Prepare to Install

Installation System Requirements

The following table lists the server requirements for the Cisco HCM-F application node.

Table 1: Cisco HCM-F application node installation server requirements

Requirement	Notes
Product	Cisco HCS Mediation - Fulfillment
Version	Cisco HCS Release 12.5(1)
Operating System	Red Hat Enterprise Linux RHEL6 (64-bit) **Note** The .iso file includes the Linux OS. A separate installation of Linux is not required for Cisco HCM-F is based on an appliance model.
CPU	4 vCPUs (7.2 GHz), a VMware CPU reservation and the minimum acceptable
Memory	16 GB (RAM) with 16 GB reservation
Hard Drive	80 GB (one)

The following table lists the server requirements for the Cisco HCM-F Web Services (WS) node.

Table 2: Cisco HCM-F WS node installation server requirements

Requirement	Notes
Product	Cisco HCS Mediation - Fulfillment

Requirement	Notes
Version	12.5(1)
Operating System	Red Hat Enterprise Linux RHEL6 (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	4 vCPUs (7.2 GHz), a VMware CPU reservation and the minimum acceptable
Memory	8 GB (RAM) with 8 GB reservation
Hard Drive	80 GB (one)

The following table lists the server requirements for Cisco HCM-F backwards compatibility.

Table 3: Cisco HCM-F backwards compatibility server requirements

Requirement	Notes
Product	Cisco HCS Mediation - Fulfillment
Version	11.5(5)
Operating System	Red Hat Enterprise Linux RHEL6 (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	4 vCPUs (7.2 GHz), a VMware CPU reservation and the minimum acceptable
Memory	16 GB (RAM) with 16 GB reservation
Hard Drive	80 GB (one)

Network Requirements

Network traffic allowance

This section describes the minimum required ports that need to be configured to support Cisco HCM-F server. The following table 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 4: 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

Frequently Asked Questions About 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 installation require?

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

Which Usernames and Passwords Do I Need to Specify?

Note The system checks your passwords for strength. For guidelines on creating a strong password, see What is a strong password?, on page 4.

During the installation, 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
- RTMT
- Administrative 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 password must have a minimum of 6 and a maximum of 31 characters. It must also contain the following characters:
  - Alphanumeric characters including upper and lower case letters
  - Special characters that are limited to [!@#$%^&*()-_]

You can change the Administrator account password or add a new Administrator account by using the command line interface. For more information, see *Cisco Hosted Collaboration Mediation Fulfillment Command Line Interface Reference Guide*.

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. Strong passwords are used to protect your computer from hackers and malicious software.

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, abc123 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 Linux2.4. Cisco recommends that you use virtual floppy that is preformatted to be compatible with Linux2.4 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 HCM-F.

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 Titan FTP Server tab athttp://www.webdrive.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 Cisco HCM-F software installations and upgrades by using the CLI. The system can upload and process only software that Cisco has approved. You cannot install or use unapproved third-party software applications.

Preinstallation Tasks

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

Table 5: Preinstallation Tasks

	Task
Step 1	Read this entire document to familiarize yourself with the installation procedure.
Step 2	If you are using DNS, 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.

Create Virtual Machines

The number of Virtual Machines to be created depends on the Cisco HCM-F configuration to be deployed:

- Cisco HCM-F Application node only.
- Cisco HCM-F Application node and Web Services node (for non-redundant API Gateway).
- Cisco HCM-F Application node and two or more Web Services nodes (for redundant API Gateway). This deployment is known as a full deployment.
- Cisco HCM-F Remote Access Portal node.

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. Contact your Cisco account manager for information on obtaining the VM template.

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

Step 3 Open the Open Virtualization Format (OVF) or OVA Template from **File** > **Deploy OVF Template...**

Step 4 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 5 Follow the wizard to complete the OVA installation process.

Step 6 Deploy the template file using vSphere Client. Enter or select the following information for the new VM:

- VM name and inventory location
- Configuration:
  - HCM-F APP for Application Node
  - HCM-F WS for Web Services Node
  - HCM-F RAP for Remote Access Portal Node
- Host/Cluster
- Storage
- Disk format: select thick provisioning
- Network mapping: target VLAN

Step 7 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.

Installation Information Gathering

Use the following table 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 6: 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. 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 user 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:	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.

Parameter	Description	Can Entry Be Changed After Installation?
DNS Enable Your entry:	A DNS server resolves a hostname into an IP address or an IP address into a hostname. If you are using API Gateway Proxy service, we recommend using a DNS to support the operation of the API Gateway proxy. Without a DNS, there is a 10-second delay each time a session is established between the API Gateway Proxy and a southbound component. If using DNS, choose **Yes** to enable DNS. **Note** If using DNS, you must use it on all nodes.	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 primary IP_Address_of_primary_DNS_server** To view DNS and network information, use the following CLI command: CLI > **show network eth0 detail**
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 primary IP_Address_of_Secondary_DNS_server**
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**

Parameter	Description	Can Entry Be Changed After Installation?
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** The command prompts the user for the new 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 <ip_addess> <network_mask> <network_gateway>**
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**
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**

Parameter	Description	Can Entry Be Changed After Installation?
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).	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 in the entry.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security** <*orgname*>
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**

Parameter	Description	Can Entry Be Changed After Installation?
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** <*state*>
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 web-security** <*orgunit*>

Browser Compatibility for HCM-F

The following web browsers are supported for Cisco HCM-F within Cisco Hosted Collaboration Solution:

- Firefox with Windows 10 (64 bit)—Latest browser version only
- Chrome with Windows 10 (64 bit)—Latest browser version only
- Internet Explorer 11 with Windows 10 (64 bit)
- Internet Explorer 11 with Windows 8.1 (64 bit)
- Microsoft Edge browser with Windows 10 (32 bit/64 bit)