
 - If you choose LDAP, continue with [Step 7](#).

- Step 7** Choose the location as either **Internal** or **External**, and click **Next**.
- If you choose **Internal**, HCM installs an embedded LDAP server on a local machine. Continue with [Step 8](#).
 - If you choose **External**, the data is fetched from an existing LDAP server in your network; go to [Step 10](#).
- The LDAP Configuration screen appears.
- Step 8** Enter a password for LDAP authentication. The following fields are populated, by default:
- LDAP Server Port
 - Base DN
 - Group
 - Principal
- Step 9** Click **Next**.
- Step 10** The data is backed up. After the back up is complete, the Pre-Installation Summary screen appears.
- Step 11** Review the data that appears on the screen, and click **Install**.
- The Installing HCM 1.2 screen appears and shows the progress of the installation.
- Step 12** In the Install Complete screen, click **Next**.
- Step 13** In the Start HCM Service Assurance screen, check the **Yes** check box if you want to start the HCM Service Assurance server and click **Done**.
- Wait a few minutes for HCM Service Assurance to start.
- After the installation completes, see [HCM Service Assurance Post-Installation Tasks, page 2-12](#) for further tasks.

Installing HCM Service Assurance in a Cluster Setup

To install the HCM Service Assurance in a cluster setup, you need to install it on the primary and the secondary servers.

To install HCM Service Assurance on the primary server:

- Step 1** Go to the `Install_Directory/bin` directory.
- Step 2** Run `stop-hcm.sh` to stop the Apache service.
- The Apache and JBoss services stop.
- Step 3** Add the following lines in the `workers.properties` file located in the `/etc/httpd/conf` directory in the primary server:
- ```
Define Node2
modify the host as your host IP or DNS name.
worker.node2.port=8009
worker.node2.host=<secondary server ip>
worker.node2.type=ajp13
worker.node2.lbfactor=1
```

**Step 4** Add node2 for the secondary server in the cluster and node3 for the third server.  
Perform [Step 1](#) to [Step 4](#) to add more nodes.

**Step 5** Add node2 in the workers.properties file in the primary server.  
For example, see the following code example:

```
worker.loadbalancer.balance_workers=node1, node2
```

**Step 6** Go to the *Install\_Directory/bin* directory.

**Step 7** Run **start-hcm.sh** to start Apache service.  
The Apache and JBoss services start.

To install HCM Service Assurance on the secondary server:

**Step 1** Go to the *Install\_Directory/bin* directory.

**Step 2** Run **stop-hcm.sh** to stop the Apache and JBoss services.  
The Apache and JBoss services stop.

**Step 3** Go to the *Install\_Directory\thirdparty\jboss\server\default\deploy\jboss-web.deployer* directory.

**Step 4** In the server.xml file, change the jvmRoute value to node2.  
For example, see the following code example:

```
Engine name="jboss.web" defaultHost="localhost" jvmRoute="node2"
```

**Step 5** Go to the *Install\_Directory/bin* directory.

**Step 6** Run **start-hcm.sh** to start the Apache and JBoss services.  
The Apache and JBoss services start.

## HCM Service Assurance Post-Installation Tasks

After you install HCM Service Assurance, you must perform the following post-installation tasks:

- Check whether JBoss service is running—[Checking Whether JBoss Service is Running, page 2-12](#).
- Check whether Apache service is running—[Checking Whether Apache Service is Running, page 2-13](#).
- Configure for asynchronous communication between domain managers and HCM Service Assurance—[Configuring for Asynchronous Communication Between Domain Managers and HCM Service Assurance, page 2-13](#).
- Configure LDAP for authentication— [Configuring LDAP for Authentication, page 2-19](#).
- Start and update Linux firewall—[Starting and Updating Linux Firewall, page 2-21](#)

### Checking Whether JBoss Service is Running

After you install HCM Service Assurance, you must check whether JBoss service is running.

Enter the following command to check whether JBoss service is running:

```
ps -ef | grep -i jboss
```

If JBoss server is not running, stop and restart the Service Assurance server.

## Checking Whether Apache Service is Running

After you install HCM Service Assurance, you must check whether Apache service is running.

Enter the following command to check whether Apache service is running:

```
ps -ef | grep -i httpd
```

## Configuring for Asynchronous Communication Between Domain Managers and HCM Service Assurance

Sometimes service requests to the domain managers may result in long-running transactions. Domain managers support asynchronous behavior. This helps clients such as HCM Service Assurance to subscribe for asynchronous notifications and get notified by the domain manager, after the operation has completed. In such a scenario, HCM Service Assurance need not wait for a synchronous response.



### Note

You must configure the asynchronous details to run the Diagnostics Test in HCM Service Assurance.

You must perform the following configuration to ensure asynchronous communication among the domain managers and HCM Service Assurance. Before proceeding with the configuration, you must make sure that the IP address, hostname, and the port used by HCM Service Assurance are accessible from the domain managers.

To configure for asynchronous communication between domain managers and HCM Service Assurance:

- 
- Step 1** Go to the *HCM\_Dashboard\_Install\_Directory*.  
For example, /opt/hcm/dashboard
  - Step 2** Enter the following command and change the directory to bin:  
`cd bin`
  - Step 3** Run `stop-hcm.sh` and stop HCM Service Assurance server.
  - Step 4** Go to the *HCM\_Dashboard\_Install\_Directory/thirdparty/jboss/server/default/conf/portal\_props* directory.
  - Step 5** Open `monitor.properties` file.
  - Step 6** Modify the IP address on which HCM Service Assurance is installed.

The following is a code example of the property name tag before modifying:

```
WSN_CONSUMER_IPADDRESS=HCM_IP
```

The following is a code example of the property name tag after modifying. This example assumes that the IP address of the server on which HCM Service Assurance is installed is 192.168.0.1:

```
WSN_CONSUMER_IPADDRESS=192.168.0.1
```

- Step 7** Go to the *HCM\_Dashboard\_Install\_Directory*.  
For example, /opt/hcm/dashboard.

**Step 8** Enter the following command and change the directory to bin:

```
cd bin
```

**Step 9** Run **start-hcm.sh** and start HCM Service Assurance server.

---

## HCM Service Assurance Log Files

HCM Service Assurance maintains separate log files for UI, Schedulers, CUOM, synchronous and notification Web Services components. The log files are stored in the *install-directory/dashboard/thirdparty/jboss/server/default/log/msdtportal*.

The following log files are available:

- `msliferay.log`—UI
- `msscheduler.log`—Scheduler
- `mswsomclient.log`—Web services OM logs
- `mswsnotifyclient.log`—Web services OM notification
- `mswsvcclient.log`—Web services vCenter logs
- `mswsucsmclient.log`—Web services UCSM logs
- `msdcnmlanclient.log`—DCNM-LAN
- `msdcnmsanclient.log`—DCNM-SAN

The default size of a log file is 10 MB. A separate log file is created when a log file exceeds 10 MB. A maximum of two log files are maintained and older log files are recycled.

## Starting and Stopping HCM Service Assurance Server

After installing HCM Service Assurance and completing the post-installation tasks, you can start the HCM Service Assurance server.

To start the HCM Service Assurance server:

---

**Step 1** Enter the following command and go to the bin directory:

```
cd Install_Directory/bin
```

**Step 2** Enter the following command to run the `start-hcm.sh` file:

```
./start-hcm.sh
```

The HCM Service Assurance server starts.

---

To stop the HCM Service Assurance server:

**Step 1** Enter the following command and go to the bin directory:

```
cd Install_Directory/bin
```

**Step 2** Enter the following command to run the stop-hcm.sh file:

```
./stop-hcm.sh
```

The HCM Service Assurance server stops.

## Modifying Database User Password in HCM Service Assurance Configuration File

You can modify the database user password by editing the configuration file. To do this:

**Step 1** From the JBoss home directory, enter the following command and change the *password* instance with the new password:

```
../jdk/bin/java -cp
lib/jboss-common.jar:lib/jboss-jmx.jar:server/default/lib/jbosssx.jar:server/default/li
b/jboss-jca.jar org.jboss.resource.security.SecureIdentityLoginModule password
```

The encoded password appears.

For example, encoded password—5dfc52b51bd35553df8592078de921bc.

**Step 2** Copy the encoded password that is generated.

**Step 3** Go to the *HCM\_Root\_Directory*/thirdparty/jboss/server/default/conf directory.

**Step 4** Open the login-config.xml file.

**Step 5** Edit the value and paste the encoded password that you copied within the `<module-option name="password">` and `</module-option>` tags.



**Note** The `<module-option name="password">` and `</module-option>` tags appear twice in the login-config.xml file. You must edit the value at both instances.

The following is a code example of the login-config.xml file after the encoded password is modified. The `<module-option name="password">` and `</module-option>` tags have been highlighted.

```
<!-- Security domains for HCM encrypted database password jca framework -->
 <application-policy name="HCMEncryptDBPassword">
 <authentication>
 <login-module
code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
 <module-option name="username">db_username</module-option>
 <module-option name="password">5dfc52b51bd35553df8592078de921bc
</module-option>
 <module-option
name="managedConnectionFactoryName">jboss.jca:name=HCM_PORTAL,service=LocalTxCM</module
-option>
```

```

 </login-module>
 </authentication>
</application-policy>

<!-- Security domains for HCM encrypted database password jca framework -->
 <application-policy name="HCMEncryptLocalDBPassword">
 <authentication>
 <login-module
code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
 <module-option name="username">db_username</module-option>
 <module-option name="password">5dfc52b51bd35553df8592078de921bc
</module-option>
 </login-module>
 <module-option
name="managedConnectionFactoryName">jboss.jca:name=HCM_LOCAL,service=LocalTxCM</module-
option>
 </authentication>
 </application-policy>

```

---

## Configuring a New Client and New User in ACS 5.1

This section explains how to add a new client and a new user. It also explains how to modify the ACS password after installation, if needed. It includes:

- [Adding a New Client in ACS 5.1, page 2-16](#)
- [Adding a New User in ACS 5.1, page 2-17](#)
- [Modifying ACS Password in HCM Service Assurance Configuration File, page 2-18](#)

### Adding a New Client in ACS 5.1

To add a new client in ACS 5.1

- 
- Step 1** Log into ACS 5.1 as an admin user.
- Step 2** From the navigation pane, choose **Network Resources > Network Devices and AAA Clients**.  
The Network Devices page appears.
- Step 3** Click **Create**.  
The Create page appears.
- Step 4** In the General pane:
- Enter the DNS name of the client system in the Name field.  
For example, sol-tm-portal1.
  - (Optional) Enter the description of the HCM server in the Description field.
- Do not select the Location details or the Device type in the Network Device Groups pane.



- Step 5** In the IP Address pane:
- Select the **Single IP Address** radio button.
  - Enter the IP address of the client system in the IP field.

- Step 6** In the Authentication Options pane:
- Click the node to expand these Authentication Options:
    - TACACS+
    - RADIUS
  - Check the **TACACS+** check box:
  - Enter a value in the Shared Secret field.

You can enter any key value.

Do not select any of the following radio buttons under the **Single Connect Device** check box:

- Legacy TACACS+ Single Connect Support
- TACACS+ Draft Compliant Single Connect Support

Do not select the **RADIUS** check box.

---

For more information, see the *Network Devices and AAA Clients* section of the [User Guide for the Cisco Secure Access Control System 5.1](#).

## Adding a New User in ACS 5.1

To add a new user in Cisco ACS 5.1:

- 
- Step 1** Log into ACS 5.1 as an admin user.
- Step 2** From the navigation pane, choose **Users and Identity Stores > Internal Identity Stores > Users**.  
The Internal Users page appears.
- Step 3** Click **Create**.  
The Create page appears.
- Step 4** In the General pane, enter the following details:
- Name—Enter the name of the user. This username will be mapped in HCM.  
For example, admin001.
  - Description—(Optional) Enter the description for the user.  
For example, HCM Admin User.
  - Status—Select **Enabled** from the Status drop-down list. This is the default status.
  - Identity Groups—Select **All Groups** from the Identity Groups drop-down list. This is the default identity group.
- Step 5** In the Authentication Information pane, enter the following details:
- Password—Enter the password.  
For example, admin123.

Confirm Password—The password must match the password entered, earlier.

- b. Enable Password—(Optional) The internal user's TACACS+ enable password, from 4 to 32 characters.
- c. Confirm Password—(Optional) The internal user's TACACS+ enable password must match the enable password entered, earlier.

**Step 6** Click **Submit** to save the user details.

To create multiple users, go to [Step 3](#) and repeat the subsequent steps.

For more information, see the *Managing Internal Identity Stores* section of the *User Guide for the Cisco Secure Access Control System 5.1*.

## Modifying ACS Password in HCM Service Assurance Configuration File

You can modify the ACS password by editing the configuration file. To do this:

**Step 1** Enter the following command and change the *password* instance with the new password:

```
../jdk/bin/java -cp
server/default/lib/msdtportal.jar:server/default/lib/bcprov-jdk15-142.jar
com.cisco.util.Encryptor password
```

The encoded password appears.

For example, encoded password—47|112|52|126|82|31|15|46|40|32|87|45|72|65|18|15.

**Step 2** Copy the encoded password that is generated.

**Step 3** Go to the *HCM\_Root\_Directory*//thirdparty/jboss/server/default/deploy/ROOT.war/WEB-INF directory.

**Step 4** Open the *acs.properties* file.

**Step 5** Paste the encoded password that you copied in the *ACS\_SECRETKEY* parameter.

The following is a code example of the *acs.properties* file after the encoded password is modified. The *ACS\_SECRETKEY* parameter has been highlighted.

```
#ip address of the ACS server
ACS_IPADDRESS=172.20.120.145
```

```
#port number of the ACS Server
ACS_PORTNUMBER=49
```

```
#Secret Key Used for ACS Communication
```

```
ACS_SECRETKEY=47|-112|-52|126|-82|31|-15|46|-40|32|-87|45|72|-65|18|-15
```

## Configuring LDAP for Authentication

If you chose LDAP as the authentication mechanism at the time of installation, you have to configure the rules to import data to HCM or export data from HCM. You can choose to have LDAP installed internally or externally. If LDAP resides internally, the server is embedded and it resides locally. If you are using LDAP, you cannot use ACS for authentication.

In a typical scenario:

- If you installed LDAP internally, you will export data from HCM to LDAP.
- If you installed LDAP externally, you will use either of the options—Import or Export.

The following section explains how to configure HCM to use LDAP server.




### Note

HCM 1.2 has been certified only against OpenLDAP. We recommend you use only OpenLDAP for importing and exporting users.

## Exporting and Importing Users from LDAP

To export and import users from LDAP:

- 
- Step 1** Log in as `portaladmin`.
- Step 2** Click **Add Portlet** on the far right corner.  
The Add Applications pane appears on the left side.
- Step 3** Type **Enterprise Admin** in the search field.
- Step 4** Click **Add**.  
The portlet gets added.
- Step 5** From the portlet, click  and expand the pane.
- Step 6** Click **Settings**.
- Step 7** From the right pane, under General, click **Authentication**.
- Step 8** From the options that appear on the main pane, click the **LDAP** tab.
- Step 9** Verify whether the options **Enabled** and **Required** are checked. The options need to be checked for you to authenticate against an LDAP server.
- Step 10** In the Connection area, enter the following details:



### Note

The following details are shown if you specified the default values at the time of installation. The results would vary if you had changed the values.

- Base Provider URL—the URL of the LDAP server.
  - Base DN—`dc=hcm,dc=cisco,dc=com`
  - Principal—`cn=Manager,dc=hcm,dc=cisco,dc=com`
  - Credentials—the LDAP credentials that you entered during installation.
- Step 11** Click **Test LDAP Connection** to validate the connection with LDAP server.

In the LDAP Users Configuration area, the following details appear:

- Authentication Search Filter—(cn=@screen\_name@)
- Import Search Filter—(objectClass=inetOrgPerson)
- User Mapping
  - Screen Name—cn
  - Password—userPassword
  - Email Address—Mail
  - Full Name
  - First Name—[“givenName”]
  - Last Name—[“sn”]
  - Job Title—[“title”]
  - Group—ou




---

**Note** The Group name has to be *ou*.

---

**Step 12** Click **Test LDAP Users** to validate the data and know the status.

**Step 13** In the Groups area, enter the following details:

- Import Search Filter—(objectClass=groupOfNames)
- Group Mapping
  - Group Name—cn
  - Description—[*description*]
  - User—[*member*]

**Step 14** Click **Test LDAP Groups** to validate the data.

**Step 15** In the Import/Export area, check **Import** or **Export** as needed. Select only one option at a time.

If you choose **Import**, check the following options:

- Import Enabled
- Import on Startup Enabled
- Select an Import Interval

If you choose **Export**, enter the following: (Check the fonts)

- Users DN—ou=users, dc=hcm, dc=cisco, dc=com
- User Default Object Classes—top, person, inetOrgPerson, organizationalPerson
- Groups DN—ou=groups, dc=hcm, dc=cisco, dc=com

**Step 16** Click **Save**.




---

**Note** Be sure to create a new user with admin privileges before logging out. You might have to re-install HCM if you do not create one.

---

## Creating User Groups

This section explains how to create new user groups using the LDAP feature in HCM. This procedure is applicable only if you are importing users.

- 
- Step 1** Click the **User Groups** tab in the **Enterprise Admin** portlet, click **Add**.
  - Step 2** Specify a group name that matches with the group name created in LDAP. Enter a description and click **Save**.
  - Step 3** Verify whether the operation is successful.
  - Step 4** Run the command  

```
mysql -u root -p < Install_Directory/install/hcm/db/trigger-ldap-user.sql
```
- 

## Associating Roles to User Groups

This section explains how you can associate roles to user groups using the LDAP feature in HCM. This procedure is applicable only if you are importing users.

To import data from LDAP:

- 
- Step 1** In the **Enterprise Admin** portlet, open the **Roles** tab.
  - Step 2** Click the **Actions** button next to the respective administrator to associate a role, and then select **Assign Members**.  
A new page to assign roles for administrator opens.
  - Step 3** Click the **User Groups** tab and then click **Available**.
  - Step 4** Check the group name for which you want to associate roles, and click **Update Associations**.  
A confirmation message appears at the top of the screen.
  - Step 5** Click **Current** to verify whether the groups have been added.
- 

## Starting and Updating Linux Firewall

To start the firewall:

- 
- Step 1** Enter the following command and go to the bin directory:  

```
cd Install_Directory/bin
```
  - Step 2** Enter the following command to run the security.sh file:  

```
./security.sh
```
-

**To update the firewall:**

If you need to open ports for additional applications, run the following command:

```
iptables -I INPUT 16 -p tcp --dport <port number> -j ACCEPT
```

## Installing Linux 5.3—Guidelines

This section outlines some guidelines to follow while installing Linux 5.3; the options are specific to HCM 1.2. This section assumes that you are familiar with the Linux installation procedure.

**Note**

Unless specifically mentioned, you must configure the standard values for Linux machines in your network.

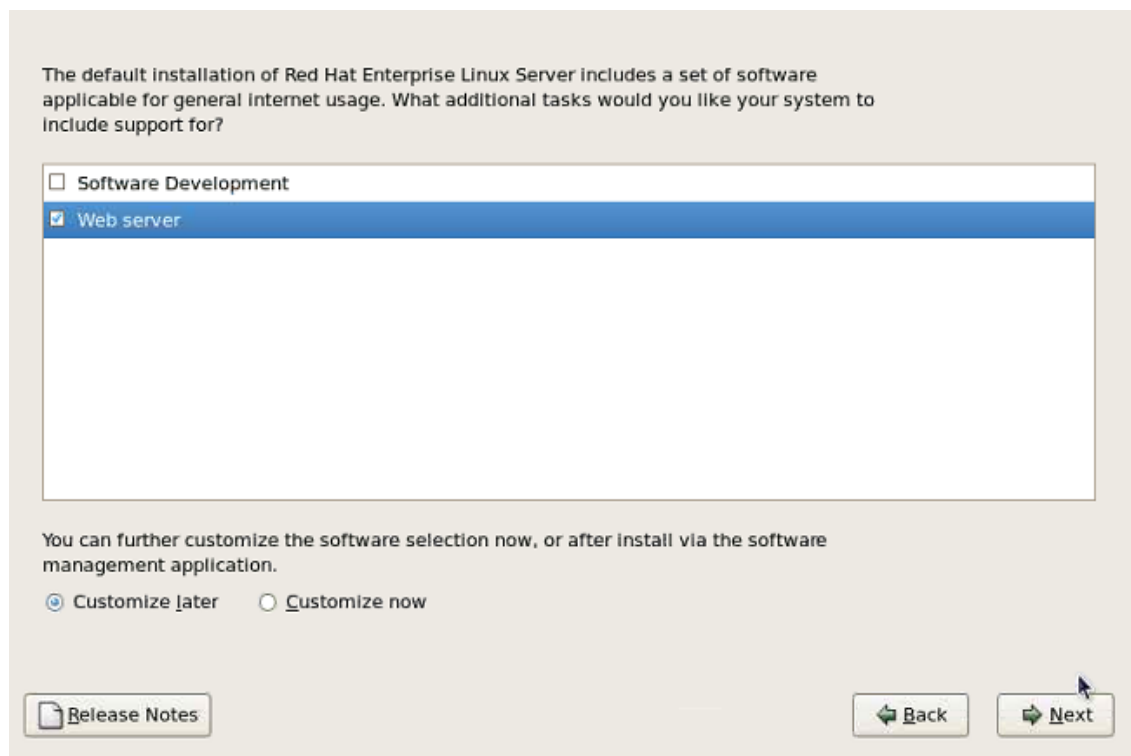
The following screens require specific configuration for HCM:

**Additional Tasks**

Figure 2-4 shows the Additional Tasks configuration screen.

1. Uncheck **Software Development**.
2. Check **Web Server**.

**Figure 2-4** Additional Tasks configuration screen



## Firewall

This section describes the initial Linux firewall configuration. The HCM installer will update these settings based on your network configuration. [Figure 2-5](#) shows the Firewall screen. Make your choice based on the parameters mentioned below.

1. Against **Trusted Services**, select all of the following as default options: SSH, HTTP, and HTTPS.
2. For additional ports, in the **Other Ports** area, click **Add**. The following are the default options:

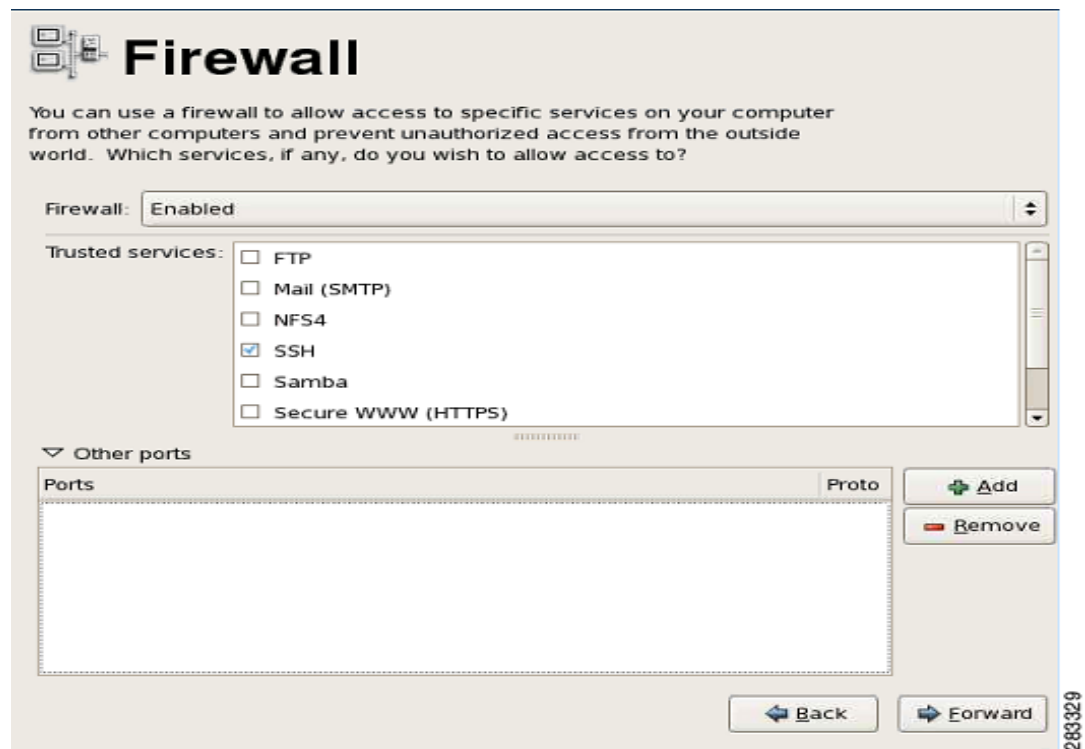
Protocol	Port Number
LDAP	389
HTTP	8090
HTTPS	8443



### Note

The actual port numbers may change depending on how your network is configured.

**Figure 2-5** Firewall configuration screen



We recommend that you read the following guides while hardening Linux:

- [Guide to the Secure Configuration of Red Hat Enterprise Linux 5](#)
- [Hardening Red Hat Enterprise Linux 5](#)

# Installing MySQL Database Server 5.1

This section describes how to install MySQL Database Server 5.1. MySQL Server is installed by default on the Red Hat Enterprise Linux operating system.

The overall installation process takes approximately 10 minutes. MySQL Database Server can be installed on the same server on which HCM Service Assurance is installed or it can be installed on a different server.

If there are more than 60 customers, we recommend that you install MySQL Database Server on a separate server.



## Note

After you do a fresh install of MySQL Database Server, you must follow the steps in the section and verify whether MySQL server is running.

If MySQL is not installed on the server, do the following to download and install MySQL:

- 
- Step 1** From the Linux server, go to <http://dev.mysql.com/downloads/mysql/>.  
The MySQL Community Server page appears.
- Step 2** From the Select Platform drop-down list, select **Red Hat & Oracle Enterprise Linux**.
- Step 3** Download the following packages:
- MySQL-client-community-5.1.53-1.rhel3.x86\_64.rpm
  - MySQL-server-community-5.1.53-1.rhel5.x86\_64.rpm
- Step 4** Enter the following command to install MySQL client:  
`rpm -ivh MySQL-client-community-5.1.53-1.rhel3.x86_64.rpm`  
The MySQL client is installed on the server.
- Step 5** Enter the following command to install MySQL server:  
`rpm -ivh MySQL-server-community-5.1.53-1.rhel5.x86_64.rpm`  
The MySQL server is installed on the server.
- 

# Uninstalling HCM Service Assurance

To uninstall HCM Service Assurance:

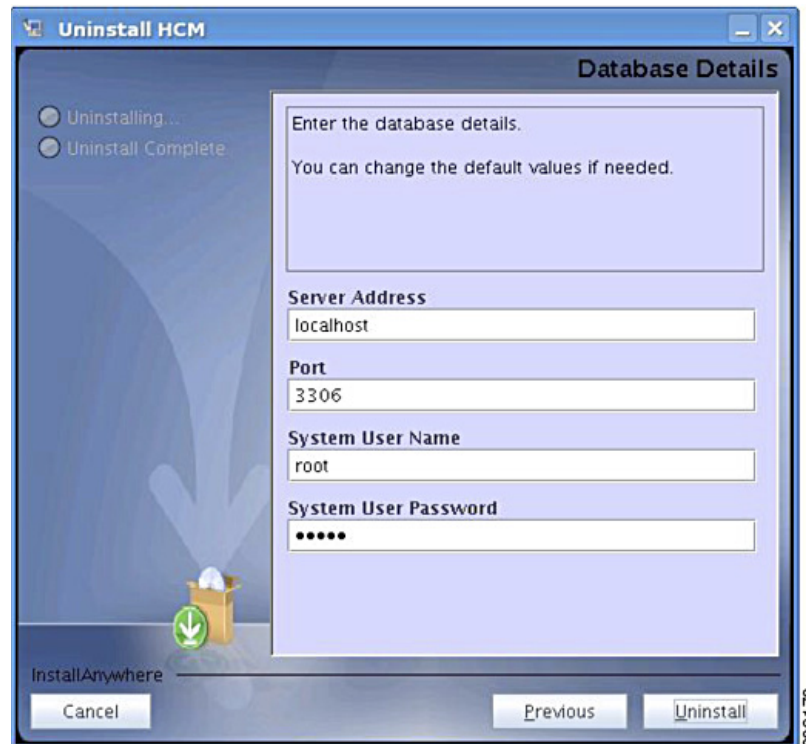
- 
- Step 1** Navigate to the *Root\_Directory*. This is the directory that you selected during installation.  
The default directory is /opt/hcm/dashboard.
- Step 2** Enter the following command to change the directory to uninstall\_hcm:  
`cd uninstall_hcm`
- Step 3** Enter the following command to open the Uninstall HCM InstallAnywhere wizard:  
`./uninstall`
- Step 4** In the Uninstall Assurance screen, click **Next**.



In the Database screen (See [Figure 2-6](#)), the values that you entered in the following fields during installation, populate automatically:

- Server Address
- Port
- System User Name
- System User Password

**Figure 2-6** Database Screen



If you have changed the values in any of the above-mentioned fields after installation, modify the details and enter the updated values.

**Step 5** After the details appear, click **Uninstall**.

**Step 6** In the Uninstall Confirmation screen, click the **Uninstall**.

The uninstall process starts.

**Step 7** In the Uninstall Complete screen, click **Done** to exit.

