CHAPTER 2

Installation of Cisco HCM-F

This chapter includes information about installing and configuring Cisco HCM-F. The HCM-F installation is new for Cisco HCS 8.6(2) and introduces new functionality that is used by service fulfillment and service assurance. The Cisco HCM-F installation integrates some services or components that previously ran on standalone virtual machines such as Platform Manager, and Service Inventory Manager into the Cisco HCM-F platform (virtual machine).

Review all installation instructions carefully before you begin the installation procedures.

This chapter contains sections on the following topics:

System Requirements for Installation

Table 2-1 lists the server requirements for the Cisco HCM-F platform.

Table 2-1 HCM-F Installation Server Requirements

Requirement	Notes
Product	Cisco Hosted Collaboration Solution (HCS)
Version	8.6

Table 2-1 HCM-F Installation Server Requirements (continued)

Requirement	Notes
Operating System	Red Hat Enterprise Linux RHEL5 (64-bit) **Note** The .iso file includes the linux OS. A separate installation of linux is not required for HCM-F is based on an appliance model.
CPU	2 vCPUs (3.6 GHz)
Memory	8 GB (RAM)
Hard Drive	80 GB (one)

Important Considerations

Before you proceed with the installation, consider the following requirements and recommendations:

- Make sure that you enable Network Time Protocol (NTP) on the Cisco HCM-F server. To verify the NTP status, log in to the Cisco HCM-F command line interface, and enter **utils ntp status**.
- Make sure that both Cisco HCM-F and CUOM are in the same time zone and are synchronized to NTP. This prevents a time out failure to the DMA-CUOM subscription.
- Be aware that when you install on an existing server, the hard drive gets formatted and all existing data on the drive gets overwritten.
- Configure Cisco HCM-F by using static IP addressing to ensure that the Cisco HCM-F obtains a fixed IP address.
- You must enable Domain Network Server (DNS) and configure NTP during installation.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete the installation.
- Carefully read the information that follows before you proceed with the installation.

Frequently Asked Questions About the Installation

The following section contains commonly asked questions and responses. Review this section carefully before you begin the installation. The section includes the following topics:

How Much Time Does the Installation Require?

The entire installation process, excluding pre- and post-installation tasks, takes 20 to 30 minutes.

What Usernames and Passwords Do I Need to Specify?

Note The system checks your passwords for strength. For guidelines on creating a strong passwords, see the "What Is a Strong Password?" section on page 2-3.

During the installation, you must specify the following usernames and passwords:

- Administrator account username and password
- Security password

Administrator Account Username and Password

You use the Administrator account username and password to log in to the following areas:

- Disaster Recovery System
- Command Line Interface

To specify the Administrator account username and password, follow these guidelines:

- Administrator account username—The Administrator account username must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Administrator account password—The Administrator account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator account password or add a new Administrator account by using the command line interface. For more information, see the "Command Line Interface for Cisco HCM-F" section on page 10-1.

Security Password

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

What Is a Strong Password?

The Installation wizard checks to ensure that you enter a strong password. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include hyphens and underscores.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert recognizable words.
- Do not use word or number patterns, such as aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Do not use recognizable words from other languages.
- Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.

What Is the Cisco Unified Communications Answer File Generator?

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations of Cisco HCM-F. Individual answer files get copied to the root directory of a floppy disk and are used in addition to the Cisco HCM-F DVD during the installation process.

The web application provides:

- Syntactical validation of data entries
- Online help and documentation
- Support for fresh installations (but does not support upgrades)

You can access the Cisco Unified Communications Answer File Generator at the following URL:

http://www.cisco.com/web/cuc_afg/index.html

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or later.

Cisco requires that you use virtual floppy image (.flp) that is compatible with Linux 2.4. Cisco recommends that you use virtual floppy that is preformatted to be compatible with Linux 2.4 for the configuration file. These virtual floppies use a W95 FAT32 format.

Which SFTP Servers Does Cisco Support?

SFTP servers are used for backups and restores, upgrades, service inventory, platform manager, and troubleshooting. Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, see the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, see the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

Can I Install Other Software on the Server?

You must perform all software installations and upgrades by using the CLI. The system can upload and process only software that Cisco approved. You cannot install or use unapproved third-party software applications.

Preinstallation Tasks

Table 2-2 contains a list of preinstallation tasks that you need to perform to ensure that you can successfully install Cisco HCM-F.

Table 2-2 Preinstallation Tasks

	Task
Step 1	Read this entire document to familiarize yourself with the installation procedure.
Step 2	Verify that all servers on which you plan to install Cisco HCM-F are properly registered in DNS.
Step 3	Record the configuration settings for each server that you plan to install.

Additional Information

Related Topics, page 2-15

Allowing Network Traffic

This section describes the minimum required ports that need to be configured to support Cisco HCM-F server. Table 2-3 provides a summary of the ports that need to be configured on a corporate firewall. The port configurations shown in this table are based on default settings. If you change the default settings, you need to update these configurations.

If you have other servers/ports required on your network, you need to allow for that traffic.

Table 2-3 Corporate Firewall Configuration

Interface	Direction	Source	Destination	Protocol	Port	Description
Inside	Inbound	Internal network or any management workstation	Cisco HCM-F server DMZ IP address	TCP	22	SFTP access to Cisco HCM-F server for uploading licenses/software, upgrade, and CLI access
Inside	Inbound	Internal network or any management workstation	Cisco HCM-F server DMZ IP address	HTTPS	443	HTTPS access to GUI and web APIs

Additional Information

Preinstallation Tasks, page 2-5

Creating Virtual Machines

Cisco provides a VM template for you to download and transfer to your virtual host. Use this template to create the VMs for Cisco HCM-F platform installation.

Before you deploy the template and create VMs, you should have the VM name, VLAN, hostname, and the IP address allocated for each new VM.

Follow these steps to create a VM and to prepare the Cisco HCM-F installation on it:

Procedure

Step 1 Download the VM template for your application. Go to http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Downloads_%28including_OVA/OVF_Templates%29

Step 2 Download the template to a location on your PC or at a designated URL.

Step 3 Deploy the template file using vSphere Client. Enter the following information for the new VM:

- hostname
- datastore—Select datastore
- Provisioning type—thick or thin
- target VLAN

Step 4 Make sure that you perform a thick provisioning of the virtual hard disk.

Step 5 Make sure that you complete the procedure to create the VM.

At this point a new VM is created with the correct amount of RAM, number of CPUs, size and number of disks for the intended application.

Setting Up Your Virtual Machine

This section provides information on how to set up a virtual machine.

Procedure

Step 1 Open the Open Virtualization Format (OVF) or OVA Template from **File > Deployed OVF Template...**

Step 2 Use the **Browse** option to find the location of the OVA file.

Note The OVA file can be located on the PC or at an URL address.

Step 3 Follow the wizard to complete the OVA installation process.

Gathering Information for an Installation

Use Table 2-4 to record the information about Cisco HCM-F. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration.

Note Because some of the fields are optional, they may not apply to your configuration.

Caution You cannot change some of the fields after installation without reinstalling the software, so be sure to enter the values that you want.

The last column in the table shows whether you can change a field after installation; if so, the appropriate CLI command is shown.

Table 2-4 Server Configuration Data

Parameter	Description	Can Entry Be Changed After Installation?
Administrator ID Your entry:	This field specifies the Administrator account user ID that you use for secure shell access to the CLI on Cisco HCM-F.	No, you cannot change the entry after installation. **Note** After installation, you can create additional Administrator accounts, but you cannot change the original Administrator account user ID.
Administrator Password Your entry:	This field specifies the password for the Administrator account, which you use for secure shell access to the CLI. You also use this password with the adminsftp user. You use the adminsftp user to access local backup files, upload server licenses, and so on. Ensure the password is at least six characters long; the password can contain alphanumeric characters, hyphens, and underscores.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password admin**
Country Your entry:	From the list, choose the appropriate country for your installation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
DHCP Your entry:	Cisco requires that you choose **No** to the DHCP option. After you choose **No**, enter a hostname, IP address, IP mask, and gateway.	No, you should not change the entry after installation.
DNS Enable Your entry:	A DNS server resolves a hostname into an IP address or an IP address into a hostname. Cisco HCM-F requires that you use a DNS server. Choose **Yes** to enable DNS.	No, you should not change the entry after installation.
DNS Primary Your entry:	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns** To view DNS and network information, use the following CLI command: CLI > **network eth0 detail**

Table 2-4 Server Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
DNS Secondary (optional) Your entry:	Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns**
Gateway Address Your entry:	Enter the IP address of the network gateway. If you do not have a gateway, you must still set this field to 255.255.255.255. Not having a gateway may limit you to being able to communicate only with devices on your subnet.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network gateway**
Hostname Your entry:	Enter a hostname that is unique to your server. The hostname can comprise up to 64 characters and can contain alphanumeric characters and hyphens. The first character cannot be a hyphen.	Yes, you can change the entry after installation. CLI > **set network hostname**
IP Address Your entry:	Enter the IP address of your server.	Yes, you can change the entry after installation. CLI > **set network ip eth0** **Note** If you have network fault tolerance enabled, you must disable it before you change the IP address by entering set network failover dis. Then, re-enable network fault tolerance after you change the IP address by entering set network failover ena.
IP Mask Your entry:	Enter the IP subnet mask of this machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network ip eth0**
Location Your entry:	Enter the location of the server. You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
MTU Size Your entry:	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. Enter the MTU size in bytes for your network. If you are unsure of the MTU setting for your network, use the default value. Default specifies 1500 bytes.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network mtu**

Table 2-4 Server Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
NIC Duplex Your entry:	Choose the duplex mode for the network interface card (NIC), either Full or Half. **Note** This parameter appears only when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**
NIC Speed Your entry:	Choose the speed for the NIC, 1 Gigabits per second or higher. **Note** This parameter appears only when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**
NTP Server Your entry:	Enter the hostname or IP address of one or more Network Time Protocol (NTP) servers with which you want to synchronize. You can enter up to five NTP servers. **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node can be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.	Yes, you can change the entry after installation by using the following CLI command: CLI > **utils ntp server**
Organization Your entry:	Enter the name of your organization. **Tip** You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
Security Password Your entry:	The password must contain at least six alphanumeric characters. The password can contain hyphens and underscores, but it must start with an alphanumeric character. **Note** Save this password.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password security**
State Your entry:	Enter the state that the server is located.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Table 2-4 Server Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Time Zone Your entry:	This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set timezone** To view the current time zone configuration, use the following CLI command: CLI > **show timezone config**
Unit Your entry:	Enter your unit.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password admin**

Additional Information

Preinstallation Tasks, page 2-5

Starting the Installation

This section describes how to install Cisco HCM-F. You install the operating system and Cisco HCM-F by running one installation program.

For information on how to navigate within the installation wizard, see Table 2-5.

Table 2-5 Installation Wizard Navigation

To Do This	Press This
Move to the next field	**Tab**
Move to the previous field	**Alt-Tab**
Choose an option	Space bar or **Enter**
Scroll up or down in a list	**Up Arrow** or **Down Arrow** key
Go to the previous window	Space bar or **Enter** to choose **Back** (when available)
Get help information for a window	Space bar or **Enter** to choose **Help** (when available)

Installing Cisco HCM-F

This section provides information on how to install the Cisco HCM-F.

Procedure

Step 1 Insert the Cisco HCS ISO disk into the DVD drive of the virtual machine.

Step 2 Reboot and start the virtual machine.

Note An installation screen appears to start the installation of the Cisco HCM-F.

Step 3 Follow the wizard installation as shown in Table 2-6.

Table 2-6 Wizard Installation procedures

Sequence	Wizard Task	Remarks
Step 1	Media Check Screen	Click **No** to skip the media check, or click **Yes** if media check is required.
Step 2	Product Deployment Selection	Click **OK.**
Step 3	Override Previous Installation	Select **Yes** or **No.**
Note	If there is a previous VM installation on the hard drive, the installation prompts you to override the previous installation. If no previous VM installation exists on the hard drive, the installation prompts you to install a new VM version on your hard drive.	
Step 4	Platform Installation Wizard	Select **Proceed.**
Step 5	Basic Installation	Select **Continue.**
Step 6	Timezone Configuration	Select the time zone from the drop-down list, and click **OK.**
Step 7	Auto Negotiation Configuration	Select **Continue.**
Step 8	MTU Configuration	Select **No** for no change, or **Yes** to enter new values.
Note	The virtual machine must be able to reach the gateway that is entered for the static configuration, or else the installation gives an error and does not proceed.	
Note	For the DNS option, if the virtual machine cannot reach the DNS and the hostname of the Cisco HCM-F server is not resolvable using that DNS server then the installation gives an error and does not proceed.	
Step 9	DHCP Configuration	The IP address is hardcoded. Select **Yes** for no change. Select **No** for DHCP.
Step 10	Static Network Configuration	Fill the fields **Host Name**, **IP Address**, **IP Mask**, **Gateway Address**. Click **OK.**
Step 11	DNS Client Configuration	If you select **Yes** to DNS client configuration, perform Step 12. If you select **No**, perform Step 13.
Step 12	DNS Client Configuration	Select **Primary DNS**, **Secondary DNS**, or **Domain**.
Step 13	Administrator Login Configuration	Fill the fields **Administrator ID**, **Password,** and **Confirm Password.** Click **OK.**

Table 2-6 Wizard Installation procedures

Sequence	Wizard Task	Remarks
Step 14	Certificate Information	Enter the appropriate information in each field. Click **OK**.
Step 15	Network Time Protocol Client Configuration	Enter the appropriate information in each field. Click **OK**.
Step 16	Security Configuration	Fill the fields **Security Password** and **Confirm Password.** Click **OK.**
Step 17	Platform Configuration Confirmation	Click **OK** to start the installation.

Step 4 When the installation process is complete, you get prompted to log in by using the Administrator account and password.

Step 5 Complete the post-installation tasks in the "Post-Installation Tasks" section on page 2-12.

Additional Information

Related Topics, page 2-15

Post-Installation Tasks

After installing Cisco HCM-F, you must complete the post-installation tasks listed in Table 2-7.

Table 2-7 Post-Installation Tasks

Configuration Steps		Related Procedures and Topics
Step 1	Configure the backup settings. Remember to back up your Cisco HCM-F data daily.	See the "Backup and Restore for Cisco HCM-F" section on page 4-1.
Step 2	In the CLI, activate the Cisco HCM-F services.	Working with Services, page 3-5

Resetting Administrator and Security Passwords

If you lose the Administrator password or security password, use the following procedure to reset these passwords.

To perform the password reset process, you must connect to the system through the system console; that is, you must connect to the server with a keyboard and monitor. You cannot reset a password when you connect to the system through a secure shell session.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: pwrecovery
- Password: pwreset

The Welcome to platform password reset window appears.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

Note For this test, you must use a data CD, not a music CD.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the Administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least six characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset. You get prompted to press any key to exit the password reset utility.

Additional Information

Related Topics, page 2-15

Upgrading Cisco HCM-F Software

This section applies to upgrades after you install Cisco HCM-F in Cisco HCS 8.6(2). Do not use this procedure to upgrade from Cisco HCS 8.6(1) or earlier releases.

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com. If you are performing an upgrade, you must obtain a DVD by using the Product Upgrade Tool (PUT) or by purchasing the upgrade from Cisco Sales.

To use the PUT, go to https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. You must enter your Cisco contract number (Smartnet, SASU or ESW) and request the DVD/DVD set. If you do not have a contract for Cisco HCM-F, you must purchase the upgrade from Cisco Sales.

Use the following procedure to upgrade the Cisco HCM-F platform software:

Procedure

Step 1 Obtain the upgrade media to upgrade the Cisco HCM-F platform.

If you downloaded the software executable from Cisco.com, do one of the following:

- Prepare to upgrade from a local directory by performing the following steps:
  - Copy the Cisco HCM-F upgrade file to a temporary directory on your local hard drive.
  - Create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

  Note If you copy the .iso file to the DVD but do not create an ISO image, you cannot upgrade your server from that DVD. Most commercial disk-burning applications can create ISO image disks.

  - Open an SFTP client and connect to the Cisco HCM-F server by using the adminsftp user and the Administrator password that you set up during installation.
  - Navigate to the upgrade directory by entering **cd upgrade** and copy the license file to that directory.
  - Type **put** <*upgrade filename*>, where <*upgrade filename*> specifies the upgrade file name that you downloaded from Cisco.com or obtained on a DVD.
- Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

  If you have a Cisco-provided upgrade disk, copy the contents of the disk to the remote server.

  If you downloaded the upgrade files, copy the files you downloaded to the remote server.

Step 2 After you have inserted the DVD into the server or uploaded the upgrade file to the remote server or local directory, log in to the Cisco HCM-F CLI and enter **utils system upgrade initiate**.

Step 3 Choose the source from which you want to upgrade:

- 1—Remote Filesystem via SFTP
- 2—Remote Filesystem via FTP
- 3—Local DVD/CD
- 4—Local Upload Directory

Step 4 Follow the system prompts for the upgrade option that you chose.

Step 5 The system prompts you when the upgrade process is complete. If you did not choose the option to automatically switch versions, enter **utils system switch-version** and enter **yes** to confirm that you want to reboot the server and switch to the new software version.

Step 6 After the installation completes, log in to the Cisco HCM-F CLI and verify the following:

- Perform an **admin: show version active** to verify that the current version is the one that was upgraded to.
- Perform an **admin: utils service list** to verify that the appropriate services are up and running.

Additional Information

Related Topics, page 2-15

Related Topics

- Important Considerations, page 2-2
- Frequently Asked Questions About the Installation, page 2-2
- Preinstallation Tasks, page 2-5
- Starting the Installation, page 2-10
- Post-Installation Tasks, page 2-12
- Resetting Administrator and Security Passwords, page 2-12