Getting Started with Cisco Instant Connect Express, Release 4.9(1)

March 30, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Introduction

This guide provides you with the information that you need to install and administer Cisco Instant Connect Express.

Organization

This document is organized as follows:

Chapter 1, “Overview”	Provides an overview of Cisco Instant Connect Express and its components
Chapter 2, “Installing Cisco Instant Connect Express”	Describes how to install and set up Cisco Instant Connect Express, and provides related information
Chapter 2, “Cisco Instant Connect Administration”	Describes how to administer and manage Cisco Instant Connect Express

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which is available at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Overview

This chapter provides an overview of Cisco Instant Connect Express and the components that can be part of a deployment.

This chapter includes the following topics:

Introduction to Cisco Instant Connect Express

Cisco Instant Connect Express is a mobile push-to-talk (PTT) solution based on the Cisco IP Interoperability and Collaboration System (IPICS). The system enables users of Cisco Instant Connect for Android Devices to communicate with each other by using their Android devices. Cisco Instant Connect Express supports up to 50 concurrent mobile users and up to 15 concurrent talklines, and is preconfigured with 4 users, 4 talk lines, and a multicast pool. The system provides a subset of the features and functionality of Cisco IPICS and can be upgraded to Cisco IPICS at any time.

A Cisco Instant Connect Express deployment includes various hardware and software components, including some or all of the following:

- Cisco Instant Connect Express server—A deployment includes a Cisco Instant Connect Express server, which is the center of all Cisco Instant Connect Express activity. The Cisco Instant Connect Express server software runs on the Cisco Linux operating system. and performs the following functions:
  - Hosts the Administration Console, which gives you control over operation and administration of Cisco Instant Connect Express
  - Provides Cisco Instant Connect Express authentication and security services
  - Stores data that is required for operation
  - Enables integration with various media resources
- Unified media service (UMS)—Provides media connectivity for mobile users to join and communicate on associated talklines.
- Networking components—May include switches, routers, firewalls, mobile access routers, and wireless access points and bridges.
- Cisco Instant Connect—An application for Android devices that allows users to use these devices to interact with other participants Cisco Instant Connect Express talkline.

Cisco IPICS and Cisco Instant Connect Express Feature Comparison

Table 1-1 compares major features and functionality of Cisco IPICS and Cisco Instant Connect Express.

Table 1-1 Cisco IPICS and Cisco Instant Connect Express Features

Feature	Cisco IPICS	Cisco Instant Connect Express
Channels	Supported	Not supported
Cisco Instant Connect MIDlet	Supported	Not supported
Cisco Unified IP Phones	Supported	Not supported
DFSI gateway	Supported	Not supported
Dial engine	Supported	Not supported
Dial in users	Supported	Not supported
High availability	Supported	Not supported
Incident Dispatch Console	Supported	Not supported
Incident VTGs	Supported	Not supported
ISSI gateway	Supported	Not supported
LDAP integration	Supported	Not supported
Locations	Supported	Not supported
Mobile users	Unlimited number supported	Up to 50 supported concurrently
Ops views	Supported	Not supported
Policy engine	Supported	Not supported
Radios	Supported	Not supported
Reporter	Supported	Not supported
RMS	Supported	Not supported
User groups	Supported	Not supported
VTGs	Supported	Up to 15 talklines are supported for communication concurrently

Installing Cisco Instant Connect Express

This chapter describes how to install and set up Cisco Instant Connect Express, and provides related information.

This chapter includes the following sections:

Installing the Cisco Instant Connect Express Server Software

The following sections describe how to install the Cisco Instant Connect Server Software and how to perform related procedures:

Installation Guidelines

The following guidelines apply to a Cisco Instant Connect Express installation:

- To facilitate communications between your users, your Cisco Instant Connect Express system requires a pool of IP addresses that can be reached by all users in your network domain.
- The Cisco Instant Connect Express server requires a static, local IP address that is advertised on the network. Cisco Instant Connect Express end points must have the static address of the Cisco Instant Connect Express server to maintain communications.
- Obtained the Media Access Control (MAC) address for the eth0 interface of the Cisco Instant Connect Express server. Cisco Instant Connect Express uses the MAC address of the server to validate the Cisco Instant Connect Express license.

- Obtain the static local IP address, subnet mask, default gateway, and DNS server (optional) information for the Cisco Instant Connect Express server.

  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, after you install Cisco Instant Connect Express, access the Cisco Instant Connect Express 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 Instant Connect Express always uses the eth0 MAC address to validate the license, even if eth0 is disabled.
- You can install a third party certificate to replace the Cisco Instant Connect Express self-signed certificate. For more information about installing third party certificates, see the "Installing Third Party Certificates on the Cisco Instant Connect Express Server" section on page 2-17. A third-party certificate is not required for use with Cisco Instant Connect Express.
- If your network uses the Network Time Protocol (NTP), obtain the IP address or DNS name of the NTP server.
- Cisco strongly recommends that you attach an uninterruptible power supply (UPS) to your system and ensure that the UPS is operating correctly.

Deploying the VM

The following sections describe how to configure a virtual machine (VM) for Cisco Instant Connect Express. You install and operate the Cisco Instant Connect Express application and the UMS on a VM. Each component must run in its own VM.

This chapter includes the following sections:

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 Instant Connect Express Operating System

This section describes how to obtain and deploy the VM OVA image for Cisco Instant Connect Express. This process installs the Cisco Instant Connect Express 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 Instant Connect Express 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

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 Instant Connect Express server. Cisco Instant Connect Express 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 Instant Connect Express server as the root user and change it by using the **reset_pw** command.

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 six 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.

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 install a time-bound license for your system, use caution when enabling NTP. Adjustments to the system date can cause Cisco Instant Connect Express to invalidate your license. For more information, see the "Managing Time-Bound Licenses" section on page 2-13.

  Cisco recommends that NTP be used.

- 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 Instant Connect Express displays the following text, where *hostname* represents the host name that you specified in Step 16:

```
Cisco IPICS
hostname login:
```

You can now install the Cisco Instant Connect Express server software and the UMS in the VM.

Installing the Cisco Instant Connect Express Server Software

After you successfully deploy the VM OVA Image for the Cisco Instant Connect Express Operating System, you can install the Cisco Instant Connect Express server software.

The Cisco Instant Connect Express 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 Instant Connect Express server software
- Upgrade—This option upgrades your server from a previous version of Cisco Instant Connect Express

You must log in as the Linux root user to perform the Cisco Instant Connect Express 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 Instant Connect Express server software, follow these steps on the server on which you deployed the VM:

Procedure

Step 1 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 Instant Connect Express begins the installation process. After a short time, you see a Welcome message.

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

A message informs 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 Instant Connect Express Administration Console.

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

Cisco Instant Connect Express requires that you use strong passwords that include the following elements:

- Minimum of eight 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 Instant Connect Express application-related folders, files, and scripts. The informix linux group includes full permission to the Cisco Instant Connect Express 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 Instant Connect Express 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 Instant Connect Express requires that you use strong passwords that include the following elements:

- Minimum of eight 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 Instant Connect Express 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 Instant Connect Express server becomes available.

Note If you enter **no**, complete the restart before you attempt to log in to Cisco Instant Connect Express. Cisco Instant Connect Express 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 2-7.

Restarting or Shutting Down the Server

To restart the server, follow these steps:

Caution When you shut down or restart your server, some functionality is affected and endpoints may get disconnected. In addition, Cisco Instant Connect Express logs out all users who are logged in to the Administration Console.

Procedure

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

- To log in to the server from the server console:
  a. Log in to the Cisco Instant Connect Express 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:
  a. Access the Cisco Instant Connect Express 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 appears.

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

[root]# **reboot**

The server reboots.

Cisco recommends that you gracefully shut down the Cisco Instant Connect Express server by performing the following procedure instead of pressing the power button to shut down the server. To shut down the server, follow these steps:

Procedure

Step 1 Log in to the Cisco Instant Connect Express server with the root user ID.

A terminal window appears.

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

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

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
- **now** causes the running processes to shut down immediately

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 Instant Connect Express

After you complete the software installation, you must perform the following tasks before you can use Cisco Instant Connect Express:

- Checking the Installation, page 2-8
- Managing Your Licenses and Certificates, page 2-9
- Viewing the License Summary Information, page 2-12

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

Checking the Installation

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

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

To access the Cisco Instant Connect Express Administration Console and check the installation, follow these steps:

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 Instant Connect Express server:

https://*server*

Because your browser does not trust the Cisco Instant Connect Express server self-signed SSL certificate, a Security Alert window appears. You can suppress this window by using a third-party certificate or by adding the Cisco Instant Connect Express 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 appears 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 2-9.

Managing Your Licenses and Certificates

After you install Cisco Instant Connect Express, 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 Instant Connect Express product package to obtain a license file.

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

- Concurrent Talkline Ports
- Concurrent Mobile Endpoint Users
- Concurrent UMS Server
- Cisco IPICS Base Server 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

Your Cisco Instant Connect Express 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 Instant Connect Express installation.

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

To use your PAK to obtain your Cisco Instant Connect Express licenses, follow these steps:

Procedure

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

Note If you ordered your Cisco Instant Connect Express server software directly from Cisco, your package may include only one PAK. However, if you purchased Cisco Instant Connect Express 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 before you began the installation procedure.

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 Instant Connect Express 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 Instant Connect Express 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 appears.

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 Instant Connect Express 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 Instant Connect Express license.

See the "Uploading the Cisco Instant Connect Express License Files" section on page 2-11 for instructions about uploading the Cisco Instant Connect Express 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 Instant Connect Express License Files

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

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

To upload license files, follow these steps:

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 Instant Connect Express server:

https://*server*

Because your browser does not trust the Cisco Instant Connect Express server self-signed SSL certificate, a Security Alert window appears. You can suppress this window by using a third-party certificate or by adding the Cisco Instant Connect Express 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 Instant Connect Express Login window appears.

Step 4 Log in to the Cisco Instant Connect Express 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 appears.

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 Instant Connect Express 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 Instant Connect Express 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 Instant Connect Express 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, see the "Deleting Older Time-Bound Licenses from the Server" section on page 2-14.

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.

To understand how Cisco Instant Connect Express features use the available licensed features, see the "Tracking Your License Usage" section on page 2-12.

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 Instant Connect Express 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 Instant Connect Express uses to determine license usage.

Table 2-1 Cisco Instant Connect Express License Usage Criteria

Field	Description
Concurrent Talkline Ports	An activated talkline uses a talkline port license. After an administrator deactivates a talkline, the server releases the license and makes it available for use.
Concurrent Mobile Endpoint Users	The number of concurrent users who are accessing Cisco Instant Connect Express from mobile endpoints. **Note** If you use all of the available mobile endpoint licenses, Cisco Instant Connect Express 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 UMS Servers	The number of UMSs that can be configured and enabled in the Administration Console.
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	Not used for Cisco Instant Connect Express.
Policy Engine Base License	Not used for Cisco Instant Connect Express.
High Availability License	Not used for Cisco Instant Connect Express.

Managing Time-Bound Licenses

Cisco Instant Connect Express 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 Instant Connect Express 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 information, see the "Deleting Older Time-Bound Licenses from the Server" section on page 2-14

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 Instant Connect Express server software, Cisco Instant Connect Express 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 Instant Connect Express system to become inoperable.

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 licenses, follow these steps:

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

Step 2 Navigate to the directory where Cisco IPICS stores the license files by entering the following command:

[root]# **cd /opt/cisco/ipics/tomcat/current/webapps/license**

Step 3 View the license files by entering the following command:

[root]# **ls -l *.lic**

The license files display with the time and date that the license was last modified.

Step 4 Make a note of the licenses that you no longer need.

The time and date that displays with the file information might assist you with determining which files you need to delete.

Step 5 Delete the unnecessary license files by entering the following command, where *licensefilename*.lic is the name of the license file that you want to delete:

[root]# **rm** *licensefilename***.lic**

Caution Make sure that you do not delete the cisco.opt file. This file is required for the correct operation of Cisco IPICS.

Step 6 Repeat Step 5 for each license file that you need to delete.

Step 7 Restart the server by entering the following command:

[root]# **service ipics restart**

Step 8 Log in to the Administration Console by using the ipics user ID and navigate to the **Administration > License Management** window.

Step 9 To apply the license deletions to the system configuration, click **Apply**.

Step 10 If a message displays that indicates that a license is about to expire, click **Dismiss Warnings**.

Managing Server Certificates

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

- Backing Up Server Certificates and Stores, page 2-15
- Customizing and Generating a Self-Signed Server Certificate, page 2-16
- Installing Third Party Certificates on the Cisco Instant Connect Express Server, page 2-17

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 Instant Connect Express 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 Instant Connect Express 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 2-15.

To generate and customize a self-signed server certificate, follow these steps:

Procedure

Step 1 Access the Cisco Instant Connect Express 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 Instant Connect Express 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 Instant Connect Express services:

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

Installing Third Party Certificates on the Cisco Instant Connect Express Server

The Cisco Instant Connect Express 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 Instant Connect Express server:

- Requesting a Third Party Certificate, page 2-17
- Installing a Third Party Certificate, page 2-18
- Converting DER Formatted Certificates to PEM Format, page 2-20

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

Requesting a Third Party Certificate

Because Cisco Instant Connect Express 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 2-15.

To request a third party certificate, follow these steps:

Procedure

Step 1 Follow Step 1 - Step 6 in the “Installing Third Party Certificates on the Cisco Instant Connect Express Server” section on page 2-17. Do not start the Instant Connect Express services, as described in step Step 7.

Step 2 Stop all Instant Connect Express 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 2-18 to install the certificate.

Installing a Third Party Certificate

Because Cisco Instant Connect Express 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 2-15.

To install a third party certificate on the server, follow these steps:

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).

If the CA provides more than one intermediate CA certificate, give each additional certificate a unique name, such as **intermediateroot_ca1.cert.pem**, **intermediateroot_ca2.cert.pem**, and so on.

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 2-20 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 Instant Connect Express.

Step 5 Upload all of the certificate files from the local workstation to the Instant Connect Express server:

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

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

Step 6 Access the Cisco Instant Connect Express 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 three 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, follow these steps:

Procedure

Step 1 Access the Cisco Instant Connect Express 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 Instant Connect Express server from the command line on the Instant Connect Express 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 Instant Connect Express 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 Instant Connect Express 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.

Installing the UMS

The Universal Media Services (UMS) is a media services platform for Cisco IPICS and its endpoints. The UMS provides a variety of media hosting, streaming, mixing, transcoding, talker ID, and processing functions.

The UMS installs and operates in a dedicated VM. For a list of supported VMs, see *Cisco IPICS Compatibility Matrix*.

Before You Begin

Deploy the VM OVA image for Cisco IPICS as described in the "Obtaining and Deploying the VM OVA Image for the Cisco Instant Connect Express Operating System" section on page 2-2. In Step 1c of this procedure in that section, make sure to download the ums-4.9.1-2cpu.ova file. After you deploy the VM OVA for your environment, you are ready to install the UMS software on the server.

To install the UMS software, follow these steps:

Procedure

Step 1 Log in as the root user to the VM that you deployed for the UMS if you are not logged in already and enter the following commands, where *installerfilename*.bin specifies the name of the installer file:

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

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

After a short time, you see a Welcome message.

Step 2 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.

Step 3 When you are prompted to continue, type **y** then press **Enter**.

Step 4 When you are prompted for a Cisco IPICS administrator password, enter a administrative password to be used for services on this server, then press **Enter**.

The password must follow these guidelines:

- Must contain at least 8 characters
- Cannot contain any variation of cisco or ocsic (for example, abCiSCo12 is not valid)
- Cannot contain three or more same consecutive characters (for example, a password that contains AAA or 888 is not valid)
- Must contain at least one uppercase letter, one lowercase letter, one number, and one special character (special characters include !, @, and #)

Step 5 Reenter the Cisco IPICS administrator password when you are prompted to do so, then press **Enter**.

Step 6 When you see the "Password accepted" message, press **Enter**.

Step 7 When you are prompted to continue, type **y** then press **Enter**.

The UMS software installs on the server.

Step 8 When you are prompted whether you want to reboot the server, type **y** then press **Enter**.

The server reboots and the installation is complete.

To configure the UMS, see *Cisco IPICS Administration Guide*.

Cisco Instant Connect Administration

This chapter describes how to administer and manage Cisco Instant Connect Express.

This chapter includes the following topics:

Cisco Instant Connect Express Roles

Cisco Instant Connect Express roles are granted to each user to define the features that the user can access and the operations that the user can perform. In this way, roles help to provide system security.

Table 2-1 describes the Cisco Instant Connect Express roles. By default, every Cisco Instant Connect Express user is configured with the User role and the Dispatcher role. You can modify role assignments as needed.

Table 2-1 Cisco Instant Connect Express Roles

Role	Description
User	Has the ability to maintain personal information, specify communication preferences that are used to configure audio devices,
System administrator	Responsible for installing and setting up Cisco Instant Connect Express resources. Also manages Cisco Instant Connect Express licenses, and monitors the status of the system and its users via the activity log files and the Dashboard.
Operator	Responsible for setting up and managing users, granting access to Cisco Instant Connect Express and assigning roles.
Dispatcher	Responsible for setting up inactive talklines, activating talklines to begin conferences, and adding or removing participants in talklines Also monitors active talklines and can mute and unmute users as necessary.
All	Equivalent to being assigned each of the other Cisco Instant Connect Express roles.

Cisco Instant Connect Express also supports various Linux user roles. For detailed information about these roles, see the "Linux User Roles" section in *Cisco IPCIS Server Administration Guide*."

Cisco Instant Connect Express Administration Console

The Cisco Instant Connect Express Administration Console is a web-based application that you use to perform and manage Cisco Instant Connect Express activities.

This section includes the following topics:

Accessing the Administration Console

After you install Cisco Instant Connect Express, you can access the Administration Console from any computer that has IP connectivity to the Cisco Instant Connect Express server and meets the requirements that *Cisco IPICS Compatibility Matrix* specifies.

To access the Administration Console, perform the following procedure:

Procedure

Step 1 Start Internet Explorer, and in the Address field, enter the fully qualified hostname **o**r the IP address of the server on which Cisco Instant Connect Express is running.

A fully qualified hostname (for example, express001.cisco.com) is preferred. If you enter an IP address and the PC that you are using does not have a valid trust certificate from the server, a pop-up window prompts you to download a certificate. Follow the prompts to do so.

A hostname is not case-sensitive.

The Authentication window appears.

Step 2 Enter your user name in the User Name field.

User names are not case-sensitive.

Step 3 Enter your password in the Password field.

Passwords are case-sensitive, so make sure to enter your password exactly as it is configured.

Step 4 Click **Log In**.

The Administration Console appears. The My Profile window appears on the right. The left pane in this window shows the available drawers in the Administration Console. The drawers that appear for you correspond to your roles, so you may not see all drawers in your window.

Exiting the Administration Console

You can exit the Administration Console from any window within the application. To do so, click **Logout** at the top right of any Administration Console window.

Administration Console Usage Guidelines

Be aware of the following guidelines when you use the Cisco Instant Connect Express Administration Console:

- The Server tab at the left of the Administration Console window provides access to drawers and windows in which you perform Cisco Instant Connect Express administration and management activities. These activities include configuring and managing Cisco Instant Connect Express components, uploading licenses, managing the database, monitoring activity logs, setting system performance options, and monitoring system performance.
- Many Administration Console window let you enter a variety of information. You might enter information by typing in fields, choosing from drop-down lists, or checking check boxes, depending on the window. An red asterisk (*) next to a field, drop-down list, or check box indicates required information. You must provide this information before you can save your changes and exit the window.
- Most windows contain a **Save** button and a **Cancel** button. The **Save** button saves any changes that you make in a window and may close the window. The **Cancel** button discards any changes that you have made and may close the window.
- Many Cisco Instant Connect Express resources, such as users talklines, display in lists in the Administration Console. These lists include check boxes that you can check to select resources for which to perform certain functions. Most resource lists include a check box at the top of the list that allows you to select all resources at one time.
- Many Administration Console windows include drop-down lists. Some of these lists become available only after you perform certain functions. If you do not perform the required function, the drop-down list is dimmed to indicate that it is not available.
- For some resources, separate windows display in which you can take the following actions:
  - To move an item from one list to another list, click the item to highlight it and then click **>** or **<**, or double-click the item.
  - To move several items from one list to another list at one time, Shift+click or Ctrl+click to select the items and then click **>** or **<**.
  - To move all items from one list to another list at one time, click **>>** or **<<**.
- Windows in the Administration Console do not refresh automatically. To ensure that a current window displays the most up-to-date information, refresh it by clicking the link or tab that you used to display it. Alternatively, some windows provide a **Refresh** button, which you can use to refresh the window. Cisco Instant Connect Express does not support the use of the browser **Refresh** button to refresh a window in the Administration Console.

As a best practice, refresh windows 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 update in a window that does not display the most current data, the update may not succeed and Cisco Instant Connect Express may display an error. If this situation occurs, update your browser window and retry the operation.

- For increased system security, the Administration Console times out after 30 minutes of no use. In this situation, the current Administration Console window remains displayed, but Cisco Instant Connect Express prompts you to log back in when you attempt to perform a function. To log back in, enter your user name and password, and then click **Log In**. To exit the Administration Console, click **Logout** in any Administration Console window.

  To change the timeout period of your Cisco Instant Connect Express session, navigate to **Administration > Options** in the Administration Console and modify the value of the **Cisco IPICS Session Timeout Period** option.
- The Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.
- Cisco Instant Connect Express does not support accessing the Administration Console in more than one browser session at the same time on the same machine. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.
- To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Administration Console.
- All all time stamps that appear in the Administration Console web interface in Greenwich Mean Time (GMT).

Using Search Windows

Several activities that you perform in the Administration Console require you to locate or to identify items that the activities affect. To let you locate the items that you need, Cisco Instant Connect Express provides a Search or a Search Results window. This window pops-up automatically when needed. It provides one or more fields that let you search for the item or items that you want based on a variety of criteria.

The following guidelines apply to Search or Search Results windows:

- These windows may contain one of more filter fields in which you can type characters. The names of these fields depend on the activity that you are performing and the information that you need to find.

  In a filter field, you can enter a character string that includes the first few characters of the name that you want to find. Characters are not case-sensitive.
- The windows may contain one or more filter drop-down lists. These lists depend on the activity that you are performing and the information that you need to find.

  From a filter drop-down list, you can choose the option that matches the item that you want to find. For example, if you are searching for a user and choose **Dispatcher** from a Roles drop-down list, Cisco Instant Connect Express finds users who are assigned the Dispatcher role.
- If you enter information in more than one filter field, Cisco Instant Connect Express finds only items that match all search criteria that you specify.

- To perform a search based on filters that you specify, click **Go** in the Filter area of a Search or a Search Results window. If you click **Go** without specifying any filters, Cisco Instant Connect Express locates all items of the type that you are searching for.
- To clear fields and reset drop-down lists to their default values, click **Clear Filter** in the Filter area of a Search or a Search Results window.
- The results of a search, except a search for locations, depend on the ops view to which you belong. Search for results for locations include all locations that match the search criteria, regardless of your ops view.
- Some search results depend on items that you can choose from the results list. For example, if you search for channels to associate with a user, the results do not include channels that disallow associations to users. Similarly, if you search for channels to add to a VTG, the results do not include channels that disallow associations to VTGs.
- To view the results in a results list at the bottom of a Search or a Search Results window, see the "Navigating Item Lists" section on page 2-5.
- To choose one or more items that display in the results list in a Search or a Search Results window, check the check box next to each item.
- To exit a Search or a Search Results window, take one of these actions:
  - Click the **OK** button—The window closes and then results that you checked are entered in the window that you return to.
  - Click the **Cancel** button—The window closes and the results that you checked are not in the window that you return to.

Navigating Item Lists

Several windows in the Administration Console may display lists of information. For example, the Users window in the User Management drawer displays a list of Cisco Instant Connect Express users.

To view items in these lists, follow these guidelines:

- Lists are divided into *pages* of information. To specify how many rows of items are included in a page, choose the desired value from the Rows per page drop-down list at the top of the window, and then click the **Go** button next that list. You may need to use the scroll bar next to the result list to see all items in a page.
- You can navigate pages of information in a list by using the following navigation controls at the bottom of the list:
  - Page field—To go to a specific page, enter the page number and press **Enter**.
  - |< (First Page button)—Displays the first page in the list. This button is not available when the first page is displayed.
  - < (Previous Page button)—Displays the previous page in the list. This button is not available when the first page is displayed.
  - > (Next Page button)—Displays the next page in the list. This button is not available when the last page is displayed.
  - >| (Last Page button)—Displays the last page in the list. This button is not available when the last page is displayed.

Getting Help

You can access the Cisco Instant Connect Express help system from any window in the Administration Console. The help system provides online access to the information that is in this *Cisco IPICS Server Administration Guide*.

To access Cisco Instant Connect Express online help, click **Help** in any Administration Console window.

Viewing Information about Cisco Instant Connect Express

To view the following information about Cisco Instant Connect Express, click **About** in any Administration Console window:

- Cisco Instant Connect Express version that is running
- Ops view to which the logged-in user is accessible
- Current server date and time
- Server operating system (this information appears only if you are assigned the Cisco Instant Connect Express system administrator role)
- Date and time of the most recent database backup (this information appears only if you are assigned the Cisco Instant Connect Express system administrator role)

Administration Console Windows

The Administration Console windows contain options that you can use to configure, manage, and monitor Cisco Instant Connect Express. Table 2-2 provides an overview of these windows and references to documentation that provides detailed information about the options in each window.

Note If you refer to *Cisco IPCIS Server Administration Guide* for additional information, make sure to use the version of that document that corresponds to your version of Cisco Instant Connect Express.

Table 2-2 Administration Console Windows

Window	Description	Reference
Home Drawer		
My Profile	Your user profile, also referred to as My Profile, includes your name, password, default location, communications preferences, optional address information, client device permissions, and communications preferences. Your user profile was initially set up by a Cisco Instant Connect Express operator or administrator. You can change information, as needed.	See the "Managing Your User Profile" section in *Cisco IPCIS Server Administration Guide*."

Table 2-2 Administration Console Windows (continued)

Window	Description	Reference
My Associations	Displays the Cisco Instant Connect Express resources with which you have been associated.	See the "Managing User Associations" section in *Cisco IPCIS Server Administration Guide*."
TalkLine Management Drawer		
TalkLines	Provides information about each talkline in Cisco Instant Connect Express, and lets you add, delete, and manage talklines and their operations.	See the "Managing Talklines" section on page 2-12
User Management Drawer		
Users	Lets you add, delete, and manage Cisco Instant Connect users.	See the "Managing Users" section on page 2-8
Configuration Drawer		
Multicast Pool	Provides information the multicast pool in Cisco Instant Connect Express, and lets you add, delete, and manage the multicast pools.	See the "Managing the Multicast Pool" section in *Cisco IPCIS Server Administration Guide*."
UMS	Provides information the UMS components in Cisco Instant Connect Express, and lets you add, delete, and manage these components.	See the "Managing the UMS" section in *Cisco IPCIS Server Administration Guide*."
Splash	Lets you configure the optional splash screen that can appear during the Cisco Instant Connect login process.	See the "Configuring the Splash Screen" section in *Cisco IPCIS Server Administration Guide*."
Trust Management	Let you view and manage trust relationships between servers in your Cisco Instant Connect Express deployment.	See the "Managing Trust Between Servers" section in *Cisco IPCIS Server Administration Guide*."
Administration Drawer		
Database Management	Lets you schedule and manage Cisco Instant Connect Express database backups, and restore backed up data if needed.	See the "Performing Cisco IPICS Database Backup and Restore Operations" chapter in *Cisco IPCIS Server Administration Guide*."
License Management	Provides information about the licenses that are configured for your Cisco Instant Connect Express installation, and allows you to upload and apply new licenses.	See the "Managing Licenses" section in *Cisco IPCIS Server Administration Guide*."
Active Users	Lets you view the activity for users who are logged in to the system.	See the "Viewing Active Users" section in *Cisco IPCIS Server Administration Guide*."

Table 2-2 Administration Console Windows (continued)

Window	Description	Reference
Activity Log Management	Lets you search for and download activity logs.	See the "Managing Activity Logs" section in *Cisco IPCIS Server Administration Guide*."
Activity Log Options	Lets you specify the activities that you want Cisco Instant Connect Express to log.	See the "Choosing Activities to Log" section in *Cisco IPCIS Server Administration Guide*."
Options	Lets you configure various Cisco Instant Connect Express options.	See the "Managing Cisco IPICS Options" section in *Cisco IPCIS Server Administration Guide*."
Serviceability Drawer		
Dashboard	Displays current, real-time information regarding the overall status of your system.	See the "Viewing the Information in the Dashboard Window" section in *Cisco IPCIS Server Administration Guide*."
Diagnostics	Displays diagnostic information for various components of the Cisco Instant Connect Express server.	See the "Viewing Cisco IPICS Server Diagnostic Information" section in *Cisco IPCIS Server Administration Guide*."
System Logs	Lets you view current server log information.	See the "Viewing the Cisco IPICS System Logs" section in *Cisco IPCIS Server Administration Guide*."
System Event Notify	Lets you enable and disable system event email notification.	See the "Managing System Event Notifications" section in *Cisco IPCIS Server Administration Guide*."

Managing Users

The following sections provide general procedures for managing users in Cisco Instant Connect Express. For more detailed information about the options for managing users, see the "Managing Users" section in *Cisco IPCIS Server Administration Guide*."

- Adding a User, page 2-9
- Updating Information for a User, page 2-11
- Deleting a User, page 2-11

Cisco Instant Connect Express includes four preconfigured users, named user1, user2, user3, and user4. The default password for each of these users is Ipics_123. Cisco recommends that you reset these default passwords as described in the "Updating Information for a User" section on page 2-11 when you start using the system.

Adding a User

Adding a user to Cisco Instant Connect Express involves entering information about the user and configuring various options for the user. After a user is added, that user can log in to Cisco Instant Connect Express from a mobile client.

Cisco Instant Connect Express supports up to 50 concurrent mobile client users.

If you add a user who has the same channel assignments, roles, and other information as that of an existing user, you might find it convenient to start by copying the information of the existing user. When you copy such information, Cisco Instant Connect Express opens a New User window and enters all information that is stored for the existing user, except the user ID and password.

To add a user, follow these steps:

Procedure

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

Step 2 In the Users window, take either of the following actions:

- To add a user starting with a blank New User window, click **Add**.
- To add a user starting with a New User window that includes information based on an existing user, check the check box next to the existing user, and then click **Copy**. (The **Copy** button appears dimmed if you do not check an existing user or if you check more than one existing user.)

The New User window appears. If you clicked **Copy**, this window includes information from the existing user, except for the user ID and password.

Step 3 In the New User window, take these actions:

a. In the User Name field, enter a unique identification name for this user.

The User ID can include alphanumeric characters, numbers, underscores (_), and periods (.).

A User ID is not case-sensitive. If a User ID contains alphabetic characters, a user can enter the characters in upper case or lower case when logging in to Cisco IPICS.

b. In the First Name field, enter the First name of the user.

Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (').

c. In the Last Name field, enter Last name of the user.

Valid characters include: alphanumeric characters, space, hyphen (-), and apostrophe (').

d. In the Password and the Confirm Password fields, enter the password that the user enters when logging in to Cisco IPICS or the IDC. (The actual characters in the password are represented by asterisks (*)).

You specify requirements for passwords, including length and character requirements, in the **Administration > Options** window.

Valid characters include: alphanumeric characters and these special characters: @ [\ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?.

Passwords are case-sensitive. A user must enter a password exactly as it is configured.

e. (Optional) In the Description field, enter a description of, or notes that relate to, the user for your reference.

f. (Optional) To include an image of the user or an image that relates to the user, click **Browse**, then navigate to and select the image file.

g. (Optional) In the Roles area, add one or more Cisco Instant Connect roles for the user by selecting a role from the drop-down list.

For information about roles, see the "Cisco Instant Connect Express Roles" section on page 2-1.

Step 4 (Optional) In the Address tab, enter the physical address and the e-mail address for the user.

Step 5 (Optional) In the Permission tab, configure these items:

- Disable Audio—Disables the microphone and speaker on the mobile client from which the user is logged in to Cisco Instant Connect Express, which prevents a user from listening and talking on a talkline
- Listen Only—Disables the transmission of audio on the mobile client from which the user is logged in to Cisco Instant Connect Express, which restricts a user to listening only
- Allow Latch—Enables the latch feature on the mobile client from which the user is logged in to Cisco Instant Connect Express.
- Maximum Talk Priority—Highest talk priority that the user can choose from Cisco Instant Connect. When two talkers with the same priority talk on a Cisco Instant Connect mobile device, the system mixes the streams. When a higher priority user talks while a lower priority user is talking, the system stops streaming (preempts) the lower priority call. When a higher priority user is talking and a lower priority user attempts to PTT, the system denies PTT access to the lower priority user.
- Default Talk Priority—Default talk priority for the user. The system uses this talk priority if the user does not choose another one. The system default talk priority value is 4.

Step 6 In the Communications tab, configure these items:

- Notification Preferences—Any combination of one or more email, Short Message Service (SMS), or pager addresses for the user.

  To add a notification preference:

  a. Click **Add**.

  b. From the drop-down list, choose a method by which the user receives notifications (e-mail, pager, or SMS).

  c. In the field next to the drop-down list, enter the e-mail address for the corresponding notification method.

  For the SMS and Pager methods, the e-mail address is for a gateway through which the message will be sent to the device.

  d. Click **Done**.

  Repeat these steps as needed to add more notification preferences.

- Dial Preferences—One or more telephone numbers for the user.

  To add a dial preference:

  a. Click **Add**.

  b. From the drop-down list, choose a description for the dial preference.

  c. In the field next to the drop-down list, enter the telephone number for the corresponding dial preference.

  The first character must be a digit or a plus sign (+).

  This character can be followed by zero or one or more of these characters: digits, upper case or lower case letters, space, : . , - ( ) # *.

  d. One or more digits must be included next.From the drop-down list, choose a description for the dial preference.

e. In the field next to the drop-down list, enter the telephone number for the corresponding dial preference.

   The first character must be a digit or a plus sign (+).

   This character can be followed by zero or more of these characters: digits, upper case or lower case letters, space, : . , - ( ) # *.

   The number may end with a digit or with one or more pound signs (#) or asterisks (*).

f. Click **Done**.

g. Repeat these steps as needed to add more dial preferences.

Step 7 Click **Save** to add the user.

If you do not want to add the user, click **Cancel**.

Updating Information for a User

To update information for a user who has been added to Cisco Instant Connect Express, follow these steps:

Procedure

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

Step 2 Check the link in the User Name column for the user whose information you want to update.

Step 3 Update information in the General, Address, Permission, and Communications tabs as needed.

For information about the options in these tabs, see the "Adding a User" section on page 2-9.

Step 4 Click **Save** to save the updates.

If you do not want to save the updates, click **Cancel**.

Deleting a User

If a user is no longer needed, you can delete the user from Cisco Instant Connect Express.

If you delete a user who is logged in to Cisco Instant Connect Express from a mobile client, that user is logged out from the mobile client when the mobile client receives its next automatic update from Cisco Instant Connect Express.

You can delete a single user or you can delete several users at one time.

To delete a user or users, perform the following procedure:

Procedure

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

Step 2 Check the check box next to each user that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the user or users, click **Cancel**.

Managing Talklines

A talkline is a virtual mechanism that enables Cisco Instant Connect Express users to communicate with each other by joining the talkline from an Android device that is running Cisco Instant Connect. A user who has joined a talkline is called a *participant*.

Cisco Instant Connect Express includes four preconfigured talklines, named talkline1, talkline2, talkline3, and talkline4,

The following sections describe how to manage talklines:

- Adding a Talkline, page 2-12
- Updating Information for a Talkline, page 2-13
- Activating or Deactivating a Talkline, page 2-13
- Deleting a Talkline, page 2-14

Adding a Talkline

To add a talkline, follow these steps:

Procedure

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

Step 2 In the Talklines window, click **Add**.

Step 3 In the General tab, configure these items:

- Talk Line Name—Enter a unique name for the talkline. The name can contain alphanumeric characters, special characters, and spaces.
- Description—Enter a description for the talkline.

The Status field is view only and indicates whether the talkline is active or inactive. For more information, see the "Activating or Deactivating a Talkline" section on page 2-13.

Step 4 In the Mobile tab, configure these items:

- Allow Latch—Check this check box enable the latch feature on Cisco Instant Connect mobile clients that communicate on this talkline
- Listen Only—Check this check box if you want users to be able to listen only when communicating on this talkline

Step 5 (Optional) Designate each who can join this talkline (when it is active) from a mobile client by dragging and dropping the user name from the Users Resources area to the Participants area.

You can use the **Search** button to locate a user.

After you complete the drag and drop operation and release the mouse button, the user that you added to the inactive talkline appears in green until you click **Save** to commit the change. To remove a user that appears in green, drag the name out of the Participants area and into the Resources area.

Step 6 Click **Save** to add the talkline.

If you do not want to add the talkline, click **Cancel**.

Updating Information for a Talkline

To update information for a talkline, follow these steps:

Procedure

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

Step 2 Check the link in the Talkline Name column for the talkline that you want to update.

Step 3 Update information in the General, Mobile, and Participants tabs as needed.

For information about the options in these tabs, see the "Adding a Talkline" section on page 2-12.

Step 4 Click **Save** to save the updates.

If you do not want to save the updates, click **Cancel**.

Activating or Deactivating a Talkline

A talkline can have either of the following statuses:

- Active—A talkline that provides a live connection to each participant, so that the participants can communicate with each other. An active talkline consumes system resources.
- Inactive—A talkline that does not provide a live connection to its participants. You can activate an inactive talkline at any time.

You can change the status of a single talkline, or you can change the status of several talklines that have the same status at one time.

Activating a talkline causes Cisco Instant Connect Express to commit the network resources that are required to enable talkline participants to communicate with each other.

Note When you activate a talkline, there may be a delay before users can communicate with each other, especially if the talkline contains many users,. The delay may range from a few seconds to more than one minute, depending on the number of participants in the talkline.

To change the status of a talkline, follow these steps:

Procedure

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

Step 2 Check the link in the Talkline Name column for each talkline for which you want to update the status.

If you choose multiple talklines, each one must have the same status.

Step 3 From the Change Status drop-down menu, choose **Activate** (for an inactive talkline) or **Deactivate** (for an active talkline).

The option that does not apply appears dimmed.

Deleting a Talkline

If a talkline is no longer needed, you can delete the talkline from Cisco Instant Connect Express. You can delete a single talkline or you can delete several talklines at one time.

A talkline must be inactive before you can delete it.

To delete a talkline, follow these steps:

Procedure

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

Step 2 Check the check box next to each inactive talkline that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the talkline or talklines, click **Cancel**.

Upgrading Cisco Instant Connect Express to Cisco IPICS

You can upgrade Cisco Instant Connect Express to Cisco IPICS by uploading and applying a Cisco IPICS license file.

The upgrade process can take approximately 10 minutes for a standalone system. When you upgrade, your Cisco Instant Connect Express data and configuration settings are preserved in Cisco IPICS.

Cisco recommends that you perform an upgrade during off-peak hours.

Before you begin, contact your Cisco representative to purchase the appropriate Cisco IPICS license file and save that file in a location that you can access from the Cisco Instant Connect Express server.

To upgrade Cisco Instant Connect Express to Cisco IPICS, follow these steps:

Procedure

Step 1 From the Administration Console, choose **License Management** from the Administration drawer.

The Administration: License Management window appears.

Step 2 Click **Browse** button and use the File Upload pop-up window to locate and select the Cisco IPICS license file.

Step 3 In the Administration: License Management window, click **Upload**.

The license file uploads to the appropriate location in the Cisco Instant Connect Express server and the following message appears in the Administration: License Management window:

```
License file uploaded successfully. Please click Apply for the license changes to take
effect.
```

Step 4 When you see the "License file uploaded successfully" message, click **Apply**.

INDEX

Symbols

A

B

C

D

H

I

L

M

N

O

P

R

S

T

U

V