Installing Cisco IPICS

This chapter describes how to deploy and configure a VM and install the Cisco IPICS server software. The VM OVA file includes the Cisco IPICS installer.

This chapter includes the following sections:

Before You Begin

This section describes the activities that you must follow to prepare for the Cisco IPICS operating system and server installations and includes the following sections:

Obtaining the IP Addresses for Your Cisco IPICS System

To facilitate communications between your users, your Cisco IPICS system requires a pool of IP addresses that can be reached by all users in your network domain.

The Cisco IPICS server requires a static, local IP address that is advertised on the network. Cisco IPICS end points, such as the IDC or Cisco Unified IP Phone, must have the static address of the Cisco IPICS server to maintain communications.

Because Cisco IPICS converts analog push-to-talk (PTT) radio traffic to IP traffic, each radio channel gets mapped to an IP multicast address. Similarly, in hoot'n'holler systems, each talk group gets mapped to an IP multicast address. Users on IP-connected devices, such as the IDC, can participate in these channels by connecting via a multicast IP address or by using a unicast remote connection through the Session Initiation Protocol (SIP).

Cisco IPICS requires a multicast address for a variety of communication activities:

For ease of allocating IP addresses, it is helpful to obtain a subnet of IP addresses from which you can configure the devices that are part of that subnet.

Note Cisco recommends that you specifically configure the Loopback0 interface when there is more than one IP path to the RMS. However, you may configure an interface other than Loopback0 if specific criteria are met. For details about this criteria, see the "Configuring the Cisco IPICS RMS Component" appendix in *Cisco IPICS Server Administration Guide*.

For information about configuring and using IP addresses with Cisco IPICS, and for more information about the RMS, refer to the "Configuring the Cisco IPICS RMS Component" appendix in *Cisco IPICS Server Administration Guide*.

Preinstallation Checklist

Before you begin the installation, make sure that you perform the following tasks:

Preinstallation Tasks	Checkoff
Cisco strongly recommends that you attach an uninterruptible power supply (UPS) to your system and ensure that the UPS is operating correctly.	❑
Ensure that you have obtained the IP address, subnet mask, default gateway, and DNS server (optional) information for the Cisco IPICS server from your network administrator.	❑
Check that you have obtained the Media Access Control (MAC) address for the eth0 interface of the Cisco IPICS server. Cisco IPICS uses the MAC address of the server to validate the Cisco IPICS license. **Note** To obtain the MAC address, enter the following command. The HWaddr field in the command output contains the MAC address for the eth0 interface: `[root]# ifconfig eth0` Alternatively, you can start the Cisco IPICS Administration Console from a web browser. When the License Management page appears, the MAC address is displayed near the top of the page. In a system with multiple network interface cards (NICs), Cisco IPICS always uses the eth0 MAC address to validate the license, even if eth0 is disabled.	❑
If your network uses the Network Time Protocol (NTP), obtain the IP address or DNS name of the NTP server.	❑
You can install a third party certificate to replace the Cisco IPICS self-signed certificate. For more information about installing third party certificates, see the "Installing Third Party Certificates on the Cisco IPICS Server" section on page 2-21. A third-party certificate is not required for use with Cisco IPICS.	❑

To ensure the functionality of Cisco IPICS, you should also perform the following tasks either before or after you install Cisco IPICS:

Tasks	Checkoff
Ensure that you have obtained multicast IP addresses for channels and VTGs. (If you do not have access to this information, contact your system administrator.)	❑
If your deployment includes the RMS component, check to make sure that the T1/E1 interfaces on the RMS are connected via a loopback cable. This cable is a short-length crossover cable with the following pinouts: 1-4, 2-5, 4-1, 5-2. One end of the cable is attached to each of the RJ-45 connectors on the T1/E1 interfaces for the RMS device. The connected interfaces are used for voice signaling and media for any SIP-based connections with Cisco IPICS. If you do not have a crossover cable, contact your authorized Cisco support representative for assistance to obtain one.	❑

If you use the Cisco IPICS dial engine, which controls dial-in and dial-out functionality, ensure that you complete the following tasks before you use the dial engine:

Tasks	Checkoff
Ensure that you have the IP address, SIP listening port, and preferred transport type of your SIP provider. Support for SIP-based dial functionality is provided via Cisco Unified Communications Manager or a Cisco router that runs a supported version of Cisco IOS and Cisco Unified Communications Manager Express as the SIP provider. The policy engine requires that a SIP provider be configured in the customer network. For information about configuring a SIP provider, see *Cisco IPICS Server Administration Guide*.	❑
If your SIP provider is Cisco Unified Communications Manager, determine the authentication credentials that Cisco IPICS uses when it initiates a call into Cisco Unified Communications Manager. Authentication is not required with Cisco Unified Communications Manager Express.	❑
Be sure that your SIP provider uses a supported version of Cisco Unified Communications Manager, Cisco IOS or Cisco Unified Communications Manager Express. See *Cisco IPICS Compatibility Matrix* for a current list of supported hardware and software for use with Cisco IPICS.	❑
Determine how your Cisco IPICS system fits into the dial plan of your SIP provider. For example, determine the range of directory numbers (DNs) that must be routed from the SIP provider to the Cisco IPICS system.	❑

Deploying the VM

The following sections describe how to configure a virtual machine (VM) for Cisco IPICS. You can install and operate the Cisco IPICS application, the UMS, the ISSIG, and the DFSIG on a VM. Each component must run in its own VM.

This chapter includes these sections:

Installing VMWare ESX or ESXi on a Device

The following sections describe how to install VMware ESX or ESXi on the device on which you will run the VM. Perform the steps that are described in the section for your device.

- Installing VMware ESX or ESXi on a Cisco UCS B-Series Server, page 2-4
- Installing VMware ESX or ESXi on a Cisco UCS C-Series Server, page 2-4
- Installing VMware ESX or ESXi on a Cisco UCS E-Series Server, page 2-4

Installing VMware ESX or ESXi on a Cisco UCS B-Series Server

To install VMware ESX or ESXi on a Cisco UCS B-Series server, see *Cisco UCS B-Series Blade Servers VMware Installation Guide*.

This document is available at:

http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_B-Series_VMware_Install.html

Installing VMware ESX or ESXi on a Cisco UCS C-Series Server

To install VMware ESX or ESXi on a Cisco UCS C-Series server, see *Cisco UCS C-Series Servers VMware Installation Guide*.

This document is available at:

http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_C-Series_VMware_Install.html

Installing VMware ESX or ESXi on a Cisco UCS E-Series Server

To install VMware ESX or ESXi on a Cisco UCS E-Series server, see *Getting Started Guide for Cisco UCS E-Series Servers*.

This document is available at:

http://www.cisco.com/en/US/docs/unified_computing/ucs/e/1.0/gs/guide/b_Getting_Started_Guide_chapter_010.html

Obtaining and Deploying the VM OVA Image for the Cisco IPICS Operating System

This section describes how to obtain and deploy the VM OVA image for Cisco IPICS. This process installs the Cisco IPICS operating system and configures the VM.

The VM OVA image is approximately 1.6 GB. This file can take some time to download.

Procedure

Step 1 From a client PC, take these actions to obtain the VM OVA image:

a. Go to this URL (you must have a valid Cisco.com user ID and password to access this URL):

http://www.cisco.com/cisco/software/navigator.html?mdfid=280723930&flowid=7120

b. Click the **IPICS Release 4.9** link.

c. Click **Download** next to the appropriate file for your installation:

- ipics-4.9.1-2cpu.ova—Use this file if you are running the VM on a device that has two CPUs and on which you are installing the Cisco IPICS server software
- ipics-4.9.1-4cpu.ova—Use this file if you are running the VM on a device that has four CPUs and on which you are installing the Cisco IPICS server software
- ums-4.9.1-2cpu.ova—Use this file if you are running the VM on a device that has two CPUs and on which you are installing the UMS software
- issig-4.9.1-2cpu.ova—Use this file if you are running the VM on a device that has two CPUs and on which you are installing the ISSIG software
- dfsig-4.9.1-2cpu.ova—Use this file if you are running the VM on a device that has two CPUs and on which you are installing the DFSIG software

d. Follow the onscreen instructions to download the file to your local drive.

Step 2 From a client PC, use the VMware vSphere client application to log in to VMware ESX or ESXi on the device that is to host the VM.

Step 3 From the list of hosts in the left panel of the vSphere client window, click the host on which you want to deploy the OVF template.

Step 4 Choose **File > Deploy OVF Template...** .

The Deploy OVF Template Wizard starts.

Step 5 In the Deploy OVF Template Wizard, take these actions:

a. In the Deploy OVF Template window, navigate to and select the OVF template that you downloaded in Step 1, and then click **Next**.

b. In the OVF Template Details window, click **Next**.

c. In the Name and Location window, enter a name for the VM in the Name field, and then click **Next**.

d. In the Datastore window, click the datastore in which to store the VM files, and then click **Next**.

e. In the Disk Format window, click the **Thin provisioned format** radio button, and then click Next.

f. In the Ready to Complete window, click **Finish**.

Step 6 When the Deployment Completed Successfully window appears, click **Close** in that window.

Step 7 From the list of hosts in the left panel of the vSphere client window, click the name of the new VM that you configured in Step 5c.

Step 8 Power on the new VM.

Step 9 At the Welcome window, click **Forward** to display the Root Password window.

Step 10 Enter and confirm a password for the root user.

The root user has access to all the files in the Cisco IPICS server. Cisco IPICS requires that you use strong passwords that include the following elements:

- Minimum of 8 characters
- At least one upper case letter
- At least one lower case letter
- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

If you need to change the root password at a later date, you can log in to the Cisco IPICS server as the root user and change it by using the **reset_pw** command. For more information, refer to the "Using the Cisco IPICS CLI Tools and Service Commands" chapter in the *Cisco IPICS Troubleshooting Guide*.

Step 11 Click **Forward**.

Step 12 Enter and confirm a password for the GRUB (boot loader) menu.

The boot loader password enables access to the boot loader menu, which allows a system administrator to boot the server into single-user mode. Single-user mode is required to recover a lost root password.

This password must contain at least 6 characters.

Step 13 Click **Forward**.

Step 14 Enter a system user name and user full name, and enter and confirm a password.

You must create a system user to perform administrative tasks on your server. This user password has the same requirements as the root password.

Step 15 Click **Forward** to open the Network Setup window.

Step 16 In the Interface Settings area, enter the fully-qualified hostname, IP address, subnet mask, and gateway information in the specified fields.

Step 17 (Optional) In the DNS Information area in the Network Setup window, enter the IP address of your primary and secondary DNS server.

Step 18 Click **Forward** to open the Timezone window.

Step 19 Choose the correct time zone for your area from the choices in the selection list.

If your system clock uses Universal Coordinated Time (UTC), make sure that you check the **System Clock uses UTC** check box. Cisco recommends that UTC be used, particularly in Cisco IPICS deployments that include high availability.

Step 20 Click **Forward** to open the Date and Time window.

Step 21 Choose one of the following options to set the system date and time:

- If your network uses the Network Time Protocol (NTP), choose the **Network Time Protocol** tab and check the **Enable Network Time Protocol** check box. Enter the name or IP address of an NTP server in the Server field, and click **Add**. Repeat to add additional servers. To delete a server, choose the server, and click **Delete**.

  If you configure NTP on the server, your system administrator should provide instructions to IDC users to also configure the Windows Time Service on their IDC client machines to enable synchronization between the IDC and the server logs. For detailed information about configuring the Windows Time Service, go to the Microsoft support site and search for Article ID 307897.

  If you install a time-bound license for your system, use caution when enabling NTP. Adjustments to the system date can cause Cisco IPICS to invalidate your license. For more information, see the "Managing Time-Bound Licenses" section on page 2-17.

  Cisco recommends that NTP be used, particularly in Cisco IPICS deployments that include high availability.

- If your network does not use NTP, choose the **Date & Time** tab and enter the current date and time in the appropriate fields.

Step 22 Click **Forward** to open the Finish Setup window.

Step 23 Click **Forward**.

The system processes an internal check list as it boots up. After the system has booted up, Cisco IPICS displays the following text:

```
Cisco IPICS
hostname login:
```

where *hostname* represents the host name that you specified in Step 16.

You can now install the Cisco IPICS server software, the UMS, the ISSIG, or the DFSIG in the VM.

Installing the Cisco IPICS Server Software

After you have successfully deploy the VM OVA Image for the Cisco IPICS Operating System, you can install the Cisco IPICS server software.

The Cisco IPICS server installation program uses a text-based interface. This installation procedure allows you to choose from the following install options:

- Install—This option installs the Cisco IPICS server software.
- Upgrade—This option upgrades your server from a previous version of Cisco IPICS. For information about performing an upgrade of the Cisco IPICS server software, see Chapter 3, "Upgrading Cisco IPICS."

Be aware that the options that the installer displays may differ depending on the software version that is running on your system.

You must log in as the Linux root user to perform the Cisco IPICS installation. If you attempt to run the installation from any other user ID, the installation returns an error and exits.

To terminate the installation process at any time, press **Ctrl+C**.

To install the Cisco IPICS server software, perform the following procedure on the server on which you deployed the VM:

Procedure

Step 1 To start the installation, log in as the root user and enter the following commands, where *installerfilename*.bin specifies the name of the installer file:

[root]# **cd /root/installer**

[root]# ***./installerfilename*.bin**

Cisco IPICS begins the installation process. After a short time, you see a Welcome message.

Step 2 When you see the "Welcome to the Cisco IPICS Software Installation Program" message, type **y**, then press **Enter**.

Text displays to inform you that you must read and accept the terms of the End User License Agreement (EULA) before you can proceed.

Step 3 Take these actions:

a. Press **Enter** to display the EULA.

b. Press the **Spacebar** to scroll through and view the EULA, then type **y** and press **Enter** to continue with the installation.

You must accept the terms of the EULA to proceed.

The installation program prompts you to enter a password for the ipics user. The ipics user has the capability to perform all administration-related tasks via the Cisco IPICS Administration Console.

Step 4 Enter a password for the ipics user in the password field and press **Enter**.

Cisco IPICS requires that you use strong passwords that include the following elements:

- Minimum of 8 characters
- At least one upper case letter
- At least one lower case letter
- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

Note The installation program also creates a password for the informix Linux user by using a randomizing algorithm. The informix user has full administrative permission to the Informix database instance and belongs to the ipics and informix linux groups. The ipics linux group includes permission to Cisco IPICS application-related folders, files, and scripts. The informix linux group includes full permission to the Cisco IPICS database server folders, files, and scripts. The password for this user ID never expires.

Step 5 Reenter the password for the ipics user, then, press **Enter**.

The installation program prompts you to enter a password for the Cisco IPICS ipicsadmin (administrative) Linux user. That ipicsadmin user belongs to the ipics linux group. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database.

When you see the prompt that the password has been accepted, press **Enter** to continue.

Step 6 Enter a password for the ipicsadmin user in the password field to create the ipicsadmin user password, then press **Enter**.

Cisco IPICS requires that you use strong passwords that include the following elements:

- Minimum of 8 characters
- At least one upper case letter
- At least one lower case letter
- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

Note The password for the ipicsadmin user never expires.

Step 7 Reenter the password ipicsadmin user, then press **Enter**.

Step 8 When you see the prompt that the password has been accepted, press **Enter** to continue.

Step 9 To begin the installation process, type **y** then press **Enter**.

The Cisco IPICS software begins the installation process.

A progress bar indicates the percentage of the installation that has completed.

Step 10 After the installation completes, a message informs you of the status and prompts you to reboot.

Step 11 Type **y** and press **Enter** reboot your server.

The server reboots and your Cisco IPICS server becomes available.

Note If you enter **no**, complete the restart before you attempt to log in to Cisco IPICS. Cisco IPICS processes, such as the tomcat service and database server, do not start until you reboot the server.

To reboot your server at a later time, follow the procedure in the "Restarting or Shutting Down the Server" section on page 2-9.

Restarting or Shutting Down the Server

To restart the server, perform the following procedure:

Caution When you shut down or restart your server, some functionality is affected and some types of endpoint may get disconnected. In addition, Cisco IPICS logs out all users who are logged in to the Administration Console. Therefore, make sure that you only shut down or restart your server during a maintenance window or other period of system non-use.

Procedure

Step 1 Log in to the Cisco IPICS server with the root user ID by taking either of the following actions:

- To log in to the server from the server console, follow these steps:
  a. Log in to the Cisco IPICS server by entering **root** for the user name.
  b. When you are prompted, enter the root user password.
- To log in to the server remotely, follow these steps:
  a. Access the Cisco IPICS server via an SSH client.
  b. Log in to the server by entering the IP address or host name of the server.
  c. Log in by using the root user ID by entering **root** for the user name.
  d. When you are prompted, enter the root user password.

  A terminal window displays.

Step 2 To reboot the server, enter the following command:

[root]# **reboot**

The server reboots.

To shut down the server, perform the following procedure.

Note Cisco recommends that you gracefully shut down the server by performing the following procedure instead of pressing the power button to shut down the server.

Procedure

Step 1 Log in to the Cisco IPICS server with the root user ID.

A terminal window displays.

Step 2 To shut down the running processes in the server, enter the following command:

[root]# **shutdown -h** [*hh***:***mm*|**+***m*]

where:

- *hh***:***mm* specifies the time at which the shutdown should occurs (*hh* is one or two digits that designate the hour and *mm* is the minute of the hour.
- **+***m* specifies the number of minutes (*m*) to wait before the shutdown occurs

Tip To immediately shut down the running processes, enter the following command:

[root]# **shutdown -h now**

The server terminates its running processes. If you are directly connected to the server, the console displays messages as each process terminates.

Preparing to Use Cisco IPICS

After you complete the software installation, you must complete the following tasks before you can use Cisco IPICS:

- Checking the Installation, page 2-11
- Managing Your Licenses and Certificates, page 2-11
- Viewing the License Summary Information, page 2-15

For more information about Cisco IPICS administration and configuration tasks, See *Cisco IPICS Server Administration Guide*.

Checking the Installation

After you complete the Cisco IPICS server software installation, you should be able to access the Cisco IPICS Administration Console by logging in via a supported browser. (There may be a delay of a few minutes before you can access the console.)

You can access the Administration Console from any computer that has IP connectivity to the Cisco IPICS server and that meets the requirements that are described in *Cisco IPICS Compatibility Matrix*.

To access the Cisco IPICS Administration Console and check the installation, perform the following procedure:

Procedure

Step 1 Open a supported Internet browser window on your PC.

Step 2 In the Address field in the browser, enter the following address, where *server* is the IP address or the host name that you configured for the Cisco IPICS server:

https://*server*

Because your browser does not trust the Cisco IPICS server self-signed SSL certificate, a Security Alert window displays. You can suppress this window by using a third-party certificate or by adding the Cisco IPICS server self-signed certificate to the browser trust list.

Step 3 Click **Continue to this website** to close the window and access the login screen.

Step 4 Log in by using the ipics user ID and password.

The ipics user ID is the application-level user ID that can perform all administration-related tasks by using the Administration Console.

The **Administration > License Management** window displays with a message that informs you to upload a license file before you can use the system.

To obtain your license file, see the "Obtaining Your License File" section on page 2-12.

If you are not able to access Cisco IPICS from your browser, see the "You Cannot Connect to the Server By Using Your Browser" section on page 9-3.

Managing Your Licenses and Certificates

After you install Cisco IPICS, you can log in to the Administration Console, but you will not be able to use any features until you upload the license file. You use the Product Authorization Key (PAK) that was included in your Cisco IPICS product package to obtain a license file.

The license that you purchased is based on the following licensable features:

- The concurrent number of land mobile radio (LMR) ports
- The concurrent number of multicast ports
- The concurrent number of Cisco Unified IP Phone users
- The concurrent number of dial users
- The number of IDC Silver licence users

- The number of IDC Platinum license users
- The total number of ops views
- The concurrent number of mobile endpoint users
- The concurrent number of end-to-end vocoders (used for P25 channels)
- The concurrent number of gateway vocoders (used for P25 channels)
- The concurrent number of DFSI gateway fixed station ports
- The concurrent number of UMS servers
- The concurrent number of ISSI gateway servers
- The concurrent number of DFSI gateway servers
- The number of Cisco IPICS ops views
- Cisco IPICS base server license
- UMS high availability license
- Policy engine base license
- High availability license

Note To enable the policy engine for use, you must obtain a separate license.

The licenses that you purchased determine the total number of corresponding features that you can use. If you require additional licenses, contact your Cisco representative.

This section includes the following sections:

- Obtaining Your License File, page 2-12
- Uploading the Cisco IPICS License Files, page 2-14

Obtaining Your License File

Your Cisco IPICS product package includes a Software License Claim Certificate that contains a PAK, which is uniquely created from your sales order. You use this key to obtain licenses for your Cisco IPICS installation.

You can order initial or additional licenses any time after you begin the installation process.

To use your PAK to obtain your Cisco IPICS licenses, perform the following procedure:

Procedure

Step 1 Locate your Software License Claim Certificate that was included in your Cisco IPICS product package. Look for the PAK at the bottom of this certificate.

Note If you ordered your Cisco IPICS server software directly from Cisco, your package may include only one PAK. However, if you purchased Cisco IPICS through a distributor or reseller, you should have several individual packages, each with its own PAK. In this case, you must process all of your PAKs individually. Cisco sends you a license file for each one.

Step 2 Retrieve the MAC address that you noted during the Cisco IPICS operating system installation.

Note If you misplaced the MAC address, enter the following command to obtain it. The HWaddr field in the command output contains the MAC address for the eth0 interface:

[root]# **ifconfig eth0**

Alternatively, you can start the Cisco IPICS Administration Console from a web browser. When the License Management page appears, the MAC address is displayed near the top of the page.

Step 3 Order a license by accessing Cisco.com at the following URL (you must have a valid Cisco.com user ID and password to this URL):

http://www.cisco.com/go/license

After you process your license order, Cisco.com sends you an e-mail with the license file as an attachment. If you processed several separate PAKs, Cisco.com sends you several e-mail responses with a license file attached to each one. When you upload these files, Cisco IPICS adds the licenses from each file and monitors your system activity based on the aggregated license files.

Step 4 Save the license file to your PC by performing the following steps:

a. Open the e-mail that contains the license file attachment.

b. Right-click the license file attachment in the e-mail.

c. Click **Save As**.

The Save Attachment window displays.

d. Select the folder on your PC where you would like to download the license file.

e. Ensure that the following values appear in the fields of the Save Attachment window:

- The file name of the license appears with a .lic file type in the File name field.
- **All Files (*.*)** appears in the Save as type field.

f. Click **Save**.

The e-mail program downloads the license file to your PC.

Note Cisco IPICS does not support the editing or modification of the license file name or file type. If you change the license file name or use an extension other than .lic, you may invalidate your license and cause the system to become inoperable.

Step 5 Upload the Cisco IPICS license.

See the "Uploading the Cisco IPICS License Files" section on page 2-14 for instructions about uploading the Cisco IPICS license file.

After you upload your license file, the license manager processes the new licenses and updates the total number of licenses.

Step 6 If you require additional licenses, contact your distributor or reseller to purchase the licenses.

Uploading the Cisco IPICS License Files

After you receive your license files, you can upload them by accessing the **Administration > License Management** window in the Cisco IPICS Administration Console.

Note When you upload a license file, Cisco IPICS places the file in the /root/tomcat/current/webapps/license directory.

To upload license files, perform the following procedure:

Procedure

Step 1 Open a supported browser window on your PC.

Step 2 In the Address field in the browser, enter the following address, where *server* is the IP address or the host name that you configured for the Cisco IPICS server:

https://*server*

Because your browser does not trust the Cisco IPICS server self-signed SSL certificate, a Security Alert window displays. You can suppress this window by using a third-party certificate or by adding the Cisco IPICS server self-signed certificate to the browser's trust list.

Step 3 Click **Continue to this website** to close the window and access the login screen.

The Cisco IPICS Login window displays.

Step 4 Log in to the Cisco IPICS server by using the ipics user ID and password.

The system prompts you to upload the license file.

Note The system does not prompt you to upload a license file if you have previously uploaded a license file. If you are not prompted to upload the license file, navigate to **Administration > License Management** from the **Server** tab in the Administration Console.

The License Management window displays.

Step 5 Click **Browse**, then navigate to the license file that you downloaded to your PC.

Step 6 Select the license file and click **Open**.

Step 7 Click **Upload** to upload the license file to the server.

The license manager processes the new license.

Step 8 Click **Apply**.

Cisco IPICS associates the license file with the server and restarts the license manager. The updated license information displays in the License Summary pane in the License Management window.

After you click **Apply**, there may be a delay of a few minutes before you can access the Administration Console.

Step 9 If you have more than one license file, repeat Step 5 through Step 8 until you have uploaded all license files.

Cisco recommends that you click **Apply** after you upload each license file, so that you can more easily track the progress of the upload process.

Note Cisco IPICS does not overwrite older license files with newer license files. You can purchase additional features by obtaining a new license; when you upload and apply the new license, Cisco IPICS adds the new license features to the existing license features.

As a best practice, Cisco recommends that you remove old license file(s) whenever license changes occur (such as when you replace a time-bound license with a permanent license). For information about deleting time-bound licenses, see the "Deleting Older Time-Bound Licenses from the Server" section on page 2-18.

Viewing the License Summary Information

From the **Administration > License Management > Summary** tab in the Administration Console, you can access the License Summary pane to view the licensed features for your system. This pane also displays license information for the Cisco IPICS Base Server License and the Policy Engine Base License.

To understand how Cisco IPICS features use the available licensed features, see the "Tracking Your License Usage" section on page 2-15.

Note The data that displays in the License browser window shows the usage at the time that the license window was last accessed. To view the most current license information, refresh your browser window. Make sure to refresh your browser window often and before you perform any server administration functions to ensure that you are working with the most current information. If you attempt to perform an administration update in a window that does not display the most current data, the update does not succeed, and Cisco IPICS displays an error. If you receive an error, refresh your browser window and retry the operation.

This section includes the following sections:

Tracking Your License Usage

Table 2-1 describes the criteria that Cisco IPICS uses to determine license usage for ports, IDCs, IP phones, the policy engine, and ops views.

Table 2-1 Cisco IPICS License Usage Criteria

Field	Description
Concurrent LMR Ports	An enabled channel or radio uses an LMR port license. After an administrator disables a channel or radio, the server releases the LMR license and makes it available for use. Associating a radio and channel selector combination with a channel does not affect license usage. Cisco IPICS bases license usage for channels on the unique combination of a multicast address and a location. If a channel uses two multicast addresses, the single channel uses two licenses. If an administrator removes one of the multicast addresses, the system releases one of the licenses so that the port now uses one license.
Concurrent Multicast Ports	An activated VTG uses a multicast port license. After an administrator deactivates a VTG, the server releases the multicast license and makes it available for use. Be aware that an inactive VTG uses a license when a policy triggers (activates) that VTG. Therefore, if the number of licenses has been exceeded, the policy is not able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.
Concurrent Cisco Unified IP Phone Users	An IP phone user uses a license each time that a user logs in to Cisco IPICS from an IP phone. If you use all IP phone licenses, additional IP phone users cannot dial into a channel or VTG.
Concurrent Dial Users	The policy engine uses a license each time the dial engine performs a dial-in or dial-out action. If you use all dial user licenses, the dial engine cannot perform additional dial-in or dial-out actions.
Concurrent Dispatch Console Silver Users	The number of concurrent users with silver licenses. An IDC user uses a license each time that the user logs in to an IDC session. If the same IDC user logs in to multiple IDC sessions from different IDC client machines, that user uses multiple licenses (one for each IDC session). **Note** If you use all of the available IDC licenses, Cisco IPICS interrupts IDC user access to the system. Make sure that you are aware of the current status of IDC licenses, and purchase and install additional licenses immediately if you use all of the available IDC licenses.
Concurrent Dispatch Console Platinum Users	The number of concurrent users with platinum licenses. An IDC user uses a license each time that the user logs in to an IDC session. If the same IDC user logs in to multiple IDC sessions from different IDC client machines, that user uses multiple licenses (one for each IDC session). **Note** If you use all of the available IDC licenses, Cisco IPICS interrupts IDC user access to the system. Make sure that you are aware of the current status of IDC licenses, and purchase and install additional licenses immediately if you use all of the available IDC licenses.

Table 2-1 Cisco IPICS License Usage Criteria (continued)

Field	Description
Concurrent Mobile Endpoint Users	The number of concurrent users who are accessing Cisco IPICS from mobile endpoints. **Note** If you use all of the available mobile endpoint licenses, Cisco IPICS interrupts mobile endpoint user access to the system. Make sure that you are aware of the current status of mobile endpoint licenses, and purchase and install additional licenses immediately if you use all of the available mobile endpoint licenses.
Concurrent EndtoEnd P25 Vocoders	The number of end-to-end P25 channels that can be active at any time on the IDC. An IDC user uses a license each time a P25 channel is powered up in end-to-end mode. **Note** The IDC supports a maximum of 4 concurrent connections to end-to-end P25 channels per user session. If a user is logged in from 2 IDC consoles at the same time, only one IDC can join P25 channels in end-to-end mode.
Concurrent Gateway P25 Vocoders	The number of P25 channels that can be concurrently enabled at any time on the Cisco IPICS server. The Cisco IPICS server uses a license each time a P25 channel is enabled on that server.
Concurrent DFSI Gateway Fixed Station Ports	The number of fixed stations that can be configured on the Cisco IPICS server.
Concurrent UMS Servers	The number of UMSs that can be configured and enabled in the Administration Console.
Concurrent ISSI Gateway Servers	The number of ISSI Gateways that can be configured on the Cisco IPICS server.
Concurrent DFSI Gateway Servers	The number of DFSI Gateways that can be configured on the Cisco IPICS server.
Cisco IPICS Ops View	If you have purchased a license that includes additional ops view functionality, each ops view that you create uses one license.
Cisco IPICS Base Server License	License usage does not apply to this field. This field displays whether you have a base license for Cisco IPICS.
Cisco UMS High Availability License	License usage does not apply to this field. This field indicates whether you have a base license for UMS high availability.
Policy Engine Base License	License usage does not apply to this field. This field indicates whether you have a base license for the policy engine.
High Availability License	License usage does not apply to this field. This field indicates whether you have a base license for high availability.

Managing Time-Bound Licenses

Cisco IPICS also includes support for time-bound licenses. Time-bound licenses, such as evaluation or demonstration licenses, differ from purchased (non-time-bound) licenses in that they include a preconfigured license expiration date.

When a time-bound license is about to expire (about 30 days before expiration), Cisco IPICS displays a warning message to alert you of the upcoming expiration.

Note If you install a more recent time-bound license on your server, you may see this warning message if additional unexpired time-bound licenses are installed and you have not dismissed this warning. To suppress this warning message, delete the older, unexpired licenses that are installed on your server. For more information, see the "Deleting Older Time-Bound Licenses from the Server" section on page 2-18.

- When a license feature expires, the relevant functionality of that license becomes disabled.
- After your license expires, it remains valid for a maximum of 24 hours after the expiration date. (The server checks for expired licenses every 24 hours.)
- After you install the Cisco IPICS server software, Cisco IPICS invalidates time-bound licenses when you change the system date to a date that is before the license start date. Invalid licenses cause the Cisco IPICS system to become inoperable.

Note You must restart the license manager, or reboot the server, for system date changes to become effective.

To restart the license manager and revalidate the license(s), perform the following procedure:

Procedure

Step 1 Open a terminal window and log in using the root user ID.

Step 2 Restart the license manager by entering the following command:

[root]# **service ipics_lm restart**

Step 3 To revalidate the license(s), navigate to **Administration > License Management**; then, click **Apply** to restart the license server.

Deleting Older Time-Bound Licenses from the Server

If you receive license expiration warning messages, and you have more than one unexpired time-bound license installed, you must delete the older time-bound licenses to suppress this warning message. To delete time-bound licenses, perform the following procedure:

Procedure

Step 1 From the Administration drawer in the Administration Console, click **License Management**.

Step 2 Click the **Installed License Files** tab.

Step 3 Check the check box to the left of the license file name to delete, then click **Delete**.

Managing Server Certificates

This section describes how to perform the following server certificate tasks:

- Backing Up Server Certificates and Stores, page 2-19
- Customizing and Generating a Self-Signed Server Certificate, page 2-20
- Installing Third Party Certificates on the Cisco IPICS Server, page 2-21

To perform the tasks in this section, make sure that the following tools are available:

- A Secure Shell (SSH) client, such as
  - SSH Tectia Client
  - Putty SSH
  - Cygwin ssh
- A Secure Copy (SCP) and/or Secure File Transfer Protocol (SFTP) client, such as
  - Putty pscp
  - Putty sftp
  - Cygwin scp
  - Cygwin sftp
  - WinSCP

Backing Up Server Certificates and Stores

Before generating and installing a server certificate, back up existing certificate files by performing the following steps:

Procedure

Step 1 Access the Cisco IPICS server via an SSH client and log in as the Linux root user.

Step 2 Change to the security directory and create a backup directory:

[root]# **cd /opt/cisco/ipics/security/**

[root]# **mkdir backup**

Step 3 Create a backup copy of the server.truststore.jks file, which includes all of the trusted certificates for the server.

[root@ipics-server]# **cp -a server.truststore.jks backup/**

Step 4 Create a backup copy of the server.keystore.p12 file, which contains the server private key:

[root@ipics-server]# **cp -a server.keystore.p12 backup/**

Step 5 Create backup copies of the certificate files:

[root@ipics-server]# **cp -a *.pem backup/**

Step 6 Create a backup copy of security properties files:

[root@ipics-server]# **cp -a security.properties backup/**

Customizing and Generating a Self-Signed Server Certificate

Because Cisco IPICS services are disrupted during generation and customization of a self-signed server certificate, Cisco recommends that you perform the following procedure during a maintenance window. Before doing so, back up any existing certificate files as described in the "Backing Up Server Certificates and Stores" section on page 2-19.

To generate and customize a self-signed server certificate, perform the following steps:

Step 1 Access the Cisco IPICS server via an SSH client and log in as the Linux root user.

Step 2 Change to the security directory:

[root]# **cd /opt/cisco/ipics/security/**

Step 3 If you plan to use a third party security certificate, customize the security properties for your company by editing the security.properties file and changing the parameters listed in Table 2-2.

Note the following:

- The information that you enter may vary according to the CA that you use. For example, for the name of your state or province [x500StateName], VeriSign requires that you spell out the complete name rather than using the abbreviated form.
- The system requires that you use the same value for the private key password and the keystore password. If you enter different passwords, the Tomcat server cannot successfully restart. (When these passwords are the same, the system does not prompt you again for the key password.)
- If you change the passwords in the security.properties file, also update the password in the Tomcat server.xml file in /opt/cisco/ipics/tomcat/current/conf.

Table 2-2 Customizing Security Properties

Entry	Description
certValidity=1095	The number of days the certificate is valid.
keySize=2048	Key size, in bits. Sometimes referred to as encryption strength.
keystorePassword=changeit	Password for the key store (default is **changeit**).
privateKeyPassword=changeit	Password for the private key.
truststorePassword=changeit	Password for the trust store.
x500OrginizationName=Cisco Systems, Inc.	Your company name.
x500OrginizationalUnit=PSBU	You company division.
x500LocalityName=San Jose	Your city.
x500StateName=California	Your state or province.
x500Country=US	Your country (2 letter ISO code)
x500Email=admin@ipics.cisco.com	Your e-mail address.

Step 4 Stop all IPICS services:

[root@ipics-server]# **service ipics stop-all**

Step 5 Remove the existing certificate

[root@ipics-server]# **sudo -H -u ipicsadmin ./security-manager unsetup**

Step 6 Generate a new set of self-signed certificates using the properties that you defined in Step 3.

[root@ipics-server]# **sudo -H -u ipicsadmin ./security-manager setup**

This command creates the following certificates:

ca.cert.pem	Local self-signed CA certificate)
server.cert.pem	Server certificate, signed by the local CA
server.csr.pem	Certificate signing request (CSR)

Step 7 Start all IPICS services:

[root@ipics-server]# **service ipics start-all**

Because the **security-manger** script shown in Step 6 does not restart all of the essential high availability processes, you must start all IPICS services to ensure system stability.

Installing Third Party Certificates on the Cisco IPICS Server

The Cisco IPICS server ships with a self-signed certificate. However, you may replace this certificate with a customer-specific, third party certificate that has been issued by a CA. A CA, as a trusted third party, issues and manages digital certificates that provide enhanced security by verifying the credentials of the user, organization, server, or other entity as specified in the certificate. VeriSign, Thawte, and Entrust are examples of CAs.

The following sections include information about requesting a third party certificate and installing the certificate on the Cisco IPICS server:

- Requesting a Third Party Certificate, page 2-21
- Installing a Third Party Certificate, page 2-22
- Converting DER Formatted Certificates to PEM Format, page 2-24

For related information, including a method for obtaining and installing third party certificates from the Cisco IPICS Administration Console, see the "Managing Trust Between Servers" section in *Cisco IPICS Server Administration Guide*.

Requesting a Third Party Certificate

Because Cisco IPICS services are disrupted, Cisco recommends that you perform the following procedure during a maintenance window. Before doing so, back up any existing certificate files as described in the "Backing Up Server Certificates and Stores" section on page 2-19.

To request a third party certificate, perform the following steps:

Procedure

Step 1 Follow Step 1 - Step 6 in the "Installing Third Party Certificates on the Cisco IPICS Server" section on page 2-21. Do not start the IPICS services, as described in step Step 7.

Step 2 Stop all IPICS services (in the event that any are running):

[root]# **service ipics stop-all**

Depending on the Certificate Authority that you use, you may need to copy and paste the contents of the server.csr.pem file into your browser, or you may need to upload the CSR file to request the certificate.

Step 3 To the paste text into a browser:

a. List the file contents:

[root]# **cat server.csr.pem**

b. Paste CSR text into the CA web page.

Step 4 If the CA does not accept the certificate request, make the requested modifications and then repeat this procedure.

When you receive the certificate from the CA, follow the procedure in "Installing a Third Party Certificate" section on page 2-22 to install the certificate.

Installing a Third Party Certificate

Because Cisco IPICS services are disrupted when installing a third party certificate, Cisco recommends that you perform the following procedure during a maintenance window. Before doing so, back up any existing certificate files as described in the "Backing Up Server Certificates and Stores" section on page 2-19.

To install a third party certificate on the server, perform the following procedure:

Procedure

Step 1 Depending on the format in which you receive the certificate, take one of the following actions:

- If you receive the certificate file directly from the CA, rename the file to **signed_server.cert.pem**.
- If you receive the certificate enclosed in an e-mail, create a new file named **signed_server.cert.pem** (this file must contain only the certificate contents of the e-mail).

CAs may use different procedures to send root CA certificates. Some CAs embed the root CA certificate into the certificate that they provide to you; other CAs provide the root CA certificate separately. (The root CA certificate allows you to establish a chain of trust from the CA to the third party certificate on your server.)

Step 2 Depending on the format in which the CA provides the root CA certificate, take one of the following optional actions:

- If you download the root CA certificate file directly from the CA website, rename the file to **root_ca.cert.pem**.
- If the CA provides the root CA certificate enclosed in a web page, create a new file named **root_ca.cert.pem** (the file must contain only the root CA certificate contents of the web page).

Step 3 (If applicable) Some CAs also provide an intermediate CA certificate. If so, then take one of the following actions:

- If you download the intermediate CA certificate file directly from the Certificate Authority website, rename the file to **intermediate_ca.cert.pem**.
- If the CA provides the intermediate CA certificate enclosed in a web page, create a new file named **intermediate_ca.cert.pem** (the file must contain only the intermediate CA certificate contents of the web page).

Step 4 Verify that the certificates are in text (PEM) format by opening the certificate files using a text editor, and making sure that this text appears inside the certificate files:

```
-----BEGIN CERTIFICATE-----
```

If this text does not appear, follow the steps in "Converting DER Formatted Certificates to PEM Format" section on page 2-24 before continuing.

In addition, follow these guidelines for each certificate file:

- Use a basic text editor, such as Notepad or vi, to edit the certificate file. Do not use Microsoft Word because it may save the file with extra characters in it.
- The file must end with `-----END CERTIFICATE-----` followed by a blank line.
- There should only be one `-----BEGIN CERTIFICATE-----` line and one `-----END CERTIFICATE-----` line per certificate file (until you concatenate the files as described later in this procedure).
- If your certificate file contains more than one certificate, use the **chopcert** command to convert it into the necessary individual certificate files:

  [root@ipics-server]# **cd /opt/cisco/ipics/security/**

  [root@ipics-server]# **./chopcert certchain.pem**
- Some CAs offer *wildcard* certificates that work for any machine in a domain. These certificates can be used with Cisco IPICS.

Step 5 Upload all of the certificate files from the local workstation to the IPICS server:

C:\ **scp *.pem root@<ipics-server-ip-addr>:/root/**

Note The contents of the /root directory on the IPICS server are unchanged and are therefore not affected by future upgrades to the system.

Step 6 Access the Cisco IPICS server via an SSH client and log in as the Linux root user.

Step 7 Change to the security directory:

[root@ipics-server]# **cd /opt/cisco/ipics/security/**

Step 8 Copy the certificate files to the security directory and set the correct file permissions:

[root@ipics-server]# **cp /root/*.pem /opt/cisco/ipics/security/**

Step 9 Take either of these actions:

- If your CA provided three certificate files, enter this command:

  [root@ipics-server]# **./install3rdpartycerts -3**
- If your CA provided four certificate files, enter this command:

  [root@ipics-server]# **./install3rdpartycerts -4**

Converting DER Formatted Certificates to PEM Format

To convert DER formatted certificates to PEM format, perform the following steps:

Procedure

Step 1 Access the Cisco IPICS server via an SSH client and log in as the Linux root user.

Step 2 Use openssl to convert a certificate from PEM to DER format:

```
[root@ipics-server]# openssl x509 \
 -in cert.der -inform DER \
 -out cert.pem -outform PEM
```

Modifying Network Settings

You can modify network settings for the IPICS server from the command line on the IPICS server. To do so, use the network config tool, not the standard Linux tool.

To modify network settings, follow these steps:

Procedure

Step 1 Access the Cisco IPICS server via an SSH client and log in as the Linux root user.

Step 2 Access the network configuration utility:

```
[root]# network_config
```

Step 3 Enter the number of the option you want to change, and follow the on-screen instructions.

Step 4 When you are finished making changes, use the alphabetic commands to apply the configuration to the IPICS server or save the configuration to a file.

You can also use the numeric commands to import a previously saved configuration, or reset the current server configuration to the last saved version.

Step 5 Enter **q** to close the configuration utility.