Cisco IME server installation and configuration

This chapter includes information about installing and configuring the Cisco Intercompany Media Engine server. Review all installation instructions carefully before you begin the installation procedures.

System requirements

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

- Make sure that the Cisco Unified Communications Manager server is running a compatible version of the Cisco Unified Communications Manager software. See the Cisco Unified Communications Manager Software Compatibility Matrix at the following URL:

  http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html.

- Make sure that you enable NTP on the Cisco Unified Communications Manager server. To verify the NTP status, log into the Cisco Unified Communications Manager Command Line Interface, and enter `utils ntp status`.

- Be aware that when you install on an existing server, the hard drive gets formatted and all existing data on the drive gets overwritten.

- Ensure that you connect the server to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation of Cisco Intercompany Media Engine (Cisco IME).

If you want the Cisco IME node to monitor UPS signaling automatically and automatically initiate a graceful shutdown upon power loss, you should use specific UPS and server models. For more information on supported models and configurations, refer to the Release Notes for Cisco Intercompany Media Engine.

- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address.
- You must enable DNS and configure NTP on this server 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.
- Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately three hours.
- Carefully read the information that follows before you proceed with the installation.

Frequently asked questions

Installation

How much time does the installation require?

The entire installation process, excluding pre- and post-installation tasks, takes 20 to 30 minutes, depending on your server type.

What user names and passwords do I need to specify?

During the installation, you must specify the following user names and passwords:

- Administrator Account user name and password

  You use the Administrator Account user name and password to log in to the following areas:

  - Disaster Recovery System
  - Command Line Interface

  To specify the Administrator Account user name and password, follow these guidelines:

  - Administrator Account user name. The Administrator Account user name 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 *Cisco Intercompany Media Engine 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. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters
- Mix letters and numbers
- Include hyphens and underscores
- 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 Intercompany Media Engine. Individual answer files get copied to the root directory of a USB key or a floppy diskette and are used in addition to the Cisco Intercompany Media Engine DVD during the installation process.

The web application provides the following support and information:

- 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 higher.

Cisco requires that you use USB keys that are compatible with Linux 2.4. Cisco recommends that you use USB keys that are preformatted to be compatible with Linux 2.4 for the configuration file. These keys use a W95 FAT32 format.

What are the supported servers?

For information about supported server models, refer to the release notes for your product release.

Which SFTP servers are supported?

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 using GlobalSCAPE with supported Cisco Unified Communications versions, refer to 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/)

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 command line interface (CLI). The system can upload and process only software that Cisco Systems approved. You cannot install or use unapproved third-party software applications.

Perform pre-installation configurations

Complete the following pre-installation tasks to ensure that you can successfully install Cisco Intercompany Media Engine.

Procedure

Step 1 Read this entire document to familiarize yourself with the installation procedure.

Step 2 Cisco recommends that you complete a site analysis and planning session for Cisco IME that includes the off-path adaptive security appliance (ASA) configuration, IP addressing, pin holes, static network address translation (NAT), and demilitarized zone (DMZ) setup. You must understand the Cisco IME requirements that get imposed on the current network setup.
Cisco Unified Communications SRND

Step 3 Enable the necessary traffic on your corporate firewall. You must engage the teams that manage the corporate firewalls and the DMZ, such as your IT and Information Security teams, early in the design and deployment

of Cisco Intercompany Media Engine. Ensure that all of the required access control lists (ACLs) on the corporate firewalls are approved and implemented before making Cisco IME calls.

Step 4 Verify the integrity of any new server hardware (such as hard drives and memory) by running any manufacturer-provided utilities.

Step 5 Record the network interface card (NIC) speed and duplex settings of the switch port to which you will connect the new server.You should configure the same NIC settings on the server and on the switch port. For GigE (1000/FULL), you should set NIC and switch port settings to Auto/Auto; do not set hard values.
Enable PortFast on all switch ports that are connected to Cisco servers. With PortFast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay. [The forwarding delay specifies the amount of time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state].

Step 6 Verify that all servers on which you plan to install Cisco IME are properly registered in DNS.
You need to be able to resolve and ping the `GoDaddy.com` server and `intercompanymedianetwork.com` bootstrap server.

Step 7 Obtain a Cisco IME license file.
See the Obtain license file, on page 8.

Step 8 Record the configuration settings for each server that you plan to install.
To record your configuration settings, see the server configuration data.

Corporate and external firewall settings

This section describes the minimum required ports that need to be configured to support IME traffic. The Corporate Firewall Configuration table provides a summary of the ports that need to be configured on a corporate firewall. The External Cisco IME ASA Firewall table provides a summary of the ports that need to be configured on the off-path ASA. The port configuration shown in these tables 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 1: Corporate firewall configuration

Interface	Direction	Source	Destination	Protocol	Port	Description
Inside	Inbound	Cisco Unified CM IP address	Off-path ASA inside signalling address (same as physical)	TCP	8060	Off-path mapping between Cisco Unified CM and ASA signaling address. Require entries for each Cisco Unified CM in the cluster.
Inside	Inbound	Cisco Unified CM IP address	Off-path ASA inside signalling address (same as physical)	TCP	1024-65535	Off-path mapping between Cisco Unified CM and ASA signaling address. Require entries for each Cisco Unified CM in the cluster.

Interface	Direction	Source	Destination	Protocol	Port	Description
DMZ	Inbound	Offpath ASA inside signaling address (same as physical)	Cisco Unified CM IP address	TCP	5060	SIP Signaling between ASA signaling address and Cisco Unified CM. Require entries for each Cisco Unified CM in the cluster. Port number configurable.
Inside	Inbound	Cisco Unified CM IP address	Cisco IME server DMZ IP address	TCP	5620	VAP communication between Cisco IME and Cisco Unified Communications Manager
Inside	Inbound	All Unified Communication devices, including MeetingPlace, voicemail, softclient IP ranges, voice gateways, and any media device needing to communicate via ASA.	Off-path ASA inside media termination IP	UDP	16384 - 32767	UDP port can be restricted based on Cisco IME enabled ASA media termination address configuration and on the number of simultaneous calls.
DMZ	Inbound	Offpath ASA inside media termination IP (Source port range can be restricted based on Cisco IME configuration.)	All Unified Communication devices, including MeetingPlace, voicemail, softclient IP ranges, voice gateways, and any media device needing to communicate via ASA.	UDP	16384 - 32767	UDP ports for media traffic.
Inside	Inbound	Internal network or any management workstation	Cisco IME server DMZ IP address	TCP	22	SFTP access to Cisco IME server for uploading licenses/software, upgrade, and CLI access.
Inside	Inbound	Internal network or any management workstation	Cisco IME server DMZ IP address	HTTPS	443	RTMT download from Cisco IME server

Interface	Direction	Source	Destination	Protocol	Port	Description
DMZ	Inbound	Cisco IME Server DMZ IP address	GoDaddy website	HTTPS	443	Download certificates from GoDaddy.
DMZ	Inbound	Cisco IME Server DMZ IP address	Any	TLS	6084	IME distributed cache communication outbound from the Cisco IME server towards the Internet
Outside	Inbound	Any	Cisco IME Server DMZ IP address	TLS	6084	IME distributed cache communication inbound from the Internet to the Cisco IME server
DMZ	Inbound	Cisco IME Server DMZ IP address	Any	TLS	8470	IME distributed cache communication outbound from the Cisco IME server towards the Internet
Outside	Inbound	Any	Cisco IME Server DMZ IP address	TLS	8470	IME distributed cache communication inbound from the Internet to the Cisco IME server

Table 2: External Cisco IME ASA firewall (off-path ASA)

Interface	Direction	Source Description	Destination Description	Protocol	Port	Description
DMZ	Inbound	Cisco Unified CM IP address	Remote Cisco Unified CM	TCP	5060-5090	Internal Cisco Unified CM signaling to remote Cisco Unified CM (remote PAT configuration)
DMZ	Inbound	Cisco Unified CM IP address	Remote Cisco Unified CM	TCP	5060	Internal Cisco Unified CM signaling to remote Cisco Unified CM (remote PAT configuration)
Outside	Inbound	Any	Cisco Unified CM IP address	TCP	5060	Remote Cisco Unified CM signaling to internal Cisco Unified CM

Related Topics

Perform pre-installation configurations, on page 4

Obtain license file

You use the Product Authorization Key (PAK) that came with your product to obtain the necessary license for the Cisco IME server. The license file contains the supported version of Cisco IME, MAC address of the Cisco IME server, number of licensed Cisco IME applications (peercount), and information that you need to obtain a certificate from GoDaddy (tag and signature). The certificate enables the Cisco IME server to establish a TLS connection to other Cisco IME servers on the IME distributed cache ring.

Use the following procedure to obtain a license file for a Cisco IME server.

Procedure

Step 1 Enter the Product Authorization Key (PAK) that you received with your Cisco Intercompany Media Engine order in the License Registration web tool at http://www.cisco.com/go/license.

Step 2 Click **Submit**.

Step 3 Follow the system prompts. You must enter the MAC address of the network interface card (NIC) of the server on which you plan to install Cisco Intercompany Media Engine as well as a valid e-mail address. To locate the MAC address, log in to the Cisco IME command line interface (CLI) and enter show status. The MAC address displays in the License MAC field.
The system sends the license file to you via e-mail by using the e-mail address that you provided.

The format of a license file specifies `IME<timestamp>.lic`. If you retain the `.lic` extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Step 4 Upload the license file to the server with the matching MAC address that you provided in Step 3.
See the Upload license file, on page 17.

License file example

The following code shows an example of a Cisco IME license file.

```
INCREMENT IME_SERVICE cisco 8.0 permanent uncounted \VENDOR_STRING=<ime>
<peercount>5</peercount><tag>163d18ab727c0fa14fce75c6651b1362</tag>
<signature>154fe09fdbb012407cbfac8c74c55cb6be460199c813b0af29b83bc3b10824519bef7427f7a
be7a7b9e6692e9b905e73fa9a1199c90ef7fd269c89f0a9179677bbee34cb1eeb915f03e2372cb1e9d272d
af907be0077c7fd128ecc0216f036bb9447f06857cdcb4b066e746dc80ebe33fc212117b5c6c95aa404751
6120e403c320f703a9a94ac7c177a07963dd83aa79b75c1c585250481bce340ef3bf02f86633f245cbfaef
c2a1851b29c6cf48f580655c8a983b65d5584e316f350a15ff90478cbcb8e39128049edbb6972b33203130
00f28db28cc51a8eb7666a40184cb5389e216cdfeac7c1d42b0e4fdf2c608bea28faeff807fcc0862497dd
59ca676</signature></ime><LicFileVersion>1.0</LicFileVersion> \
HOSTID=00163569b2e0 \
NOTICE="<LicFileID>20090730162506350</LicFileID><LicLineID>1</LicLineID> \
<PAK></PAK>" SIGN="0288 1F4A 07D6 0C34 F35B D4D5 0339 C538 \
AC1E BC65 8697 9D5F 18D3 A57D 27DD 18D2 8C3B 14BA E72F 4932 \
E27D 7BE9 C410 5477 9B85 AAF7 2F42 8C44 0985 CFF1"
```

Related Topics

Perform pre-installation configurations, on page 4

Server configuration data

Server information

Because some of the fields are optional, they may not apply to your configuration. The last column in the table shows whether you can change a field after installation; if so, the appropriate Command Line Interface (CLI) command is shown.

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

Table 3: Server configuration data

Parameter	Description	Entry change?
Administrator ID	This field specifies the administrator account user ID that you use for secure shell access to the CLI on the Cisco Intercompany Media Engine server.	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	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	From the list, choose the appropriate country for your installation. **Note** The value that you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI >**set web-security**

Parameter	Description	Entry change?
DHCP	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	A DNS server resolves a hostname into an IP address or an IP address into a hostname. Cisco IME requires that you use a DNS server. Choose **Yes** to enable DNS.	No, you should not change the entry after installation.
DNS primary	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**
DNS secondary	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	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.	es, you can change the entry after installation by using the following CLI command: CLI > **set network gateway**
Hostname	Enter a host name that is unique to your server. The host name 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**

Parameter	Description	Entry change?
IP address	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 changing 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	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	Enter the location of the server. The system uses this information to generate certificate signing requests (CSRs), which are used to obtain third-party certificates. 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	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	Choose the duplex mode for the network interface card (NIC), either Full or Half. Choose the duplex mode for the network interface card (NIC), either Full or Half.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**

Parameter	Description	Entry change?
NIC speed	Choose the speed for the NIC, either 10 megabits per second or 100 megabits per second. This parameter displays 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	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. To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should 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	Enter the name of your organization. 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. The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
Security password	The password must contain at least six alphanumeric characters. The password can contain hyphens and underscores, but it must start with an alphanumeric character. Save this password.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password security**

Parameter	Description	Entry change?
State	Enter the state where the server is located. The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
Time zone	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 timezone configuration, use the following CLI command: CLI > **show timezone config**
Unit	Enter your unit. The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password admin**

Installation wizard navigation

Table 4: Navigation options and actions

Navigation option	Keyboard action
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 or down arrow
Go to the previous window	Space bar or **Enter** to choose **Back** (when available)
Get help information on a window	Space bar or **Enter** to choose **Help** (when available)

Related Topics

Perform pre-installation configurations, on page 4

Start installation

Note If you have a new server with the software pre-installed, you do not need to install from a DVD, unless you want to reimage the server with a later product release.

To start the installation, follow this procedure.

Procedure

Step 1 Insert the installation DVD into the tray and restart the server, so that the server boots from the DVD. After the server completes the boot sequence, the **DVD Found** window displays.

Step 2 To perform the media check, click **Yes**.
If your DVD previously passed the media check, you may choose to skip the media check.
The media check checks the integrity of the DVD and the **Media Check Result** window displays.

Step 3 If you chose **Yes** to perform the media check, perform one of these tasks:

- If the Media Check Result displays Pass, click **OK** to continue the installation.
- If the media fails the Media Check, either download another copy from `Cisco.com` or obtain another DVD directly from Cisco.

The system installer performs the following hardware checks to ensure that your system is configured correctly. If the installer makes any changes to your hardware configuration settings, you get prompted to restart your system. Leave the DVD in the drive during the reboot.

- First, the installation process checks for the correct drivers. Click **Yes**, if you see the following warning: No hard drives have been found. You probably need to manually choose device drivers for install to succeed. Would you like to select drivers now?
- The installation next checks whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this failure is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.
  Note If this step repeats, click **Yes** again.
- If the installation program must install a BIOS update, a notification tells you that the system must reboot. Press any key to continue the installation.
  After the hardware checks complete, the **Product Deployment Selection** window displays.

Step 4 Click **OK**.
If software is currently installed on the server, the **Overwrite Hard Drive** window opens and displays the current software version on your hard drive and the version on the DVD. Click **Yes** to continue the installation or **No** to cancel.
Caution If you chose **Yes** in the **Overwrite Hard Drive** window, all existing data on your hard drive gets overwritten and destroyed.

The **Platform Installation Wizard** window displays.

Step 5 Perform one of the following tasks:

- To enter your configuration information manually and have the installation program install the configured software on the server, click **Proceed** and continue with the basic install.
- To do any of the following tasks, click **Skip** and continue:
  - Manually configure the software that is pre-installed on your server. In this case, you do not need to install the software, but you must configure the pre-installed software.
  - Perform an unattended installation. In this case, you provide preexisting configuration information on a USB key or floppy disk.
  - Install the software before manually configuring it. In this case, the installation program installs the software, then prompts you to configure it manually. You can choose Skip if you want to preinstall the application on your server first, then enter the configuration information at a later time. This method may take more time than the other methods.

The system restarts and the **Preexisting Installation Configuration** window displays.

Step 6 Follow the steps in the installation program.

Step 7 Specify whether you want the automatic negotiation to be enabled or disabled.
The installation process allows you to set the speed and duplex settings of the Ethernet network interface card (NIC) automatically by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, click **Yes**.
  Note To use this option, your hub or Ethernet switch must support automatic negotiation.
- To disable automatic negotiation, click **No**.
  - Choose the appropriate NIC speed and duplex settings and click **OK**.

The **MTU Configuration** window displays.

Step 8 Change the MTU size.
The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which specifies 1500 bytes.

Caution If you configure the MTU size incorrectly, your network performance can be affected.

- To accept the default value (1500 bytes), click **No**.
- To change the MTU size from the operating system default, click **Yes**.
  - Enter the new MTU size; then, click **OK**.

The **DHCP Configuration** window displays.

Step 9 When prompted to choose the DHCP, click **No**.
Cisco requires that you set up a static network IP address for the server rather than use Dynamic Host Configuration Protocol (DHCP).
The **Static Network Configuration** window displays.

Step 10 Enter your static network configuration values and click **OK.**

The **DNS Client Configuration** window displays.

Step 11 Click **Yes** to enable the DNS.
Cisco requires that you enable the DNS.

Step 12 Enter your DNS client information and click **OK.**
The network restarts by using the new configuration information, and the **Administrator Login Configuration** window displays.

Step 13 Follow the steps in the installation program.

Step 14 Choose whether you want to configure an external NTP server or to configure the system time manually.
Cisco Systems recommends that you use an external NTP server to ensure accurate system time. Ensure that the external NTP server specifies stratum 9 or higher (that is, stratums 1 through 9).

- To set up an external NTP server and click **Yes**.
  Enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers. Cisco Systems recommends that you use at least three NTP servers. Click **Proceed** to continue with the installation.

  Note If the Test button displays, you can choose Test to check whether the NTP servers are accessible.

  The system contacts an NTP server and automatically sets the time on the hardware clock.

- To configure the system time manually and click **No**.
  Enter the appropriate date and time to set the hardware clock. Click **OK** to continue with the installation.

  The **Security Configuration** window displays.

Step 15 Follow the steps to complete the installation program.

The system installs and configures the software. The DVD drive ejects, and the server restarts. Do not reinsert the DVD. When the installation process completes, you get prompted to log in by using the administrator account and password.

What to Do Next

Perform post-installation configurations, on page 16

Perform post-installation configurations

After installing the software on your server, you must complete the post-installation tasks listed in the following procedure.

Procedure

Step 1 Install the Real Time Monitoring Tool on a client machine.
You can use the Real Time Monitoring Tool to monitor system health, and to view and collect logs.

For installation instructions and more information about the Real Time Monitoring Tool, see Install RTMT.

Step 2 Upload your Cisco Intercompany Media Engine license file to the server.
See the Upload license file, on page 17.

Step 3 Obtain the Cisco Intercompany Media Engine certificates from `GoDaddy.com`.

See the Purchase and enroll certificate, on page 18 and the Renew certificate, on page 19.

Step 4 Access and install a self-signed or third-party certificate for secure communication between Cisco Unified Communications Manager and Cisco Intercompany Media Engine.
See the following topics:

- Generate self-signed certificate
- Generate third party certificate

Step 5 Configure the backup settings.
Remember to back up your Cisco Intercompany Media Engine data daily. See the Disaster Recovery System.

Step 6 Set up a VAP server.
For more information, see Set up VAP server, on page 19.

Step 7 Set up Cisco IME server.
For more information, see Set up IME server, on page 20.

Upload license file

Use the following procedure to upload a license file to the Cisco IME server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the Obtain license file, on page 8.

Before You Begin

Make sure that the Cisco IME server software has been installed on the server.

Procedure

Step 1 Save the Cisco IME license file (.lic) to a temporary directory on your local hard drive.

Step 2 Open an SFTP client and connect to the Cisco IME server by using the adminsftp user and the administrator password that you set up during installation.

Step 3 Navigate to the license directory by entering cd license and copy the license file to that directory.

Step 4 Type put `<license filename>`, where `<license filename>` specifies the license file name that you received via email.

Step 5 Upload the Cisco IME license by logging into the Cisco IME command line interface (CLI) and entering **utils ime** license file install `<license filename>`.

Note The format of the license file that you receive specifies IME<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

After installation, the server stores license files in `/usr/local/ime/conf/licfiles`. The server stores license logs at `/active/cm/trace/ime/licensing/log4j`.

Related Topics

Perform post-installation configurations, on page 16

Purchase and enroll certificate

GoDaddy provides certificates for the IME distributed cache ring. GoDaddy uses information in the Cisco IME license, including the tag, peerIDCount, and signature, to identify each server uniquely and to generate certificates.

You purchase a certificate for Cisco IME server on the GoDaddy website. After you purchase the certificate, you enroll the certificate with GoDaddy. During the enrollment process, you provide information that indicates that you have a valid server that can obtain a certificate. Certificates remain valid for one year from the date of purchase.

The Cisco IME server attempts to renew the certificate before the expiration date. If the auto-enrollment fails, the server generates an EnrollFailure alarm. You must manually renew the certificate. For more information on renewing certificates, see the Renew certificate, on page 19.

Use the following procedure to purchase and enroll a new certificate.

Before You Begin

Install the license on the Cisco IME server, as described in the Upload license file, on page 17.

Procedure

Step 1 Go to http://www.godaddy.com.

Step 2 Log in to your Account Manager.

Step 3 In the My Products section, click **SSL Certificates**.

Step 4 Purchase a certificate for the Cisco IME server.

Note For more detailed instructions on purchasing a certificate, refer to the support topic on the GoDaddy website for requesting and installing a Cisco Intercompany Media Engine certificate at http://help.godaddy.com/article/5414.

During the purchase process, you must enter the server ID of your server. To obtain this ID, log in to the CLI on the Cisco IME server and type show ime certenrollment server ID.

Step 5 When prompted, install the certificate on the Cisco IME server by typing `utils ime certenrollment enroll` in the Cisco IME server CLI.

Step 6 The Cisco IME server generates the SuccessfulEnrollment alert upon successful enrollment and generates the EnrollFailure alert upon a failed enrollment.

Step 7 To view the certificate on the Cisco IME server, go to the CLI and type `show cert own intercompanymedianetwork`.

Note The system stores manual enrollment and auto-enrollment log files in the following directories, respectively: `/active/platform/log/cli*.log` and `/active/platform/log/certm.log`.

Related Topics

Perform post-installation configurations, on page 16

Renew certificate

You must use this procedure to manually renew the certificate:

Procedure

Step 1 Go to http://www.godaddy.com.

Step 2 Log in to your Account Manager.

Step 3 In the My Products section, choose SSL Certificates and find the certificate that you want to renew.

Note For more detailed instructions on renewing a certificate, refer to the support topic on the GoDaddy website for renewing a Cisco Intercompany Media Engine certificate at http://help.godaddy.com/article/5415.

Step 4 After GoDaddy receives your payment, one of the following events occurs:

- If GoDaddy receives your payment before the old certificate expires, the certificate renews without further action from you.
- If GoDaddy receives your payment after the old certificate expires, type `utils ime certenrollment enroll` in the Cisco IME server CLI.

Step 5 The Cisco IME server generates the SuccessfulEnrollment alert upon successful enrollment and generates the EnrollFailure alert upon a failed enrollment.

Step 6 To view the certificate on the Cisco IME server, go to the CLI and type `show cert own intercompanymedianetwork`.

Note The system stores manual enrollment and auto-enrollment log files in the following directories, respectively: `/active/platform/log/cli*.log` and `/active/platform/log/certm.log`.

Related Topics

Perform post-installation configurations, on page 16

Set up VAP server

For more details about the command options listed in this procedure, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide* .

Complete the following steps to set up a VAP server:

Procedure

Step 1 In the Cisco IME CLI , run the following command to set up a VAP server name and port: `add ime vapserver` You will be prompted for the VAP server name, port, and authentication mode. The name the you enter represents a unique identifier for this instance. The name does not need to match the Cisco Unified

Communications Manager name. You need to be sure that the authentication mode that you choose matches that of the Cisco Unified Communications Manager (encrypted or authenticated).

Note If you have more than one Cisco Unified Communications Manager that uses the same Cisco IME server, you need to add a VAP server entry for each cluster. Make sure to specify a unique port number for each VAP server name. You can have multiple VAP server instances, where one instance is for authenticated mode and another is for encrypted and authenticated mode. These instances should use different ports.

Step 2 Run the following command to view all of the VAP servers that you have administered: `show ime vapserver all`

Step 3 Run the following commands to set the necessary options for each VAP server instance that you configured:

Note Cisco highly recommends that you set the authentication mode to Encrypted.

- `set ime vapserver authenticationmode`
- `set ime vapserver enabled`
- `set ime vapserver keepaliveinterval`
- `set ime vapserver maxconnectionsallowed`
- `set ime vapserver port`

Step 4 Run the following command to set up the VAP user credentials on the Cisco IME server: `add ime vapusercredentials`

The application username and password that you enter must match those that you enter for the application user in Cisco Unified Communications Manager Administration.

The ticket password and Epoch must match those configured on the Cisco IME ASA. Cisco recommends that you create a password containing at least 20 characters.

What to Do Next

You can set up the Cisco IME server before the server can join the IME Distributed Cache. For more information, see Set up IME server, on page 20.

Related Topics

Perform post-installation configurations, on page 16

Set up IME server

Complete the following steps to set up the Cisco IME server:

Procedure

Step 1 Set up the external address on the Cisco IME server.
For more information, see Set up external address on IME server, on page 22.

Step 2 Run the following commands to display the lists of IME server peer IDs and IP address of bootstrap server.

- `show ime peerid`
  If you do not see a peer ID, you may have an issue with your Cisco IME certificate. You should fix the problem before continuing the configuration.
- `show ime bootstrap ip`
  Make sure that at least one IP address displays. If no IP addresses displays, this indicates that the Cisco IME cannot reach the bootstrap severs via DNS.

Step 3 Run the following command to check the status of the IME server on the IME distributed cache: `show ime dht summary`

Example:

```
Peer ID = 514dd001c7553593ebefee2b076ad9d4
DHT Health....................... = GREEN
BootStrap: 5619e12c7a647e1d3364c8a46c9e58f7
Last Contact (sec)................... = 48
Current Sequence..................... = 1250036323
Num. Tokens Received................. = 3
Delay from BootStrap................. = 1
Peer Count Distance.................. = 5
```

The DHT Health field shows the status of the server in the Peer ID field. Green indicates a functional status.

If the peer ID status does not display as green, verify that you installed Cisco IME certificates correctly and check the Cisco IME ports and the Cisco IME-enabled ASA.

You may also need to use the show ime addressing command to verify that you set the public IP address correctly.

Step 4 Run the following command to set up the customer contact information on the IME server: `set ime customerinfo`

This information gets stored on your Cisco IME server and can be used by Cisco Technical Support to contact your company, if they detect a misconfiguration on your Cisco IME server.

After you have set your customer information, you can use the `show ime customerinfo` command to view this information.

The system prompts you for the following information:

- Company name - The name of the company using this Cisco IME server
- Unit name - Unit within the company (city name or department)
- State - State where this server is located
- Country - Country where this server is located
- Support contact name - Person that should be contacted, if Cisco detects a misconfiguration on your Cisco IME server
- Support contact e-mail - E-mail of the support contact for your company
- Support contact phone - Phone number of your support contact

Related Topics

Perform post-installation configurations, on page 16
Set up VAP server, on page 19

Set up external address on IME server

Complete the following steps to set up an external address on the Cisco IME server:

Procedure

Step 1 Log into the Cisco IME CLI and enter the following command: `set ime addressing publicipaddrv4 external ip addr`

Example:
For example, if the public IP address of the Cisco IME equals 65.65.65.65, enter: `set ime addressing publicipaddrv4 65.65.65.65`

Step 2 Check the settings by entering the following command: `show ime addressing`

Example:
The following example shows the Public and Private IP addresses of a Cisco IME server:

```
admin: show ime addressing
====================================
Public IP Address = 65.65.65.65
Private IP Address = 10.10.10.10
DHT Port = 6084
Validator Port = 8470
====================================
```

Related Topics

Perform post-installation configurations, on page 16
Set up IME server, on page 20

Reset administrator and security passwords

To perform the password reset process, you must connect to the system through the system console; 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 displays.

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 Re-enter 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.

Upgrade the Cisco IME

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

Use the following procedure to upgrade the Cisco Intercompany Media Engine (Cisco IME) server software:

Note When you upgrade the Cisco IME, the services that communicate with the Cisco IME service on the Cisco Unified Communications Manager get stopped. This stoppage causes the Cisco Unified Communications Manager to temporarily stop learning routes until the upgrade completes and the Cisco IME server gets switched to the new release. During this time, an alert that indicates that Cisco IME service is down will be seen on the Cisco Unified Communications Manager server. To minimize impact on the Cisco Unified Communications Manager, Cisco highly recommends that you upgrade the Cisco IME server during an inactive period. The upgrade procedure takes approximately 20 to 30 minutes.

Procedure

Step 1 Obtain the upgrade media to upgrade the Cisco Intercompany Media Engine server.

Step 2 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 IME 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 Create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.
  - Open an SFTP client and connect to the Cisco IME 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.
- Type put <upgrade filename>, where <upgrade filename> specifies the upgrade file name that you downloaded from Cisco.com or obtained on a DVD.
  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 3 After you have inserted the DVD into the server or uploaded the upgrade file to the remote server or local directory, log into the Cisco IME CLI and enter utils system upgrade initiate.

Step 4 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 5 Follow the system prompts for the upgrade option that you chose.

Step 6 The system prompts you when the upgrade process completes. 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 7 After the installation completes, log into the Cisco IME CLI and verify the following:

- Make sure that the DHT displays a green health status by logging into the Cisco IME CLI and entering **show ime dht summary**. The server may take 20 minutes to join the ring and for the status to turn green.
- Make sure that the Registration Status equals Registered, and the Client IP ADDR equals the IP address of the Cisco Unified Communications Manager server by entering **show ime vapstatus summary**.

If you upgraded from the Local Upgrade Directory, the system removes the ISO file from the local directory on your hard drive after the upgrade is complete. If you need to perform another upgrade using the same load, you must copy the ISO file to your local directory again or select a different source.

Troubleshooting

Use the following sections to troubleshoot problems that occur during installation of the Cisco Intercompany Media Engine software:

- Installation network errors, on page 25
- Examine log files, on page 26

Installation network errors

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If the server cannot connect, a message displays; you get prompted to select one of the following options:

- RETRY - The installation program tries to validate networking again. If validation fails again, the error dialog box displays again.
- REVIEW (check install) - This option allows you to review and modify the networking configuration. When detected, the installation program returns to the network configuration windows.

  Networking gets validated after you complete each networking window, so the message may display multiple times.
- HALT - The installation halts. You can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.
- IGNORE - The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box may display multiple times. If you choose to ignore network errors, the installation may fail.

Examine log files

If you encounter problems with the installation, you may be able to examine the install log files by entering the following commands in Command Line Interface.

To obtain a list of install log files from the command line, enter:

CLI>`file list install *`

To view the log file from the command line, enter:

CLI>`file view install log_file`

where `log_file` specifies the log file name.

You can also view logs by using the Real Time Monitoring Tool. For more information on using and installing the Real Time Monitoring Tool, refer to the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

You can get more information about installation events by viewing or downloading the system history log. Refer to the following listings for more information:

- System history log
- *Working with Trace and Log Central* chapter in the *Cisco Unified Real Time Monitoring Tool Administration Guide*.