



## **Cisco Interactive Experience Client 4600 Series User Guide**

Release 2.1.1

**January 29, 2014**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

Any 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.



## CONTENTS

<b>CHAPTER 1</b>	<b>Introduction</b>
<b>CHAPTER 2</b>	<b>Setting Up the IEC</b>
<b>CHAPTER 3</b>	<b>Configuring Settings</b>
<b>CHAPTER 4</b>	<b>Off-Line Caching</b>
<b>CHAPTER 5</b>	<b>Upgrading the IEC</b>
<b>CHAPTER 6</b>	<b>Debugging Console</b>
<b>CHAPTER 7</b>	<b>Locally Configuring the IEC</b>
<b>APPENDIX A</b>	<b>Compatible Peripherals</b>
<b>APPENDIX B</b>	<b>Printers</b>
<b>APPENDIX C</b>	<b>Optical Scanners</b>
<b>APPENDIX D</b>	<b>Magnetic Card Readers and Barcode Scanners</b>
<b>APPENDIX E</b>	<b>Infrared Remote Controls</b>
<b>APPENDIX F</b>	<b>Video Conferencing Using the Session Initiation Protocol Client</b>
<b>APPENDIX G</b>	<b>Stream Live Video</b>
<b>APPENDIX H</b>	<b>Content Guidelines</b>
<b>APPENDIX I</b>	<b>HD Video Conferencing Between Two IECs Using the Video Encoder Card</b>







# CHAPTER 1

## Introduction

---

Revised: January 29, 2014, OL-26457-05

## Chapter Overview

The Cisco Interactive Experience Client 4600 Series are state-less computer devices designed to power various-purpose kiosks, Internet terminals, and specialized workstations. The Cisco Interactive Experience Client 4600 Series can be managed remotely with the Cisco Interactive Experience Manager console.

This user guide assumes that the Cisco Interactive Experience Manager has already been installed and configured. If not, refer to the *Cisco Interactive Experience Manager Installation Guide* and the *Cisco Interactive Experience Manager Administrator Guide* for instructions on how to install and configure the software.

This chapter explains the audience and scope of this user guide and provides an overview of the Cisco Interactive Experience Client 4600 Series.

The topics in this chapter are the following:

- [What's New in This Release, page 1-2](#)
  - [HD Video Conferencing Between Two IECs, page 1-2](#)
  - [Video Snapshots and 1080p Streaming, page 1-2](#)
  - [DTMF, page 1-3](#)
  - [global.window Object, page 1-3](#)
  - [VNC, page 1-3](#)
  - [Audio Mode Fall Back, page 1-3](#)
  - [Hide Mouse Cursor, page 1-3](#)
- [About This User Guide, page 1-3](#)
  - [Terminology, page 1-3](#)
  - [Audience, page 1-4](#)
  - [Scope, page 1-4](#)
- [Cisco Interactive Services Solution, page 1-4](#)
  - [Cisco Interactive Experience Manager, page 1-5](#)
  - [Cisco Interactive Experience Client 4600 Series, page 1-6](#)

- [Principles of Operation, page 1-7](#)
- [Kiosk Navigation, page 1-7](#)
- [Package Contents, page 1-8](#)
- [What You Will Need, page 1-9](#)

## What's New in This Release

Release 2.1.1 includes the following new features or enhancements for the Cisco Interactive Experience Client (IEC) 4600 Series:

- Embedded video encoder card for high-definition video conferencing between two IECs
- Encoder driver update that enables video snapshots and 1080p streaming
- DTMF tone generated for SIP
- An API to manipulate browser windows
- VNC managed by the IEM
- Audio mode falls back to 'Analog' when USB output devices are configured but not connected
- Default value of the `mouse.cursor.visible` property is now 'Hide mouse cursor'



### Note

In addition to the new features and enhancements listed above, several of the widgets (e.g. `videoPlayer`, `webClip`, and `sipPhone`) and global objects (e.g. `keyboard` and `videoEncoder`) have been enhanced for release 2.1.1. See the *Cisco Interactive Services Solution Developer Guide v2.1.1* for the latest widgets and global objects.

## HD Video Conferencing Between Two IECs

A Video Encoder Card (VEC) has been embedded in both the IEC 4610 and 4632 models for versions 2.1 and later. The VEC is a Peripheral Component Interconnect Express (PCIe)-based encoder. The VEC allows IEC 4600 Series devices to record and transcode video using the H.264 video codec. As a result, HD video calls can be made between two IECs as an alternative to making a SIP call between an IEC and a Cisco Unified IP Phone 9951.

Refer to Appendix I for more information.

## Video Snapshots and 1080p Streaming

The encoder driver for the System Dimensions AVS 2610 video encoder dongle and the built-in VEC has been enhanced to enable video snapshots and 1080p streaming. Video snapshots are controlled by the `global.videoEncoder` object.

Refer to the *Cisco Interactive Services Solution Developer Guide 2.1.1* for the `global.videoEncoder` object.

## DTMF

In release 2.1.1, Dual-Tone Multifrequency (DTMF) is supported for SIP calls. The purpose of DTMF setup for SIP is to provide the audio prompts heard over the phone such as “Press 1 to reach \_\_\_\_.”

## global.window Object

In release 2.1.1, `global.window.open` and `global.window.close` are added to control child windows.

Refer to the *Cisco Interactive Services Solution Developer Guide 2.1.1* for the `global.window` object.

## VNC

The `vnstart` and `vnstop` debugging commands have been removed from the custom shell in the IEC so that VNC can be managed by the IEM. Chapter 2 provides instructions on how to use a VNC viewer to access an IEC.

Refer to the *Cisco Interactive Experience Manager Administration Guide 2.1.1* for instructions on how to enable VNC and push it to an IEC.

## Audio Mode Fall Back

The audio mode falls back to ‘Analog’ when the audio output is configured as ‘USB headset’ or ‘USB speaker’ but a USB headset or speaker is not connected to the IEC.

## Hide Mouse Cursor

The default value of the `mouse.cursor.visible` property has changed to ‘Hide mouse cursor’ from “Show mouse cursor”.

## About This User Guide

This version of the guide is intended for release 2.1.1.

This section describes what is included in this guide and explains who should use it.

## Terminology

The following terms are used in this user guide.

- **Accounts** - Allow multiple organizations to configure and manage devices and policies in a single Cisco Interactive Experience Manager instance. Use accounts to segregate users, devices, and policies. Each organization will have at least one account.
- **Administrators** - People who have access to all accounts on the system. The *Cisco Interactive Experience Manager Installation Guide* provides administrators with all the information necessary to install and administer the Cisco Interactive Experience Manager.

- Device - Cisco Interactive Experience Client 4600 Series
- Policies- An easy and flexible way of applying settings to multiple devices or users.
- Users - People who are associated with specific accounts on Cisco Interactive Experience Manager. They cannot access any other account except for the ones that they are assigned to.

## Audience

The intended audience for this guide are administrators who will install, configure, troubleshoot, and maintain the Cisco Interactive Experience Client 4600 Series hardware and software.

## Scope

This user guide explains how to use the Cisco Interactive Experience Client 4600 Series.

This user guide provides instructions so that an administrator or user can:

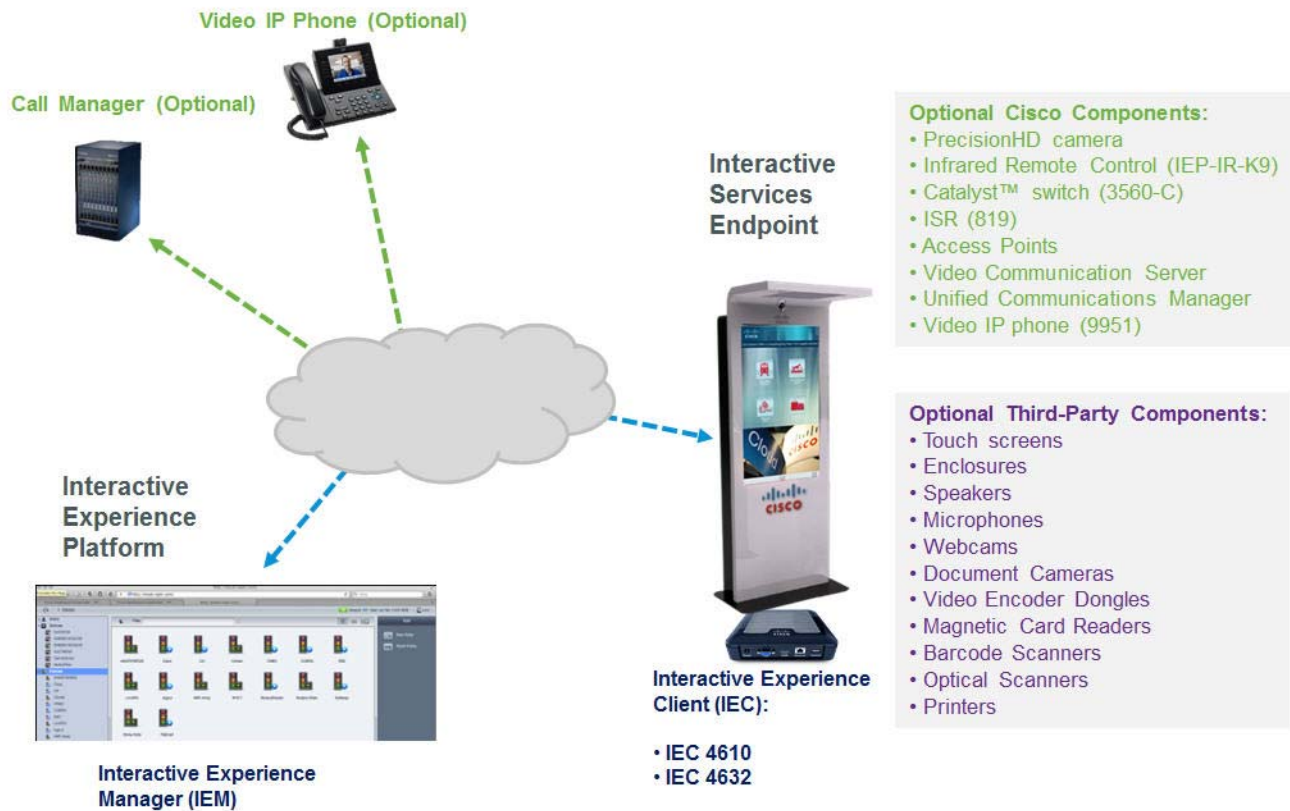
- Connect the equipment
- Configure the system
- Configure the network
- Connect to the Cisco Interactive Experience Manager
- Register an account
- Configure local settings for demos

## Cisco Interactive Services Solution

Cisco Interactive Services Solutions leverages the network as the platform to transform customer experience with interactive digital media. Leveraging Cisco's video, collaboration, and cloud architectures, the solution allows large and small enterprises and public agencies to seamlessly provide the most updated product or service information including educational content in real-time, improving customer experience and increasing customer retention. With built-in remote management capabilities, the solution enables organizations to get feedback instantaneously from end users to measure marketing effectiveness and impact as well as dynamically provision and disperse relevant content. Effective reuse of web content and applications along with remote delivery of content and advertisements helps increase advertising revenues, improve business and customer processes, through effective management of digital displays and open online spaces.

The Cisco Interactive Services Solution is the collective name for a product family that consists of hardware and software including the Cisco Interactive Experience Manager software and the Cisco Interactive Experience Client 4600 Series hardware and software.

**Figure 1-1 Cisco Interactive Services Solution Deployment Diagram**



## Cisco Interactive Experience Manager

The Cisco Interactive Experience Manager (IEM) is the management console that allows the administrator to configure, control, and monitor Cisco Interactive Experience Client 4600 Series devices. The Cisco Interactive Experience Client 4600 Series devices are configured remotely through a combination of device, user, profile, and policy settings from the Cisco IEM. Configuration settings are distributed between user and device settings. Policies represent dynamic and transportable setup rules.

With Cisco IEM, an administrator can perform the following functions:

- **Configuration:** A user can configure all Cisco Interactive Experience Client 4600 Series device settings remotely including the startup URL, VPN, display behavior, peripheral support.
- **Policy Management:** Policies provide an easy and flexible way for a user to apply settings to a group of users or devices.
- **Kiosk Control:** A user can monitor and control the behavior of a kiosk remotely in real-time including muting a station, locking out the user, sending messages to the user, etc.
- **Session Management:** A user can manage users' sessions on the kiosks by setting time limits, forcing the user to log out, etc.

- **Monitoring:** Data is sent from the Cisco Interactive Experience Client 4600 Series devices to the Cisco IEM at regular intervals. A user can analyze the event logs and performance data to troubleshoot issues.

## Cisco Interactive Experience Client 4600 Series

The Cisco Interactive Experience Client (IEC) 4600 Series is a robust, configurable, and manageable web device designed for public venues and web-centric delivery. It is an integrated thin client device with a complete operating system on board. The user interface is designed for ease-of-use and simplicity. The interface also allows a large degree of customization based on the usage requirements.

The Cisco IEC 4600 Series can operate in either Stand-alone or Management mode. When operating in Management mode, they adhere to the configuration profile set up by the administrator. This allows the administrator to control and monitor the devices as needed. When the Cisco IEC 4600 Series operates in Management mode, it adheres to the configuration profile set up by the administrator. It is highly recommended that all the Cisco IEC 4600 Series devices are managed and monitored using the Cisco Interactive Experience Manager as it ensures consistent remote management with the option to configure the devices locally.

Additionally, the Cisco IEC 4600 Series can be configured to operate in either Desktop or Kiosk mode to serve as web productivity workstations or public access terminals. Kiosk mode opens up a full-screen web resource and restricts the user from opening multiple windows whereas Desktop mode allows multiple windows to be opened with access to various web resources.

The Cisco IEC 4600 Series is powered by the COBRA browser operating system. This innovative operating system is built to provide a “desktop-in-a-browser” environment, giving the users a familiar feel of the desktop when interacting with Internet resources and applications. The COBRA browser is compatible with all major Internet sites and gives the user a very intuitive and simple way of interacting with web-based content and applications. Each Internet resource runs in its own window and is represented by an automatically updating thumbnail ribbon on the bottom of the screen. In addition to web browsing, the software supports Internet telephony client, Java, and PDF viewer.

The operating system of the Cisco IEC 4600 Series has the following capabilities:

- Full HTML browser
- Flexible windowing environment
- Single-window kiosk environment
- Dual screen support
- Touch screen support
- Display rotation
- Rich media playback support
- Remote management, control, and upgrade mechanism

The Cisco IEC 4600 Series do not store user data locally. Rather, files created from an Internet resource are typically stored at the Internet resource itself. It also allows for a USB media storage device or a camera with a USB interface to be connected for file download and upload.

## Principles of Operation

The following are principles of operation for this solution:

1. **IEC 4600 Series devices need to exist on the IEM in order to be managed by it.** IEC 4600 Series devices can either be provisioned ahead of time or from the device interactively. If registered from the device interactively, the installer has to use their account info to authorize the registration.
2. **Policy applied to the device overrides devices' own configuration.** Properties are additive, therefore if policy doesn't override a property, the property will stay unchanged.
3. **Multiple policies can be attached to the same device (group).** If policies contain conflicting settings, the policy that is higher in the stack order takes precedence. Device policies take precedence over group policies.
4. **IEC 4600 Series and IEM versions are best-effort compatible.** A device that has a version that is not actively supported by the IEM will still be supported although some things may not have full functionality. A device version which is out of sync is indicated by the red FW flag. Communication between client and the IEM is defined by the communication protocol and specification that defines capabilities of each FW build: older communication protocols are supported in the newer IEM builds, but older specifications that reflect properties of the firmware are often not fully compatible with the later versions.
5. **Policies can be persistent or transient (applied for short periods of time).** Persistent policies are long-term or permanent. Persistent policies are applied when the IEC 4600 Series device is booted or rebooted. Persistent policies are permanent until they are unapplied.

Transient, runtime, or IsAction policies are created by checking the IsAction checkbox when creating the policy or in the General tab of the policy. Transient policies are marked by a blue circle with a white arrow and are made available in form of a button under "Custom Actions". These policies change the settings on the IEC 4600 Series temporarily and will be reset by changing the settings within the policy, by applying another IsAction policy with settings that will reverse the original settings, or on the next reboot. IsAction policies can only work for runtime properties, which are marked by an orange arrow in the policy or profile.

6. **Notifications and alerts work on a subscription basis.** Once notification/alert has been created, it has to be assigned to a user. Notification/alert can submit to a third party application collecting the data – the URL has to be provisioned through User profile.
7. **In order to optimize screen behavior, the application has to implement native components.** Native components are available in form of a Browser API (refer to the documentation) and essentially move resource-intensive or asynchronously used components outside of the browser process-space.

## Kiosk Navigation

If the navigation panel is enabled, customers will interact with the buttons on the navigational panel. If the display is a touch screen, customers can touch the buttons and virtual keyboard with their fingers. Otherwise, the customers can use a mouse to choose the buttons and a keyboard to enter keystrokes. The following buttons are visible to the customer on the navigational panel:

- Question/Help button – Customer uses this button to access a help page.
- Go back one page button – Customer uses this arrow to go to a previous page.
- Stop loading this page button – Customer uses this button to stop the current page from loading.
- Go to startup URL button – Customer uses this button to go to the startup URL

- Reload current page button – Customer uses this button to reload the current page.
- Go forward one page button – Customer uses this arrow to go to the next page.
- Print currently loaded page button – Customer uses this button to print the current page if the kiosk is hooked up to a printer.
- Show virtual keyboard button – Customer uses this button to display a virtual keyboard that they can use to input information.

**Figure 1-2**      **Navigational Panel on Kiosk**

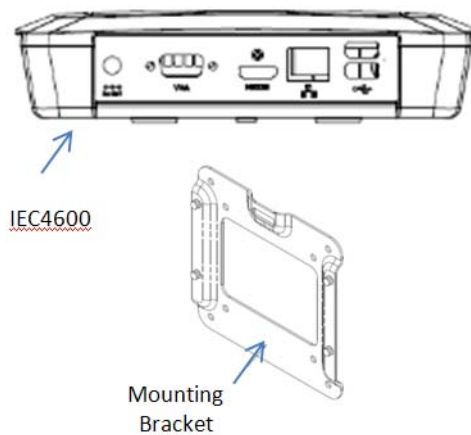


## Package Contents

The package should contain the following components:

- Cisco IEC 4600 Series
- Power adapter
- Mounting plate
- Four mounting screws

**Figure 1-3**      **Cisco IEC 4600 Series and Mounting Bracket**



If any of the contents are missing, contact <http://cisco.com/en/US/support>.



# What You Will Need

**Note**

To optimize the video quality, the IEC 4600 Series should be connected to a 1080p LED or LCD video display using either HDMI (preferred) or VGA.

To install and configure the Cisco IEC 4600 Series, you will need the following:

- Video monitor (non-touch screen or touch screen)
- HDMI or VGA cable
- USB cable if using a touch screen
- USB keyboard (wired or wireless)
- USB mouse (wired or wireless)
- Webcam (optional)
- Ethernet cable
- Wireless network credentials (optional)
- IEM installed and configured

After you have assembled all the equipment, proceed to Chapter 2.





## CHAPTER 2

# Setting Up the IEC

---

Revised: January 29, 2014, OL-26457-05

## Chapter Overview

This chapter explains how to do set up the equipment and configure the Cisco IEC 4600 Series so that it displays the startup URL.

Topics in this chapter include:

- [Connecting the Hardware, page 2-2](#)
  - [IEC Dimensions, page 2-2](#)
  - [IEC Specifications, page 2-2](#)
  - [Environmental Tolerance Ranges, page 2-4](#)
  - [Warnings, page 2-5](#)
  - [FCC Compliance Information Statement \(for USA only\), page 2-9](#)
  - [RF Exposure, page 2-10](#)
  - [Choosing a Location, page 2-12](#)
  - [Mounting the Hardware, page 2-12](#)
  - [Connecting and Powering Up, page 2-13](#)
- [Registering the IEC, page 2-15](#)
- [Configuring the System, page 2-16](#)
- [Connecting to the Network, page 2-20](#)
  - [Configuring an Ethernet \(Wired\) Connection, page 2-20](#)
  - [Configuring a Wireless Connection, page 2-24](#)
- [Connecting to the Cisco IEM, page 2-32](#)
  - [Applying a Policy, page 2-32](#)
- [Calibrating the Touchscreen, page 2-37](#)
- [Using Emergency Configuration Mode, page 2-37](#)
- [Using a VNC Viewer, page 2-39](#)

# Connecting the Hardware

The Cisco IEC 4600 Series is easy to setup. This section describes how to choose a location for the device, mount it, and connect it to a video display, keyboard, mouse, and electrical outlet.

## IEC Dimensions

The table below contains the dimensions of the IEC 4600 Series.

**Table 2-1** *Cisco IEC 4600 Series Dimensions*

US Customary Unit			Modern Metric Unit		
Width	Depth	Height	Width	Depth	Height
7.3 inches	7.4 inches	1.9 inches	18.5 cm	18.8 cm	4.8 cm

## IEC Specifications

The table below contains the IEC specifications for models IEC 4610 and IEC 4632.

**Table 2-2** *Cisco IEC 4600 Series Specifications*

Features	IEC 4610	IEC 4632
<b>PCBA Form Factor</b>		
Board size	6.0 in. x 6.0 in. (150 mm x 150 mm)	6.0 in. x 6.0 in. (150 mm x 150 mm)
<b>Processor</b>		
CPU	Intel Celeron M Processor	Intel Core 2 Duo Processor
<b>Memory</b>		
Type	DDR3-800/1066 memory (SO-DIMM Slot)	DDR3-800/1066 memory (SO-DIMM Slot)
System memory size	2 GB	4 GB
<b>Storage</b>		
Type	SATA socket Disk on Module (DOM)	SATA socket Disk on Module (DOM)
Storage Memory Size	8 GB	32 GB
<b>BIOS Flash Memory</b>		
Memory Size	32 Mbit	32 Mbit
<b>Ethernet</b>		
Count	1	1
Speeds	10/100/1000 Mbps	10/100/1000 Mbps
Connectors	1 Port RJ45 with transformer	1 Port RJ45 with transformer

Features	IEC 4610	IEC 4632
<b>Video</b>		
Onboard	GS45 HDMI	GS45 HDMI
Connectors	1 HDMI port 1 VGA port	1 HDMI port 1 VGA port
<b>USB</b>		
Type	USB 2.0 controller	USB 2.0 controller
Connectors	2 Right USB A type 2 Back USB A type 1 Front USB A type	2 Right USB A type 2 Back USB A type 1 Front USB A type
<b>WiFi+Bluetooth</b>		
Count	1	1
Speed	802.11 b/g, Bluetooth V2.1+EDR	802.11 b/g, Bluetooth V2.1+EDR
<b>Front I/O</b>		
LED	1 Green LED 1 Red LED	1 Green LED 1 Red LED
IR receiver	1 Built-in IR receiver	1 Built-in IR receiver
USB	1 USB connector (for preinstall device)	USB connector (for preinstall device)
<b>Back I/O</b>		
DC jack	1 12V DC in connector	1 12V DC in connector
Video	1 VGA port 1 HDMI port	1 VGA port 1 HDMI port
Ethernet	1 RJ45 connector with dual LEDs	1 RJ45 connector with dual LEDs
USB	1 USB two-stack connector	1 USB two-stack connector
<b>Left I/O</b>		
COM	1 x 3.5 mm phone jack type	1 x 3.5 mm phone jack type
IR extension	1 1-IR extension cable	1 1-IR extension cable
Audio	1 Audio port (MIC-in) 1 Audio port (line-out)	1 Audio port (MIC-in) 1 Audio port (line-out)
USB	1 USB two-stack connector	1 USB two-stack connector
<b>Right I/O</b>		
Buttons	1 Power On/Off button (with soft/hard power option) 1 Reset button	1 Power On/Off button (with soft/hard power option) 1 Reset button

Features	IEC 4610	IEC 4632
<b>Power</b>		
Adapter	12V@4A (48W) Input 100V - 240V ~1A 50-60HZ Output 12V ~4A	12V@4A (48W) Input 100V - 240V ~1A 50-60HZ Output 12V ~4A
Power consumption	12V@48W maximum	12V@48W maximum
CPU VR	Intel Mobile Voltage Positioning (Intel MVP6) Structure	Intel Mobile Voltage Positioning (Intel MVP6) Structure

## Environmental Tolerance Ranges

Refer to the table below for the environmental tolerance ranges.

**Table 2-3, Part 1** Cisco IEC 4600 Series Environmental Tolerance Ranges: Temperature

Temperature <sup>1</sup>	US Customary Unit		Modern Metric Unit	
	Minimum	Maximum	Minimum	Maximum
Operating long-term or short-term	32°F	104°F	0°C	40°C
Non-operating or storage	-4°F	158°F	-20°C	70°C

1. Ambient.

**Table 2-3, Part 2** Cisco IEC 4600 Series Environmental Tolerance Ranges: Humidity

Relative Humidity <sup>1</sup>	Minimum	Maximum
Operating	10 percent (Indoor)	85 percent (Indoor)
Non-operating or storage	0 percent (Indoor and Outdoor)	95 percent (Indoor and Outdoor)

1. Noncondensing; ambient.

**Table 2-3, Part 3** Cisco IEC 4600 Series Environmental Tolerance Ranges: Altitude

Altitude <sup>1</sup>	US Customary Unit		Modern Metric Unit	
	Minimum	Maximum	Minimum	Maximum
Operating and non-operating	0 feet	6,561 feet	0 meters	2,000 meters

1. Above sea level.

# Warnings



## Warning

Read the installation instructions before connecting the system to the power source.

## Attention

Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

## Waarschuwing

Raadpleeg de installatie-instructies voordat u het systeem op de voedingsbron aansluit.

## Varoitus

Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.

## Warnung

Vor dem Anschließen des Systems an die Stromquelle die Installationsanweisungen lesen.

## Avvertenza

Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.

## Advarsel

Les installasjonsinstruksjonene før systemet kobles til strømkilden.

## Aviso

Leia as instruções de instalação antes de ligar o sistema à fonte de energia.

## ¡Advertencia!

Lea las instrucciones de instalación antes de conectar el sistema a la red de alimentación.

## Varning!

Läs installationsanvisningarna innan du kopplar systemet till strömförsörjningsenheten.

## Figyelem

Mielott áramforráshoz csatlakoztatná a rendszert, olvassa el az üzembe helyezési útmutatót!

## Предупреждение

Перед подключением устройства к источнику электропитания ознакомьтесь с данной инструкцией по установке.

## אזהרה

יש לקרוא את הוראות ההתקנה לפני חיבור המערכת למקור המתח.

## Aviso

Leia as instruções de instalação antes de conectar o sistema à fonte de energia.

## 주의

시스템을 전원에 연결하기 전에 설치 지침을 읽으십시오.

## Ostrzeżenie

Przed podłączeniem systemu do źródła zasilania należy przeczytać instrukcje instalacji.

## Warnings

**Upozorneni** Pred pripojením systému k elektrické síti si prostudujte pokyny k instalaci

**Upozornenie** Pred pripojením systému k napájacímu zdroju si precítajte inštalacné pokyny.

**警告** 在将系统与电源连接之前，请仔细阅读安装说明。

**警告** 必ず設置手順を読んでから、システムを電源に接続してください。

**Opozorilo** Preden sistem priključite, preberite navodila za priključitev.



**Warning** Ultimate disposal of this product should be handled according to all national laws and regulations.

**Attention** La mise au rebut ou le recyclage de ce produit sont généralement soumis à des lois et/ou directives de respect de l'environnement. Renseignez-vous auprès de l'organisme compétent.

**Waarschuwing** Het uiteindelijke wegruimen van dit product dient te geschieden in overeenstemming met alle nationale wetten en reglementen.

**Varoitus** Tämä tuote on hävitettävä kansallisten lakien ja määräysten mukaisesti.

**Warnung** Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.

**Avvertenza** Lo smaltimento di questo prodotto deve essere eseguito secondo le leggi e regolazioni locali.

**Advarsel** Endelig kassering av dette produktet skal være i henhold til alle relevante nasjonale lover og bestemmelser.

**Aviso** Deitar fora este produto em conformidade com todas as leis e regulamentos nacionais.

**¡Advertencia!** Al deshacerse por completo de este producto debe seguir todas las leyes y reglamentos nacionales.

**Предупреждение** Окончательная установка данного изделия должна выполняться в соответствии со всеми национальными, региональными и местными правилами и нормами.



<b>Figyelem</b>	<b>A készülék végső elhelyezéséről az adott országban érvényes törvények és eloirások szerint kell intézkedni.</b>
<b>Aviso</b>	<b>O descarte definitivo deste produto deve estar de acordo com todas as leis e regulamentações nacionais.</b>
<b>Ostrzeżenie</b>	<b>Ostateczna likwidacja tego urządzenia po jego wycofaniu z eksploatacji po zgodnie z przepisami krajowymi.</b>
<b>Предупреждение</b>	<b>Окончательная установка данного изделия должна выполняться в соответствии со региональными и местными правилами и нормами.</b>
<b>警告</b>	<b>本产品的废弃处理应根据所有国家的法律和规章进行。</b>
<b>警告</b>	<b>この製品を廃棄処分する際は、各国の法律および規制に従って取り扱ってください。</b>
<b>주의</b>	<b>해당 국가의 관련 법규 및 규정에 따라 이 장치를 폐기해야 합니다.</b>
<b>Оромена</b>	<b>Крајното фрлање на овој производ треба да се изврши во согласност со законите и прописи.</b>
<b>تحذير</b>	<b>عند التخلص من المنتج يجب اتباع القوانين والتشريعات المحلية.</b>
<b>Upozorenje</b>	<b>Zbrinjavanje ovoga proizvoda u otpad treba provesti u skladu s važećim z odredbama.</b>
<b>Upozornění</b>	<b>Upozornění: Likvidace tohoto výrobku musí být provedena podle platných</b>
<b>Προειδοποίηση</b>	<b>Η τελική απόρριψη αυτού του προϊόντος πρέπει να γίνεται σύμφωνα με όλους και κανονισμούς.</b>
<b>Opozorilo</b>	<b>Uničenje izdelka, ki ni več uporaben, mora potekati po državnih zakonih in</b>

**Varning!** Vid deponering hanteras produkten enligt gällande lagar och bestämmelser.

**Advarsel** Endelig bortskaffelse af dette produkt skal ske i henhold til gældende love og regler.

**אזהרה** סילוק סופי של מוצר זה חייב להיות בהתאם להנחיות ולחוקי המדינה.

**Upozornenie** Upozornenie Likvidácia tohto výrobku musí byť vykonaná podľa platných predpisov.



**Warning**

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

**Attention** Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

**Waarschuwing** Er is ontplofingsgevaar als de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type dat door de fabrikant aanbevolen is. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften weggegooid te worden.

**Varoitus** Räjähdyksen vaara, jos akku on vaihdettu väärään akkuun. Käytä vaihtamiseen ainoastaan saman- tai vastaavantyyppistä akkua, joka on valmistajan suosittelema. Hävitä käytetyt akut valmistajan ohjeiden mukaan.

**Warnung** Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

**Figyelem**

Robbanásveszélyt idézhet elő, ha helytelenül cserélik ki az akkumulátort. Csak a által javasolttal megegyező vagy azzal egyenértékű típusúra cserélje ki az akkum. A használt akkumulátorok kidobásakor tartsa be a gyártó előírásait!

**Avvertenza** Pericolo di esplosione se la batteria non è installata correttamente. Sostituire solo con una di tipo uguale o equivalente, consigliata dal produttore. Eliminare le batterie usate secondo le istruzioni del produttore.

**Advarsel** Det kan være fare for eksplosjon hvis batteriet skiftes på feil måte. Skift kun med samme eller tilsvarende type som er anbefalt av produsenten. Kasser brukte batterier i henhold til produsentens instruksjoner.

**Aviso** Existe perigo de explosão se a bateria for substituída incorrectamente. Substitua a bateria por uma bateria igual ou de um tipo equivalente recomendado pelo fabricante. Destrua as baterias usadas conforme as instruções do fabricante.

**Figyelem**

Robbanásveszélyt idézhet elő, ha helytelenül cserélik ki az akkumulátort. Csak a által javasolttal megegyező vagy azzal egyenértékű típusúra cserélje ki az akkumulátort. A használt akkumulátorok kidobásakor tartsa be a gyártó előírásait!

**Предупреждение**

При неправильной замене батареи возможен взрыв. Для замены следует использовать батарею того же или аналогичного типа, рекомендованного изготовителем. Утилизацию батареи необходимо производить в соответствии с указаниями изготовителя.

**警告**

電池更換不當會有爆炸危險。請只用同類電池或制造商推薦的功能相當的電池更換原有電池。請按制造商的說明處理廢舊電池。

**¡Advertencia!**

Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

**警告**

電池替換錯誤可能會發生爆炸。僅限以製造商建議的同樣或同款電池替換，並遵照製造商的指示處理使用過的電池。

**警告**

不適切なバッテリーに交換すると、爆発の危険性があります。製造元が推奨するものと同じまたは同等のバッテリーだけを使用してください。使用済みのバッテリーは、製造元が指示する方法に従って処分してください。

**Varning!**

Explosionsfara vid felaktigt batteribyte. Ersätt endast batteriet med samma batterityp som rekommenderas av tillverkaren eller motsvarande. Följ tillverkarens anvisningar vid kassering av använda batterier.

## FCC Compliance Information Statement (for USA only)

Product IEP-46XX-HW-K9

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

**Note**

Equipment must be installed and operated using the relevant manuals and only installed with the correct cables and connectors. Cisco Systems Inc. is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**Responsible party:**

Cisco Systems Inc.  
170 West Tasman Drive  
San Jose, CA 95134  
USA  
+408 526-7208

## RF Exposure

The Cisco products are designed to comply with the following national and international standards on Human Exposure to Radio Frequencies.

- US 47 Code of Federal Regulations Part 2 Subpart J
- American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers / IEEE C 95.1 (99)
- International Commission on Non Ionizing Radiation Protection (ICNIRP) 98
- Ministry of Health (Canada) Safety Code 6. Limits on Human Exposure to Radio Frequency Fields in the range from 3kHz to 300 GHz
- Australia Radiation Protection Standard

**Caution**

To ensure compliance with various national and international Electromagnetic Field (EMF) standards, the system should only be operated with Cisco approved antennas and accessories.

**THIS DEVICE MEETS THE FCC GUIDELINES FOR EXPOSURE TO RADIO WAVES**

Your device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in FCC Part 1.1310. The guidelines are based on IEEE ANSI C 95.1 (92) and include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

The device has been tested and found compliant with the applicable regulations as part of the radio certification process.

**Table 2-4 Separation Distance**

MPE	Distance	Limit
x.xxx	x cm / x inches	x.xx
mW/cm <sup>2</sup>		mW/cm <sup>2</sup>

The US Food and Drug Administration has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. The FCC recommends that if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing the antennas at a greater separation distance then recommended or lowering the transmitter power output.

**THIS DEVICE MEETS THE HEALTH CODE 6 GUIDELINES FOR EXPOSURE TO RADIO WAVES**

The device has been evaluated and found compliant with the requirements set forth in Industry Canada RSS-102, Evaluation Procedure for Mobile and Portable Radio Transmitters with respect to health Canada Safety Code 6 for Exposure of Humans to Radio Frequency Fields.

Health Canada states that present scientific information does not indicate the need for any special precautions for the use of wireless devices.

**THIS DEVICE MEETS INTERNATIONAL GUIDELINES FOR EXPOSURE TO RADIO WAVES**

Your device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) recommended by international guidelines. The guidelines were developed by an independent scientific organization (ICNIRP) and include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

**Table 2-5 Separation Distance**

MPE	Distance	Limit
x.xxx	x cm / x inches	x.xx
mW/cm <sup>2</sup>		mW/cm <sup>2</sup>

The World Health Organization has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices.

However if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing the antennas at a greater separation distance than recommended.

Additional information on the subject can be found at the following links

- FCC Web site: <http://www.fcc.gov/encyclopedia/radio-frequency-safety>
- FDA Website <http://www.fda.gov>
- Health Canada: <http://hc-sc.gc.ca/ewh-semt/radiation/index-eng.php>
- World Health Organization Internal Commission on Non-Ionizing Radiation Protection at [www.who.int/emf](http://www.who.int/emf)
- Mobile Manufacturers Forum at [www.mmfa.org](http://www.mmfa.org)

## Choosing a Location

The Cisco IEC 4600 Series is intended for indoor use only. The Cisco IEC 4600 Series must be located within eight feet of an electrical outlet for the power adapter to reach the outlet.

## Mounting the Hardware

The Cisco IEC 4600 Series comes with an optional mounting bracket, which makes mounting the unit to a monitor with a VESA mount or various other surfaces (walls, desks, etc.) easy.

**Tip**

Since Cisco IEC 4600 Series is designed for convectional cooling, vertical mounting is highly recommended.

**Note**

If you want to use a remote control and you will not use an IR extender as is recommended, the infrared (IR) must be in sight of the user. Hence you will need to determine an alternative mounting to that which is recommended here.

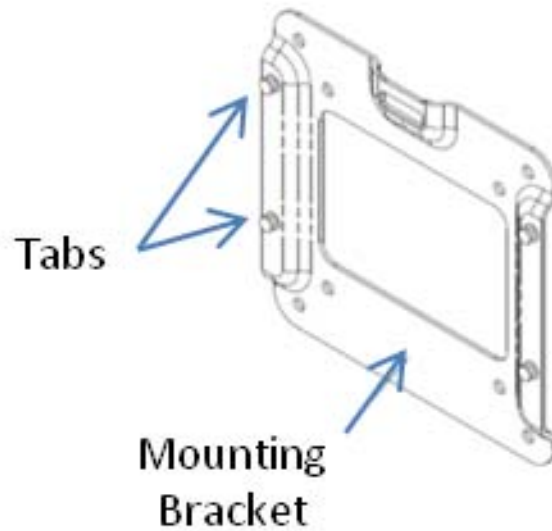
**Step 1** Locate a vertical surface near the video display where you want the IEC 4600 Series to be mounted.

**Step 2** Attach the mounting place to the video display, wall, or kiosk. Mount so that the up arrow points upwards and is visible.

**Note**

If mounting to sheet rock or other porous surface, use appropriate mounting hardware (not supplied).

**Figure 2-1** Ports on the Cisco IEC 4600 Series



- Step 3** Carefully slide the IEC 4600 Series onto the tabs on the mounting hardware. The display and network connections will be facing to the floor.
- 

## Connecting and Powering Up

The back of the Cisco IEC 4600 Series contains multiple ports that will be used to connect to the video display, keyboard, mouse, network, and electrical outlet. Follow the steps below to connect the equipment and power on the device.

---

- Step 1** Connect an USB keyboard to one of the USB ports on the Cisco IEC 4600 Series.



**Tip**

It is recommended that you use a wired keyboard as opposed to a wireless keyboard. With some wireless keyboards, the IEC detects it as a second touchscreen instead of a keyboard.

---

**Figure 2-2** Ports on the Cisco IEC 4600 Series



- Step 2** Connect an USB cable or wireless USB adapter for a mouse to an USB port on the Cisco IEC 4600 Series.
- Step 3** (Optional) Connect an USB cable for a webcam to an USB port on the Cisco IEC 4600 Series.
- Step 4** (Optional) Connect other peripherals such as speakers, microphone, magnetic card reader, barcode scanner, printer, etc.



---

**Note** If using the RS232 port for a RCA, TRS, or TRRS connector, the tip of the connector corresponds to pin 2 and the ring of the connector corresponds to pin 3 on a DB-9 connector.

---

- Step 5** Connect the video display cable to either the VGA or the HDMI port on the Cisco IEC 4600 Series. Then connect the other end of the cable to the video display.



---

**Tip** To optimize the video quality, the IEC 4600 Series should be connected to a 1080p LED or LCD video display using the HDMI cable.

---

- Step 6** If the display is a touch screen, connect an USB cable to it and an USB interface on the Cisco IEC 4600 Series.
- Step 7** Plug the power cord for the video display into an electrical outlet.
- Step 8** Turn on the power to the video display.
- Step 9** Connect an Ethernet cable to the LAN port on the Cisco IEC 4600 Series. Connect the other end of the Ethernet cable to an Ethernet wall jack or Ethernet port on a router or switch.
- Step 10** Connect the power adapter to the DC 12V in connector on the Cisco IEC 4600 Series.
- Step 11** Plug the power adapter into an electrical outlet.
- 

The Cisco IEC 4600 Series will initialize now. When it finishes initializing, the COBRA screen appears.



**Figure 2-3 Initialization Screen****Note**

After initialization “Startup URL is not configured” will appear at the top of the screen. It is referring to the URL that the Cisco IEC 4600 Series will use to display content once it is configured.

Record the serial number and IP address shown on the COBRA screen.

**Note**

If there are any problems with the initial configuration or the network, the system will not initialize and the Cobra screen will not appear. If that happens, refer to “Using Emergency Configuration Mode”.

## Registering the IEC

The IEC 4600 Series must first be registered in the IEM to manage it remotely. To register a device, you will need the following:

- Enough licenses in the IEM to cover the new device
- The IEC’s serial number, which can be found on the bottom of the device
- User credentials on the IEM

A license for the device must exist in the IEM before the device can be registered. If a license does not exist in the IEM to cover the device, the device will not register and it cannot be managed by the IEM until a license is obtained for it. For more information about licensing, refer to the *Cisco Interactive Experience Manager Administrator Guide*.

You will register the IEC using the New Device button within the Devices’ Edit menu. Refer to the “Adding a New Device” section of the *Cisco Interactive Experience Manager Administrator Guide* for instructions on how to add the device.

# Configuring the System

To configure the system, you will need the Cisco IEM URL. If you do not know the URL, contact the administrator in your company who installed and configured the Cisco IEM.

- Step 1** Press Ctrl-Alt-S. The combination of these three keys opens the System Settings window.

**Figure 2-4** *System Settings Window*



In Chapter 7, you will learn how to configure each of the settings. For now you will learn how to configure the system settings to get started.

- Step 2** Click the **System** icon.
- Step 3** Now you will configure the system to connect the Cisco IEC 4600 Series to the Cisco IEM. By default, the Server tab is displayed. If the Server tab is not displayed, click the **Server** tab.

**Figure 2-5**      **Server Tab**

**System**

Ethernet MAC: 00:21:11:00:20:6C  
 Serial number: 656015030192  
 Device name: SN656015030192  
 Device Description:   
 Device Location:

**Server**   Device   Remote channel

Management mode

☒ Managed by Cisco IE Manager (IEM)  
 IEM URL:   
☒ Get IEM server address from DHCP

☐ Stand-alone  
☐ Managed by Cisco Digital Media Manager (DMM)  
 DMM URL:

Apply   Close

- Step 4** Enter the device name in the **Device name** field. The name you choose will be used in the Cisco IEM to identify this device.



**Note** Only alphanumeric and underscores can be entered in the device name field.

- Step 5** Enter the device description in the **Device Description** field.
- Step 6** Enter the device location in the **Device Location** field.
- Step 7** Enter the Cisco IEM address in the **IEM URL** field or check the **Get IEM server address from DHCP** check box.
- Step 8** Click the **Managed by Cisco IE Manager (IEM)** radio button. The Account Details dialog box opens. The information entered here will be used to access the Cisco IEM. If you do not know this information, obtain it from the administrator who installed and configured the Cisco IEM.

- Step 9** Enter the account name in the **Account** field.

**Figure 2-6** *Account Details Dialog Box*

A screenshot of the 'Account Details' dialog box. It has a title bar with a Cisco logo and window controls. The form contains three input fields: 'Account:' with the text 'myaccount', 'User name:' with the text 'myusername', and 'Passsword:' with ten black dots. Below the password field is a checkbox labeled 'Show password' which is unchecked. A blue 'Register' button is located at the bottom right of the dialog.

- Step 10** Enter the user name in the **User name** field.
- Step 11** Enter the password in the **Password** field. To verify that you entered the correct password, check the **Show password** check box to view the password entered.
- Step 12** Click **Register**.
- Step 13** Once the account is registered, you will see the word "Success".

**Figure 2-7** *Registration Successful Notification*

A screenshot of the 'Account Details' dialog box after successful registration. The 'Account:' field still contains 'myaccount'. The 'User name:' and 'Passsword:' fields are now empty. The 'Show password' checkbox remains unchecked. A blue 'Reboot now' button is at the bottom right. The word 'Success' is displayed in a large, bold, black font in the bottom left area of the dialog.

- Step 14** Click **Reboot now**.
- Step 15** When you complete the selections in this window, click **Apply**.

- Step 16** To exit the System window, click **Close**.
- Step 17** In the System Settings window, click **Reboot**.

**Figure 2-8** Reboot Icon in the System Settings Window



The COBRA screen appears.

**Figure 2-9** COBRA Screen



Next you will connect the Cisco IEC 4600 Series to the Cisco IEM.

# Connecting to the Network

The Cisco IEC 4600 Series can be connected to the network using an Ethernet (wired) or wireless connection. Either can be configured using DHCP or entering an IP address.

By default, the IEC 4600 Series is configured to look for a DHCP-enabled Ethernet network. If you are connecting to another type of network (either static IP, Wireless, or both), you need to configure the network using the Emergency Configuration Mode as described in “Using Emergency Configuration Mode”. Once in Emergency Configuration Mode, click the Network icon and then proceed to either “Configuring an Ethernet Connection” or “Configuring a Wireless Connection”.

## Configuring an Ethernet (Wired) Connection

If you want to configure an Ethernet (wired) connection to the network using DHCP or a static IP address, follow these steps:

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Network** icon.

**Figure 2-10** Network Icon in System Settings Window



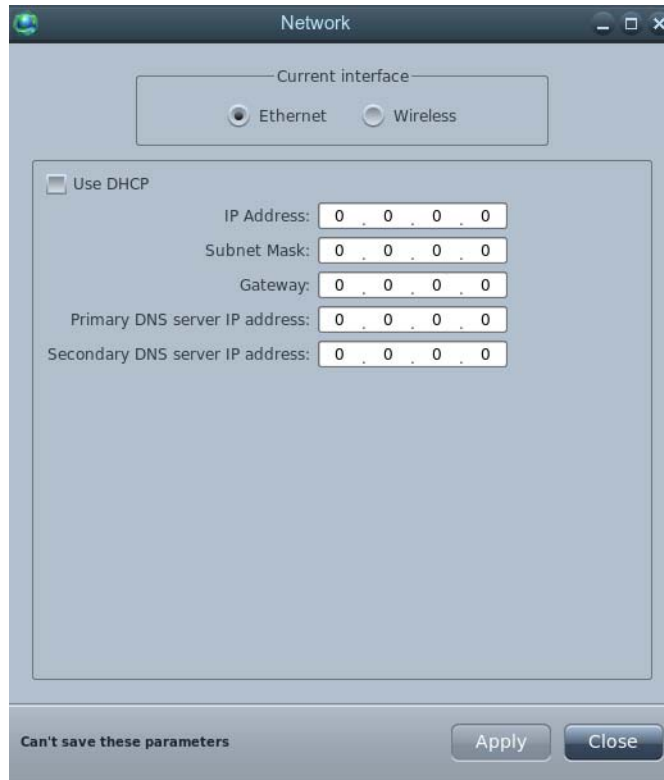
- Step 3** If Ethernet is not the current interface, click the **Ethernet** radio button.
- Step 4** Choose to use DHCP or a static IP address:  
To use DHCP, check the **Use DHCP** check box.

**Figure 2-11**      **Using DHCP**

To use a static IP address:

- a. Uncheck the Use DHCP check box.
- b. Enter the IP address in the **IP Address** field.
- c. Enter the subnet mask in the **Subnet Mask** field.
- d. Enter the gateway address in the **Gateway** field.
- e. Enter the primary DNS server's IP address in the **Primary DNS server IP Address** field.
- f. If there is a second DNS server, enter the secondary DNS server's IP address in the **Secondary DNS server IP Address** field.



**Figure 2-12** *Using a Static IP Address*

- Step 5** Click **Apply**.
- Step 6** To exit the Network window, click **Close**.
- Step 7** In the System Settings window, click **Reboot**.

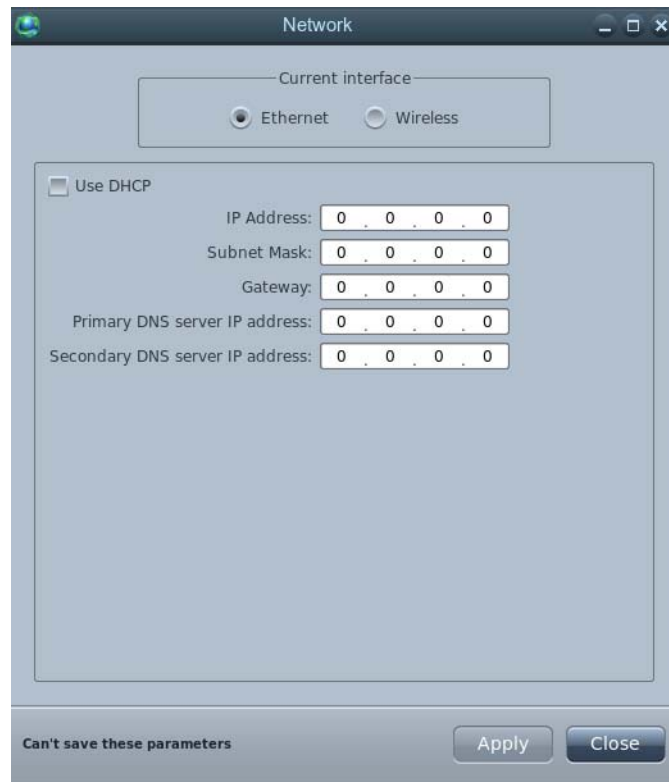
**Figure 2-13** *Reboot Icon in the System Settings Window*



If the network connection is changed, the Cisco IEC 4600 Series device's IP address will change. Record the new IP address.

- Step 8** If the DHCP check box is checked, uncheck the **Use DHCP** check box.

**Figure 2-14** Reboot Icon in System Settings Window



- Step 9** Click **Apply**.
- Step 10** Enter the IP address in the **IP Address** field.
- Step 11** Enter the subnet mask in the **Subnet Mask** field.
- Step 12** Enter the gateway address in the **Gateway** field.
- Step 13** Enter the primary DNS server's IP address in the **Primary DNS server IP Address** field.
- Step 14** If there is a second DNS server, enter the secondary DNS server's IP address in the **Secondary DNS server IP Address** field.
- Step 15** When you complete the selections in this window, click **Apply**.
- Step 16** To exit the Network window, click **Close**.
- Step 17** In the System Settings window, click **Reboot**.

**Figure 2-15** Reboot Icon in the System Settings Window



If you change the network connection, the Cisco IEC 4600 Series device's IP address will change. Be sure to record the new IP address.

## Configuring a Wireless Connection

If you want to configure a wireless connection to the network using DHCP or a static IP address, follow these steps:

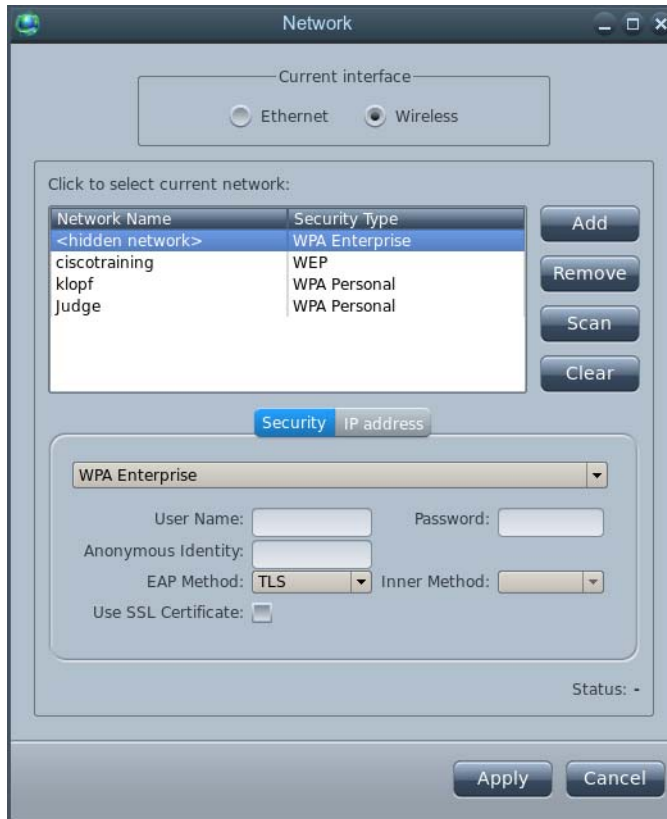
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Network** icon.

**Figure 2-16** Network Icon in System Settings Window

**Step 3** Click the **Wireless** radio button.

**Figure 2-17** Wireless Interface

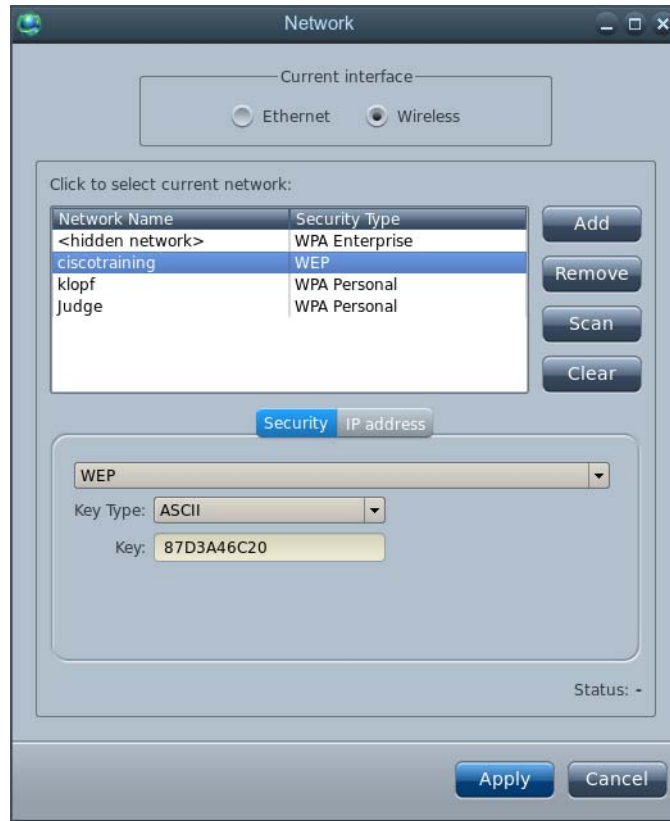
**Step 4** Click **Scan**.  
All the wireless networks detected are displayed.

**Figure 2-18** *Wireless Networks Detected*

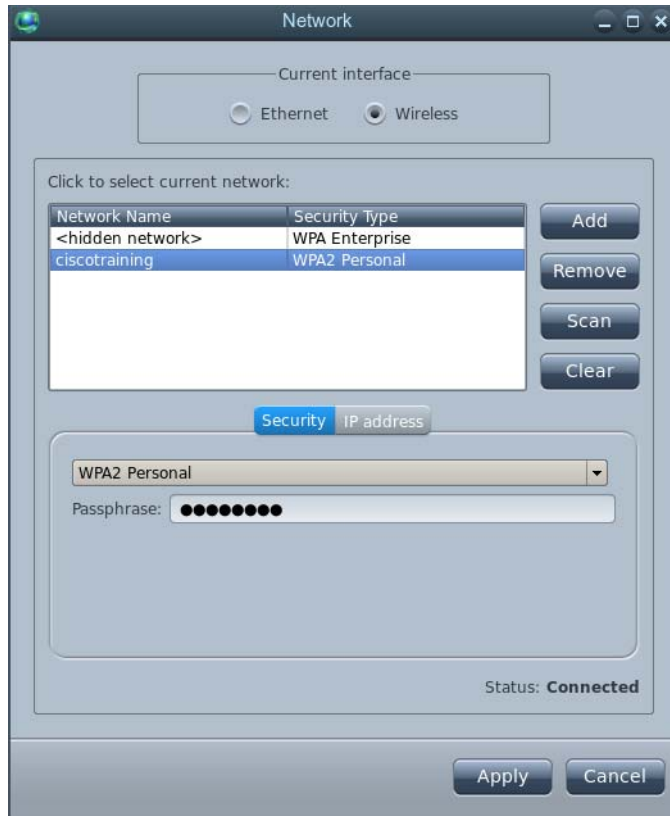
**Step 5** Click a network name to select a network.

**Step 6** In the Security tab, enter the information requested.

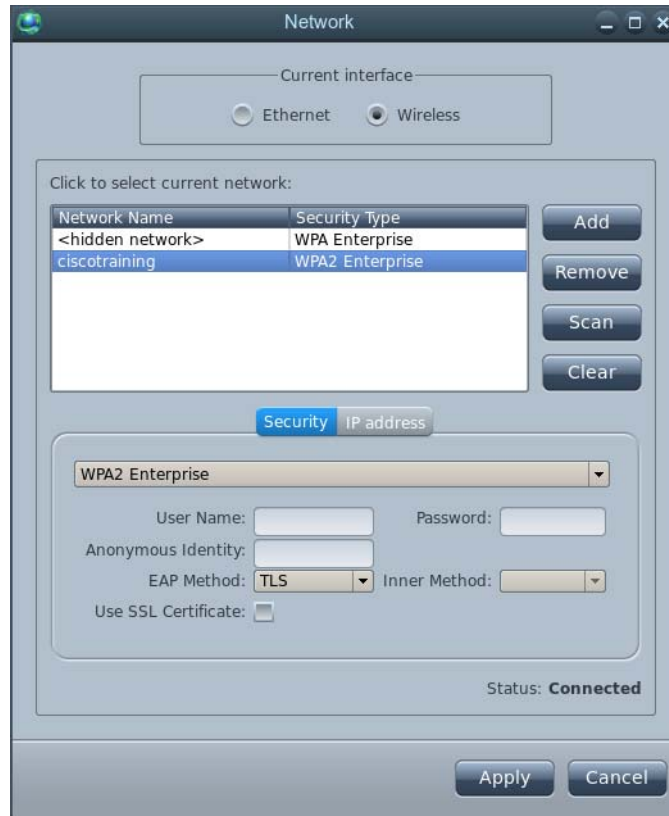
- If the security type is WEP:
  - From the Key Type drop-down list, choose **ASCII** or **HEX**.
  - Enter the key in the **Key** field

**Figure 2-19** WEP Security Key Field and Type Drop-Down List

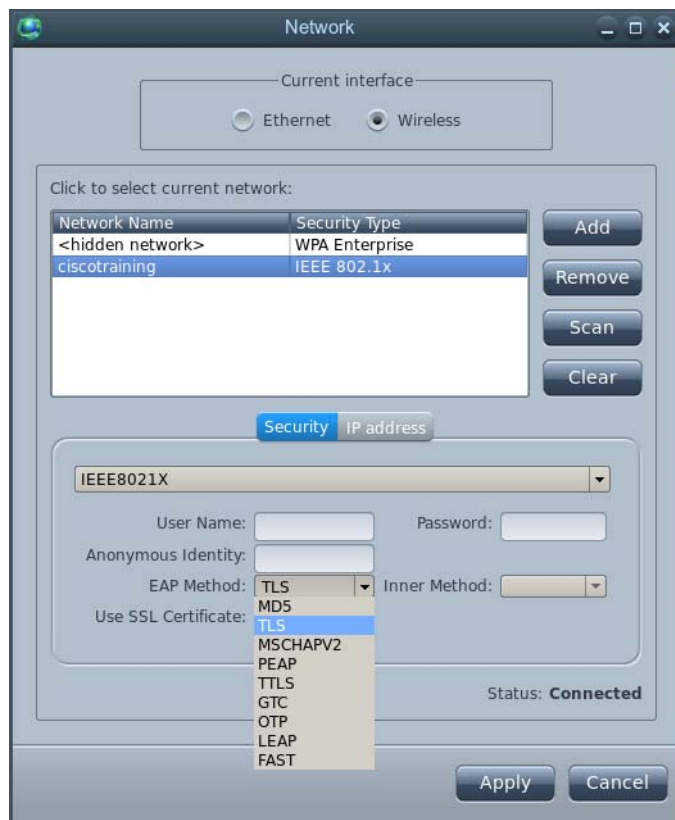
- If the security type is WPA Personal or WPA2 Personal:
  - Enter the passphrase in the **Passphrase** field.

**Figure 2-20 WPA2 Passphrase Field**

- If the security type is WPA Enterprise or WPA2 Enterprise:
  - Enter the user name in the **User Name** field.
  - Enter the password in the **Password** field.
  - Enter the anonymous identity in the **Anonymous Identity** field.
  - From the EAP Method drop-down list, choose the EAP method used.
  - From the Inner Method drop-down list, choose the inner method used.
  - If it requires a SSL certificate, check the **Use SSL Certificate** check box.

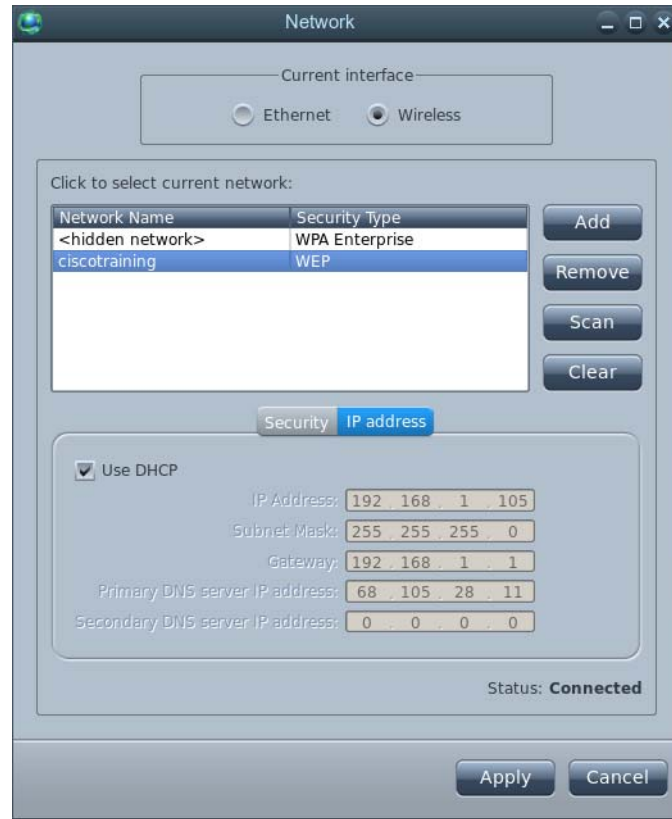
**Figure 2-21 WPA2 Security Fields, Drop-Down Lists, and Check Box**

- If the security type is IEEE802.1X:
  - Enter the user name in the **User Name** field.
  - Enter the password in the **Password** field.
  - Enter the anonymous identity in the **Anonymous Identity** field.
  - From the EAP Method drop-down list, choose the EAP method used.
  - From the Inner Method drop-down list, choose the inner method used.
  - If it requires a SSL certificate, check the **Use SSL Certificate** check box.

**Figure 2-22** IEEE802.1X Security Fields, Drop-Down Lists, and Check Box

**Step 7** Click the **IP address** tab.



**Figure 2-23 IP Address Tab**

**Step 8** Choose to use DHCP or a static IP address:

To use DHCP, check the **Use DHCP** check box.

To use a static IP address:

- a. Uncheck the **Use DHCP** check box.
- b. Enter the IP address in the **IP Address** field.
- c. Enter the subnet mask in the **Subnet Mask** field.
- d. Enter the gateway address in the **Gateway** field.
- e. Enter the primary DNS server's IP address in the **Primary DNS server IP Address** field.
- f. If there is a second DNS server, enter the secondary DNS server's IP address in the **Secondary DNS server IP Address** field.

**Step 9** Click **Apply**.

**Step 10** To exit the Network window, click **Close**.

**Step 11** In the System Settings window, click **Reboot**.

**Figure 2-24** Reboot Icon in the System Settings Window

If you change the network connection, the Cisco IEC 4600 Series device's IP address will change. Be sure to record the new IP address.

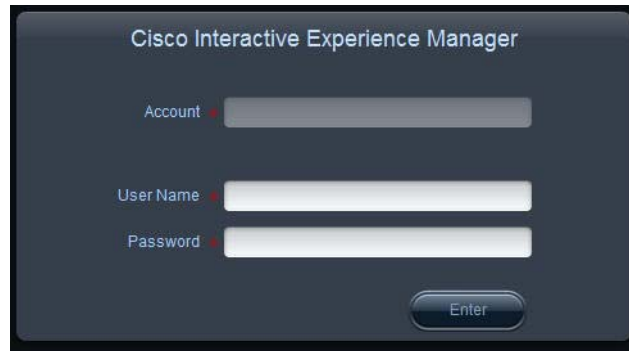
## Connecting to the Cisco IEM

This section assumes that either you or an administrator at your company has already installed and configured the Cisco IEM. If not, use the *Cisco Interactive Experience Platform Manager Install Guide* and *Cisco Interactive Experience Platform Manager User Guide* to install and configure Cisco IEM.

## Applying a Policy

The startup URL is the content that will be displayed on the kiosk. Follow these steps to apply a policy on the device so that the startup URL appears on the kiosk display.

- 
- Step 1** Open a browser on your computer.
  - Step 2** Enter the Cisco IEM URL.

**Figure 2-25 Cisco IEM Login**The image shows the Cisco Interactive Experience Manager (IEM) login interface. It has a dark blue background with the title "Cisco Interactive Experience Manager" at the top. Below the title are three input fields: "Account", "User Name", and "Password", each with a small red asterisk to its left. At the bottom right is a button labeled "Enter".

**Step 3** Enter the account name in the **Account** field.

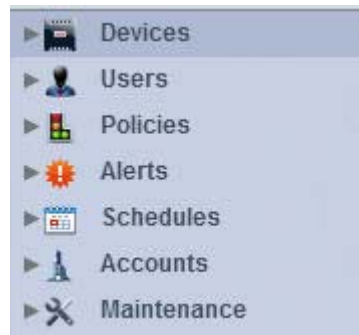
**Step 4** Enter the user name in the **User Name** field.

**Step 5** Enter the password in the **Password** field.

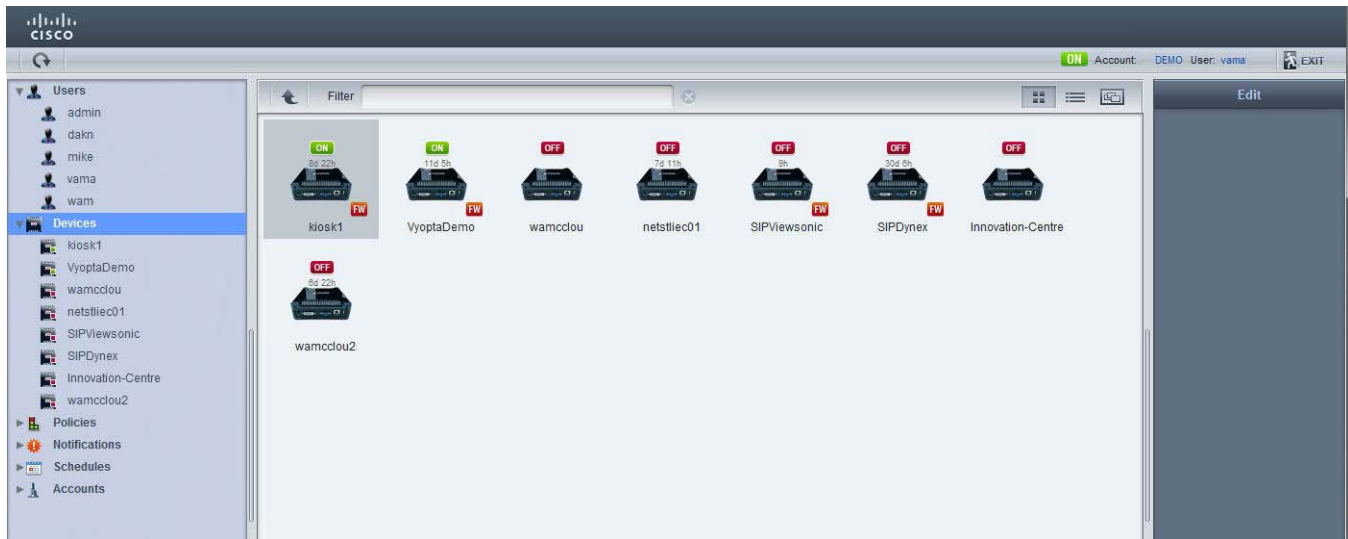
**Step 6** Click **Enter**.

After login, the Cisco IEM opens.

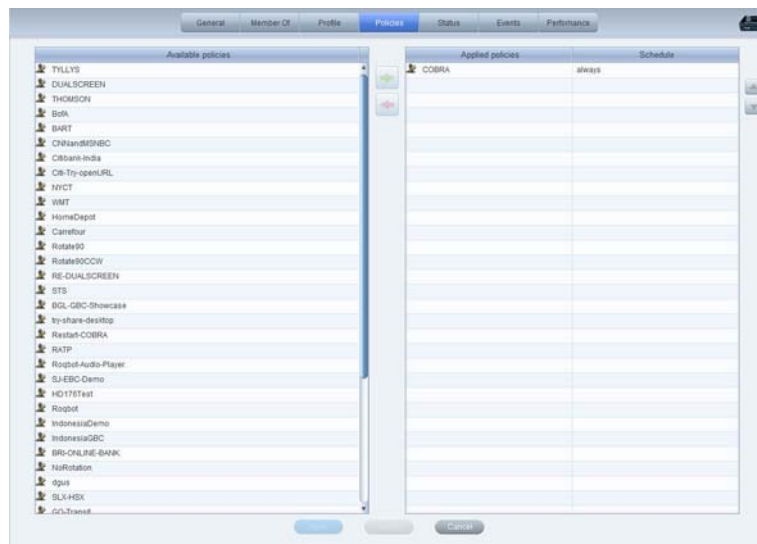
**Step 7** In the left pane, choose **Devices**.

**Figure 2-26 Devices**

**Step 8** Double-click the device's icon in the center pane.

**Figure 2-27** *Choosing a Device*

**Step 9** To get the startup URL, you need to apply a policy. Click the **Policies** tab.

**Figure 2-28** *Policies Tab*

**Step 10** Ask your administrator which policy you should apply.

**Step 11** From the Available policies list, choose the policy.

**Figure 2-29** *Available Policies*

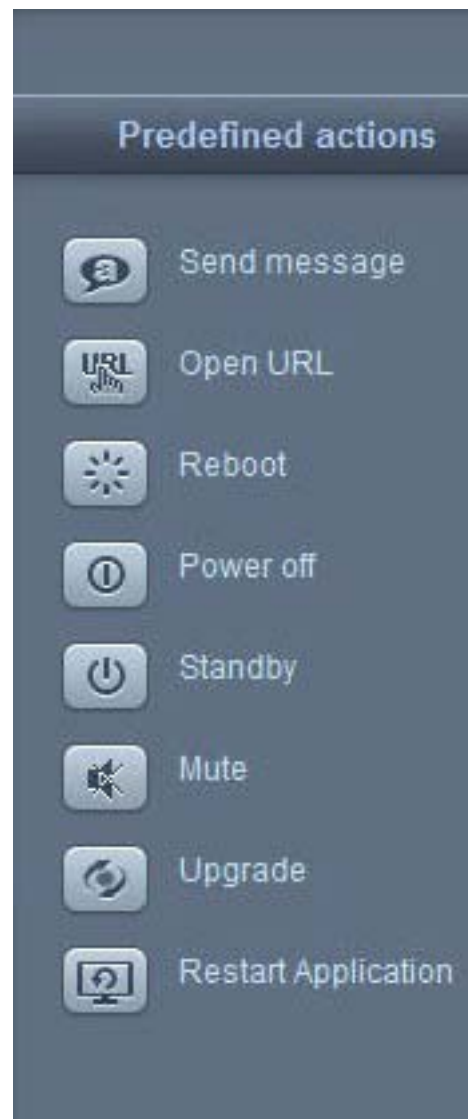
**Step 12** Click the **Green Arrow** to move that policy to the Applied policies list

**Figure 2-30 Applying a Policy**

You can select more than one policy at a time by pressing **Select** (for sequential policies) or **CTRL** (for non-sequential policies).

**Step 13** Click **Apply**.

**Step 14** In the right pane, click the Predefined actions to display the list of Predefined actions.

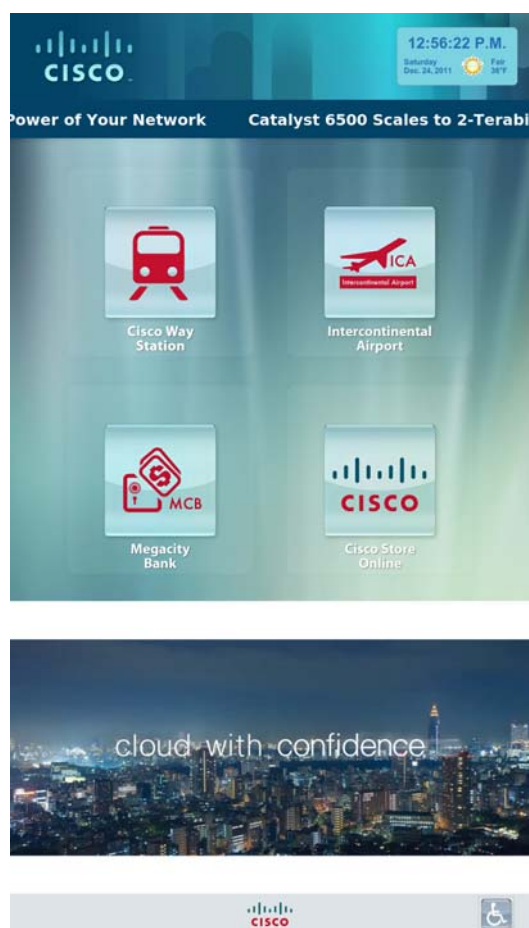
**Figure 2-31 Predefined Actions**

**Step 15** Click **Reboot**.

**Step 16** Click **Ok** in the Reboot Device dialog box to reboot the Cisco IEC 4600 Series.

**Figure 2-32** *Reboot Device Dialog Box*

The video display will now show the content from the startup URL. If you want to change how the startup URL appears, refer to the *Cisco Interactive Experience Manager Administrator Guide*.

**Figure 2-33** *Startup URL Content Displayed on the Kiosk Screen*

## Calibrating the Touchscreen

When the calibration screen appears, touch the crosses in the corners as instructed. For example, when the touchscreen is in portrait orientation, touch the screen in this order: top right, bottom right, top left, and bottom left.

You can calibrate the screen at any time. To calibrate the touchscreen, follow these steps:

- 
- Step 1** Press Ctrl-Alt-S to access the System Settings menu.

**Figure 2-34**     **System Settings Menu**



- Step 2** Click the **Calibrator** button.

The calibration utility will start. When it is finished, the startup URL content is displayed on the touchscreen.

---

## Using Emergency Configuration Mode



**Note**

Using the emergency configuration mode should be your last resort. This is primarily done if you do not have Internet access and you have tried to solve the issue to no avail. Consult the *Cisco Interactive Services Solution Troubleshooting Guide* first.

---

If the system hangs during the initialization process, enter the Emergency Configuration Mode to modify the configuration.

To use Emergency Configuration Mode, do the following:

---

- Step 1** Log into the IEM.

**Step 2** Click **Devices** in the left pane.

**Figure 2-35** *Devices Button*



**Step 3** Double-click on the device icon to display the tabs containing information about that particular device.

**Step 4** In the General tab, click on the **Maintenance Code** button.

**Figure 2-36** *Maintenance Code Button in General Tab*

A screenshot of the 'General' tab in a web application. At the top, there is a horizontal tab bar with seven tabs: 'General' (selected), 'Member Of', 'Profile', 'Policies', 'Status', 'Events', and 'Performance'. Below the tabs, the form displays various fields for a device. The 'Device Name' field is highlighted in yellow and contains the text 'ZS656015030045'. Below it, the 'Serial Number' field contains '656015030045'. The 'Maintenance Code' field has a 'Get' button next to it. Other fields include 'Product' (KAE), 'Model' (VX4602), 'Version' (4.111.251), 'User' (empty), 'Status' (ON, in a green box), 'Location' (empty), and 'Description' (empty text area).



**Figure 2-37 Maintenance Code General Tab**

General Member Of Profile Policies Status Events Performance

Device Name \* ZS656015030045

Serial Number 656015030045

Maintenance Code 0d16ae

Product KAE

Model VX4602

Version 4.111.251

User

Status **ON**

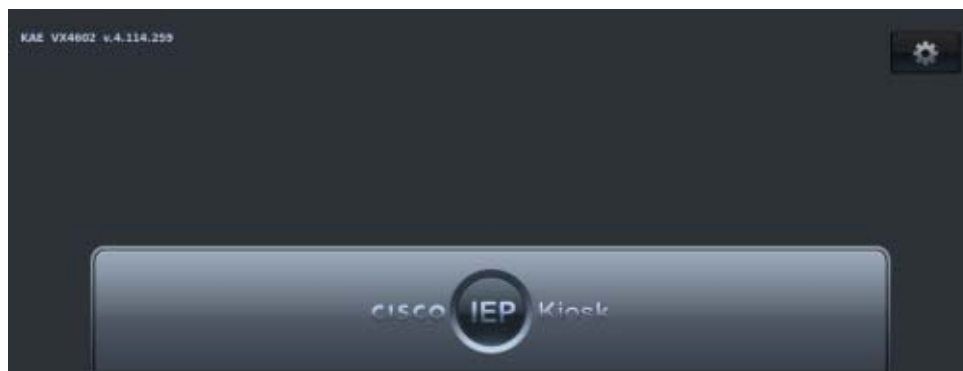
Location

Description

The maintenance code is displayed. Write down the code.

**Step 5** Go to the IEC 4600 Series.

**Step 6** Click on the gear button on the screen.

**Figure 2-38 Gear Button on Screen**

You will be prompted for an access code.

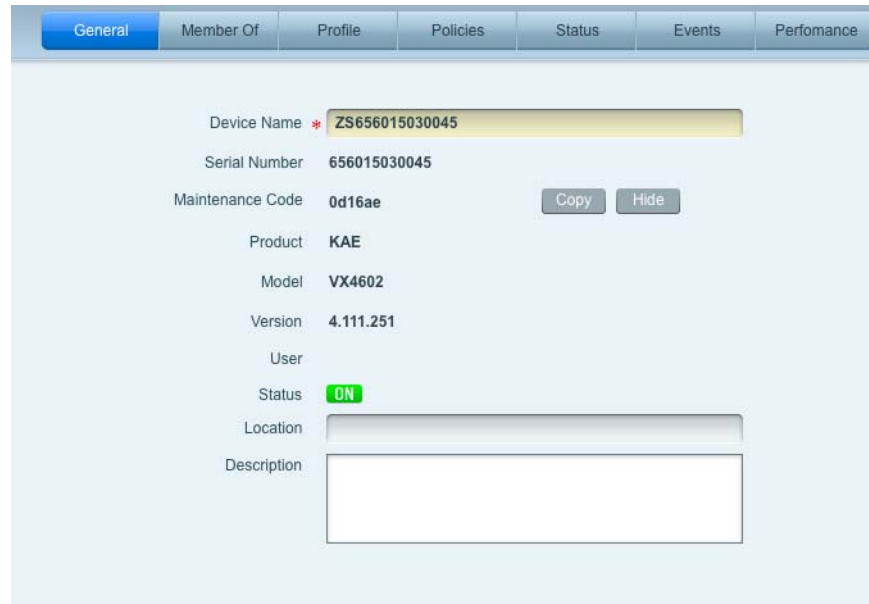
**Step 7** Enter the maintenance code.

## Using a VNC Viewer

The IEC can be accessed by a VNC viewer. VNC is enabled or disabled in the IEM. Refer to Chapter 5 of the *Cisco Interactive Experience Manager Administration Guide 2.1.1* for instructions on how to create a custom action for VNC and set the `remoteview.enabled` property in the IEM to 'true'.

You will need the IEC's Maintenance Code. It is entered as the password when prompted by the VNC viewer. The Maintenance Code can be found in the General Tab of the device.

**Figure 2-39** Maintenance Code in General Tab of Device



The screenshot shows the 'General' tab of an IEC device configuration page. The tabs at the top are General, Member Of, Profile, Policies, Status, Events, and Performance. The General tab is active. The fields and their values are: Device Name (ZS656015030045), Serial Number (656015030045), Maintenance Code (0d16ae), Product (KAE), Model (VX4602), Version (4.111.251), User (empty), Status (ON), Location (empty), and Description (empty). There are 'Copy' and 'Hide' buttons next to the Maintenance Code field.

Device Name	ZS656015030045
Serial Number	656015030045
Maintenance Code	0d16ae
Product	KAE
Model	VX4602
Version	4.111.251
User	
Status	ON
Location	
Description	

To use a VNC viewer to access an IEC, follow these steps:

- 
- Step 1** In the IEM, go to the IEC that you want to access using a VNC viewer.
  - Step 2** From the Custom actions menu, click the custom action that you created for VNC.
  - Step 3** When the VNC viewer opens, enter the IEC's Maintenance Code for the password.



**Note**

The password entered must be all upper case. If for example the Maintenance Code is 6A54F3, enter "6A54F3". The password will not work if you enter "6a54f3".

---



## CHAPTER 3

# Configuring Settings

---

Revised: January 29, 2014, OL-26457-05

## Chapter Overview



### Note

The IEC 4600 Series should be configured from the IEM by applying policies and configuring its profile. This chapter is only for configuration of a single IEC that is not connected to an IEM such as for demo purposes.

This chapter explains how to use the System Settings menu to configure the IEC 4600 Series settings for the network, proxy, and system. It also explains how to sort logs and reboot the IEC.

The topics in this chapter include the following:

- [Network Settings, page 3-2](#)
  - [Configuring an Ethernet Connection using DHCP, page 3-2](#)
  - [Configuring an Ethernet Connection using a Static IP Address, page 3-4](#)
  - [Configuring a Wireless Connection using DHCP, page 3-6](#)
  - [Configuring a Wireless Connection using a Static IP Address, page 3-14](#)
- [Proxy Server Settings, page 3-21](#)
  - [Static Option, page 3-21](#)
  - [Autoconfiguration Script Option, page 3-23](#)
  - [Autoconfiguration URL Option, page 3-25](#)
- [System Settings, page 3-27](#)
  - [Setting Management Mode, page 3-27](#)
  - [Setting Stand-Alone Mode, page 3-30](#)
  - [Changing the IEM's URL, page 3-32](#)
- [System Logs, page 3-37](#)
  - [Sorting Logs, page 3-38](#)
  - [Enabling the Debug Mode, page 3-42](#)
- [Reboot, page 3-43](#)

# Network Settings

The Cisco IEC 4600 Series can be connected to the network using an Ethernet (wired) or wireless connection. Either can be configured using DHCP or an IP address.

## Configuring an Ethernet Connection using DHCP

If you want to configure an Ethernet (wired) connection to your network using DHCP, follow these steps:

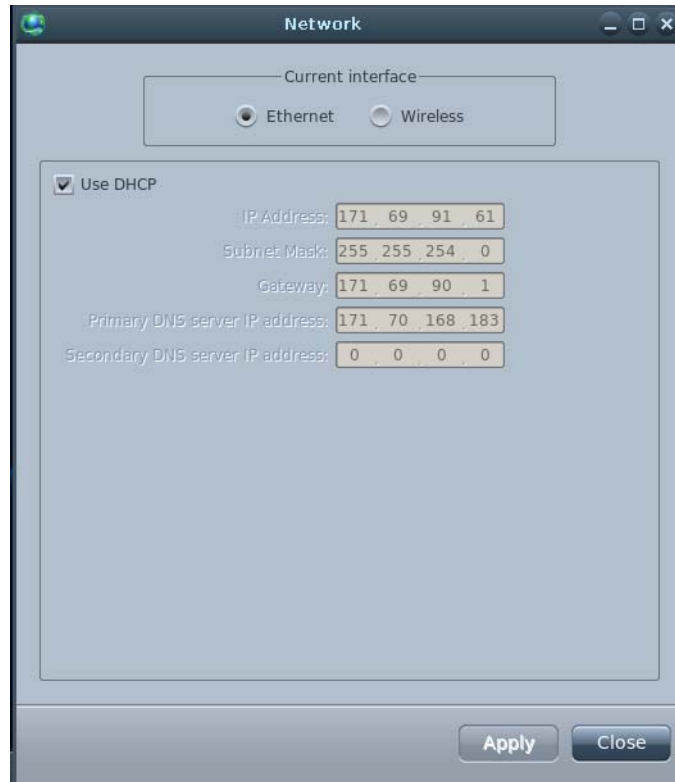
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Network** icon.

**Figure 3-1** Network Icon in System Settings Window



- Step 3** If Ethernet is not the current interface, click on the **Ethernet** radio button.
- Step 4** If the DHCP check box is not checked, check the **Use DHCP** check box.

**Figure 3-2**      *Use DHCP Check Box*



- Step 5**      Click **Apply**.
- Step 6**      To exit the Network window, click **Close**.
- Step 7**      In the System Settings window, click **Reboot**.

**Figure 3-3** Reboot Icon in the System Settings Window



If you change the network connection, the Cisco IEC 4600 Series device's IP address will change. Be sure to record the new IP address.

## Configuring an Ethernet Connection using a Static IP Address

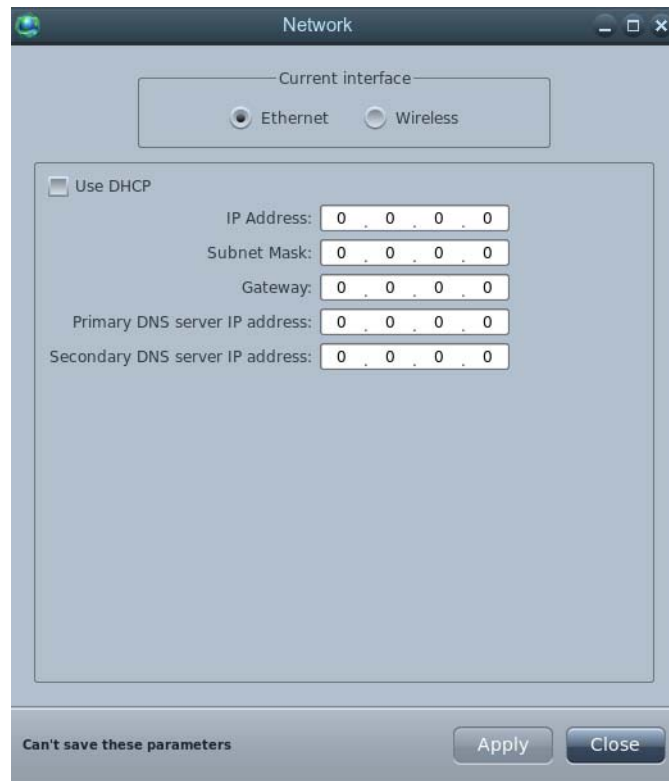
If you want to configure an Ethernet (wired) connection to your network using a static IP address, follow these steps:

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
  - Step 2** Click the **Network** icon.

**Figure 3-4** Network Icon in System Settings Window

**Step 3** If Ethernet is not the current interface, click on the **Ethernet** radio button.

**Step 4** If the DHCP check box is checked, uncheck the **Use DHCP** check box.

**Figure 3-5** Use DHCP Check Box

**Step 5** Click **Apply**.

**Step 6** Enter the IP address in the **IP Address** field.

- Step 7** Enter the subnet mask in the **Subnet Mask** field.
- Step 8** Enter the gateway address in the **Gateway** field.
- Step 9** Enter the primary DNS server's IP address in the **Primary DNS server IP Address** field.
- Step 10** If there is a second DNS server, enter the secondary DNS server's IP address in the **Secondary DNS server IP Address** field.
- Step 11** When you complete the selections in this window, click **Apply**.
- Step 12** To exit the Network window, click **Close**.
- Step 13** In the System Settings window, click **Reboot**.

**Figure 3-6** Reboot Icon in the System Settings Window



If you change the network connection, the Cisco IEC 4600 Series device's IP address will change. Be sure to record the new IP address.

## Configuring a Wireless Connection using DHCP

If you want to configure a wireless connection to your network using DHCP, follow these steps:

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Network** icon.



**Figure 3-7** Network Icon in System Settings Window



**Step 3** Click the **Wireless** radio button.

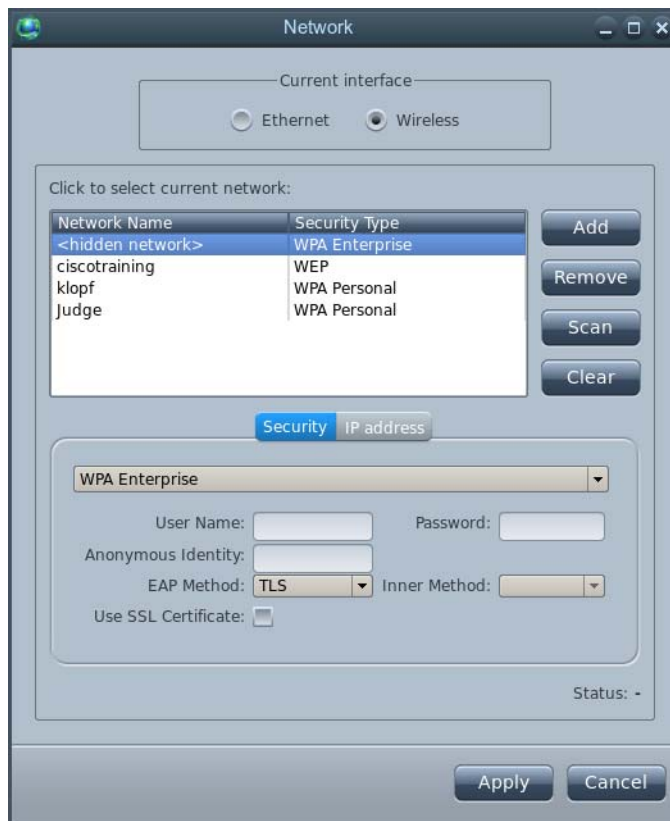
**Step 4** Click **Scan**.

**Figure 3-8** Scan Button



**Step 5** Click on a network name to select a network.

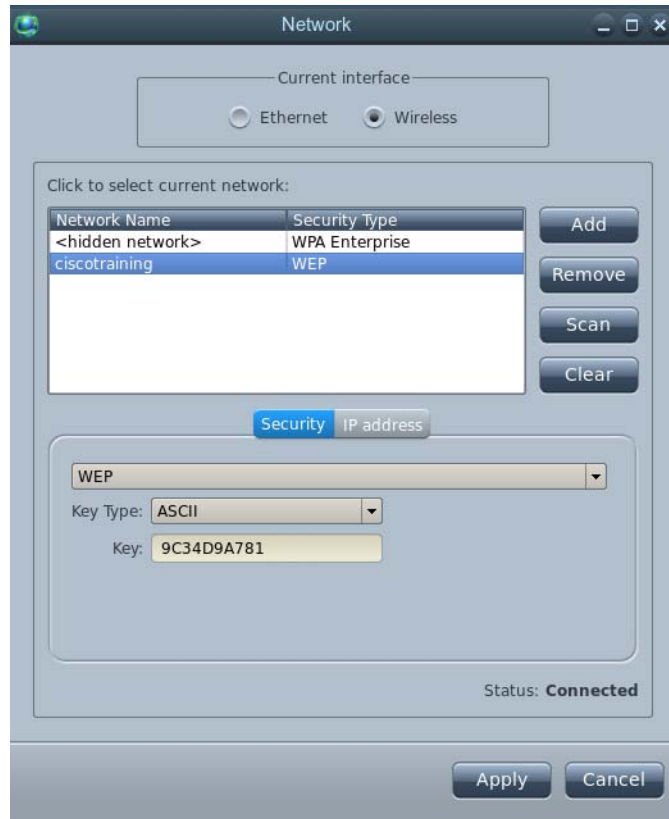
**Figure 3-9**



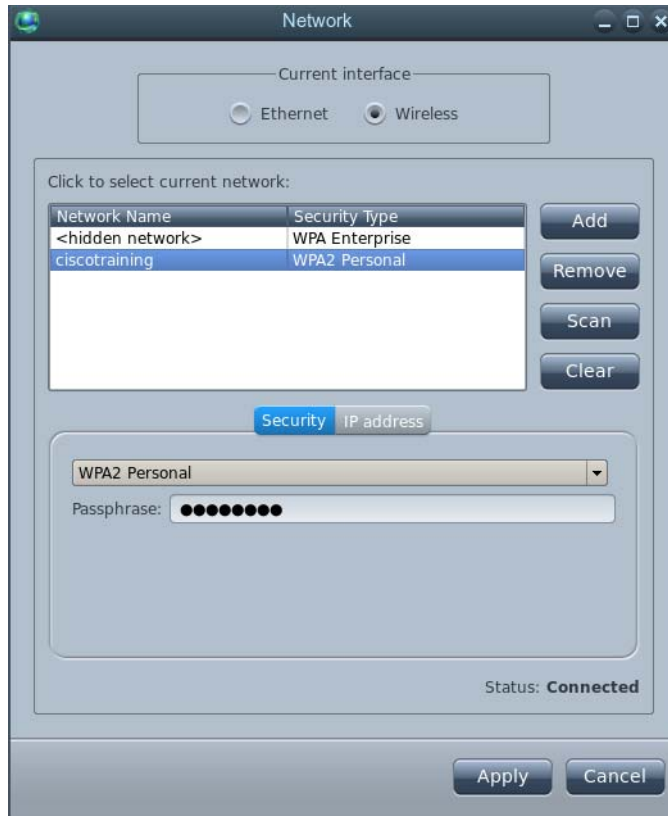
**Step 6** In the Security tab, enter the information requested.

- If the security type is WEP:
  - From the Key Type drop-down list, choose **ASCII** or **HEX**.
  - Enter the key in the **Key** field.

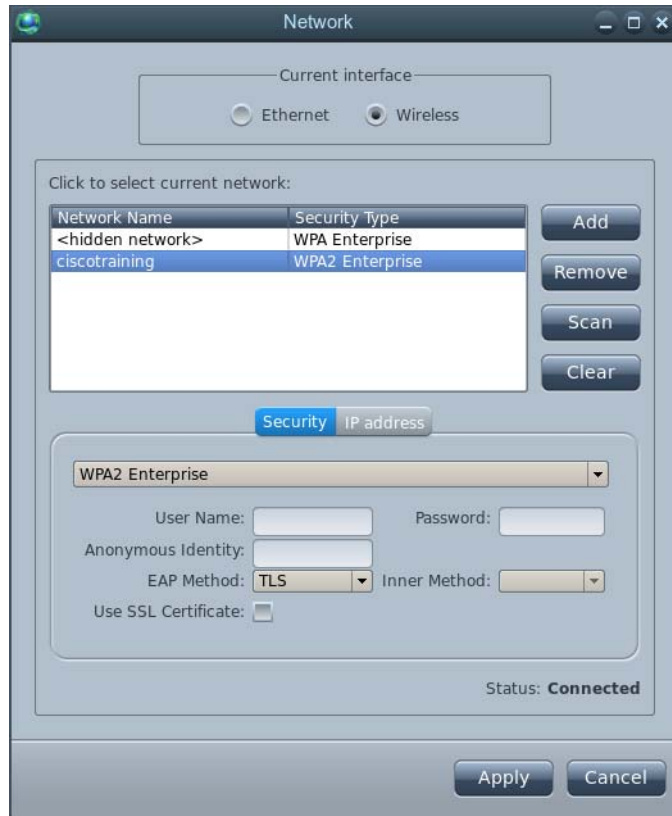
**Figure 3-10** WEP Security Key Field and Type Drop-Down List



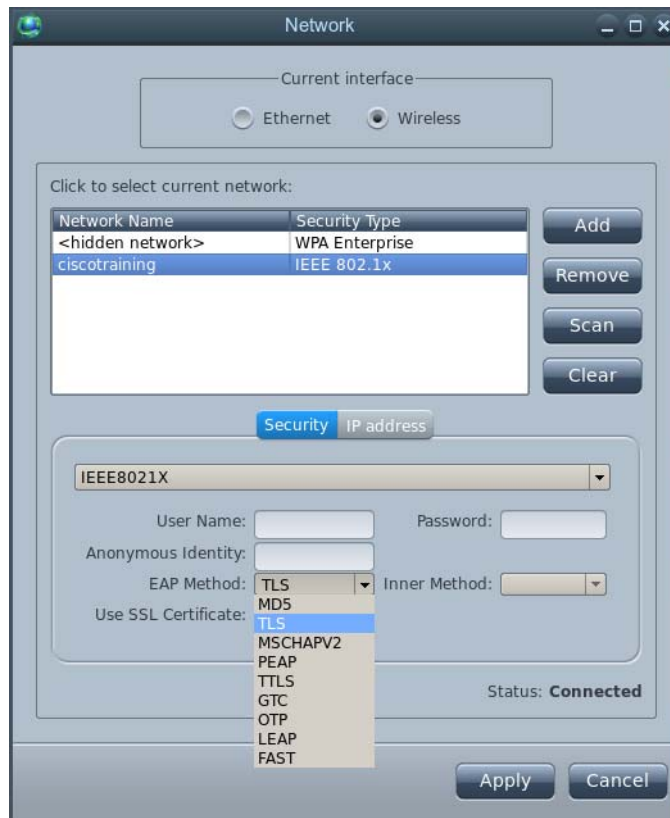
- If the security type is WPA Personal or WPA2 Personal:
  - Enter the passphrase in the **Passphrase** field.

**Figure 3-11 WPA2 Passphrase Field**

- If the security type is WPA Enterprise or WPA2 Enterprise:
  - Enter the user name in the **User Name** field.
  - Enter the password in the **Password** field.
  - Enter the anonymous identity in the **Anonymous Identity** field.
  - From the EAP Method drop-down list, choose the EAP method used.
  - From the Inner Method drop-down list, choose the inner method used.
  - If it requires a SSL certificate, check the **Use SSL Certificate** check box.

**Figure 3-12 WPA2 Security Fields, Drop-Down Lists, and Check Box**

- If the security type is IEEE802.1X:
  - Enter the user name in the **User Name** field.
  - Enter the password in the **Password** field.
  - Enter the anonymous identity in the **Anonymous Identity** field.
  - From the EAP Method drop-down list, choose the EAP method used.
  - From the Inner Method drop-down list, choose the inner method used.
  - If it requires a SSL certificate, check the **Use SSL Certificate** check box.

**Figure 3-13** IEEE802.1X Security Fields, Drop-Down Lists, and Check Box

**Step 7** Click on the **IP address** tab.

**Figure 3-14** IP Address Tab

- Step 8** If the DHCP check box is not checked, check the **Use DHCP** check box.
- Step 9** Click **Apply**.
- Step 10** To exit the Network window, click **Close**.
- Step 11** In the System Settings window, click **Reboot**.

**Figure 3-15** Reboot Icon in the System Settings Window



If you change the network connection, the Cisco IEC 4600 Series device's IP address will change. Be sure to record the new IP address.

## Configuring a Wireless Connection using a Static IP Address

If you want to configure a wireless connection to your network using a static IP address, follow these steps:

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Network** icon.



**Figure 3-16** Network Icon in System Settings Window

**Step 3** Click the **Wireless** radio button.

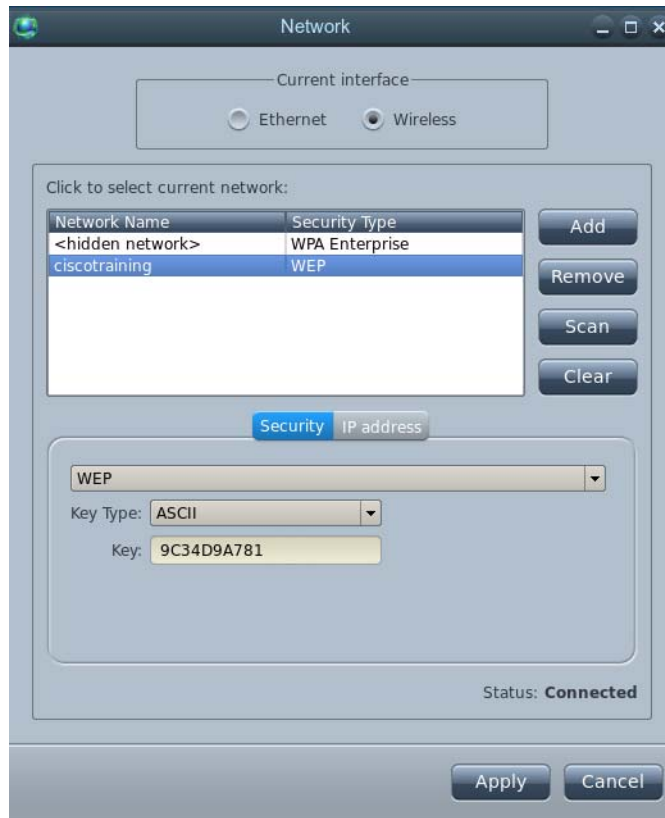
**Step 4** Click **Scan**.

**Figure 3-17** Scan Button

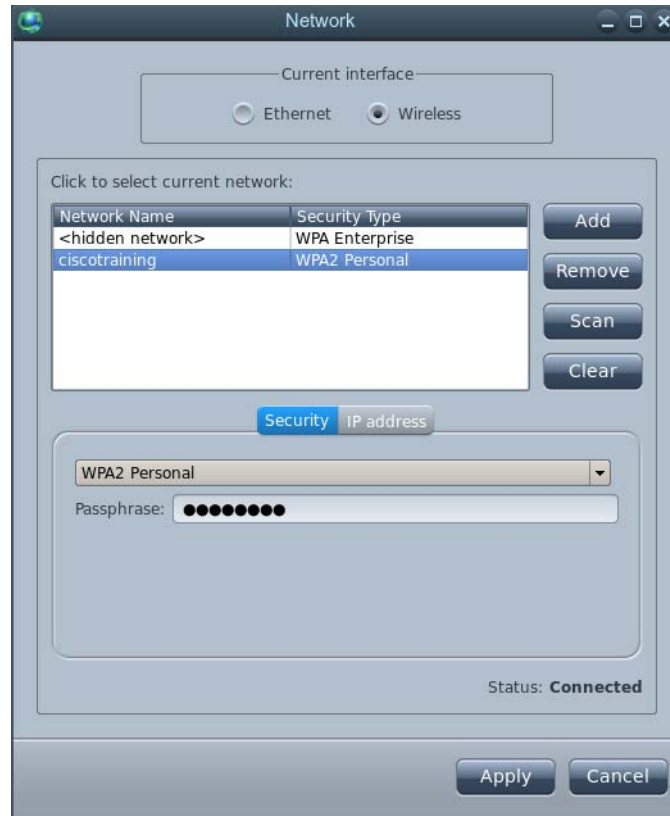
**Step 5** Click on a network name to select a network.

- Step 6** In the Security tab, enter the information requested.
- If the security type is WEP:
    - From the Key Type drop-down list, choose **ASCII** or **HEX**.
    - Enter the key in the **Key** field.

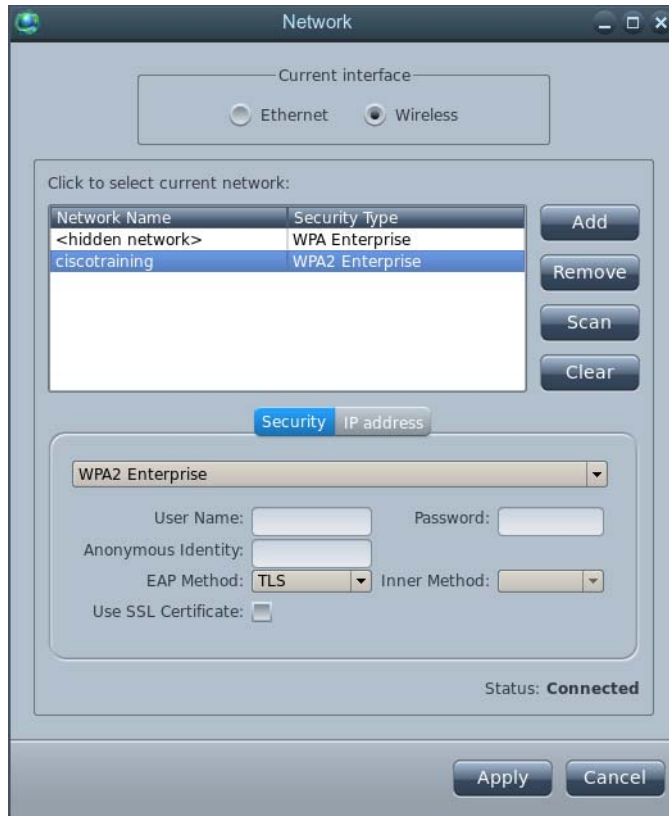
**Figure 3-18** WEP Security Key Field and Type Drop-Down List



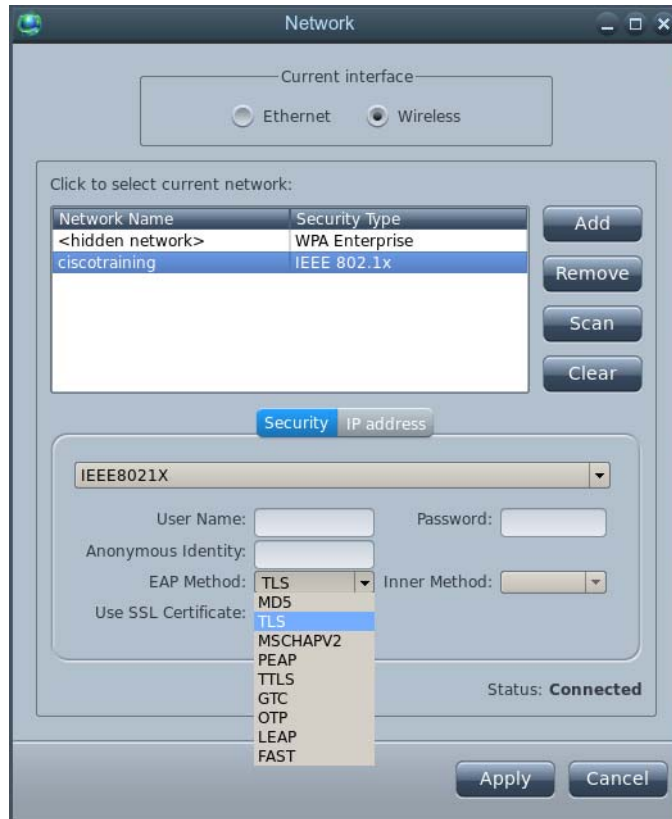
- If the security type is WPA Personal or WPA2 Personal:
  - Enter the passphrase in the **Passphrase** field.

**Figure 3-19 WPA2 Passphrase Field**

- If the security type is WPA Enterprise or WPA2 Enterprise:
  - Enter the user name in the **User Name** field.
  - Enter the password in the **Password** field.
  - Enter the anonymous identity in the **Anonymous Identity** field.
  - From the EAP Method drop-down list, choose the EAP method used.
  - From the Inner Method drop-down list, choose the inner method used.
  - If it requires a SSL certificate, check the **Use SSL Certificate** check box.

**Figure 3-20 WPA2 Security Fields, Drop-Down Lists, and Check Box**

- If the security type is IEEE802.1X:
  - Enter the user name in the **User Name** field.
  - Enter the password in the **Password** field.
  - Enter the anonymous identity in the **Anonymous Identity** field.
  - From the EAP Method drop-down list, choose the EAP method used.
  - From the Inner Method drop-down list, choose the inner method used.
  - If it requires a SSL certificate, check the **Use SSL Certificate** check box.

**Figure 3-21** IEEE802.1X Security Fields, Drop-Down Lists, and Check Box

**Step 7** Click on the **IP address** tab.

**Figure 3-22 IP Address Configuration Fields**

The screenshot shows a 'Network' configuration window. At the top, there's a 'Current interface' section with radio buttons for 'Ethernet' and 'Wireless'. Below this is a table for selecting a network. The table has two columns: 'Network Name' and 'Security Type'. The first row is '<hidden network>' with 'WPA Enterprise'. The second row is 'ciscotraining' with 'WEP'. To the right of the table are buttons: 'Add', 'Remove', 'Scan', and 'Clear'. Below the table are two tabs: 'Security' and 'IP address'. The 'IP address' tab is selected. Under this tab, there's a 'Use DHCP' checkbox which is unchecked. Below it are five input fields for IP addresses, each with a dotted decimal format: 'IP Address', 'Subnet Mask', 'Gateway', 'Primary DNS server IP address', and 'Secondary DNS server IP address'. All fields are currently set to '0 . 0 . 0 . 0'. At the bottom right of the IP configuration section, it says 'Status: Connected'. At the very bottom of the window are 'Apply' and 'Cancel' buttons.

Network Name	Security Type
<hidden network>	WPA Enterprise
ciscotraining	WEP

Buttons: Add, Remove, Scan, Clear

Tabs: Security, IP address

Use DHCP: ☐

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Primary DNS server IP address: 0 . 0 . 0 . 0

Secondary DNS server IP address: 0 . 0 . 0 . 0

Status: Connected

Buttons: Apply, Cancel

- Step 8** If the DHCP check box is checked, uncheck the **Use DHCP** check box.
- Step 9** Enter the IP address in the **IP Address** field.
- Step 10** Enter the subnet mask in the **Subnet Mask** field.
- Step 11** Enter the gateway address in the **Gateway** field.
- Step 12** Enter the primary DNS server's IP address in the **Primary DNS server IP Address** field.
- Step 13** If there is a second DNS server, enter the secondary DNS server's IP address in the **Secondary DNS server IP Address** field.
- Step 14** When you complete the selections in this window, click **Apply**.
- Step 15** To exit the Network window, click **Close**.
- Step 16** In the System Settings window, click **Reboot**.

**Figure 3-23** Reboot Icon in the System Settings Window



If you change the network connection, the Cisco IEC 4600 Series device's IP address will change. Be sure to record the new IP address.

## Proxy Server Settings

The proxy settings only apply to standalone mode. If you are in standalone mode, you can enable a proxy server.

There are four configuration options:

- Disabled
- Static
- Autoconfiguration script
- Autoconfiguration URL

By default, the proxy server is disabled.

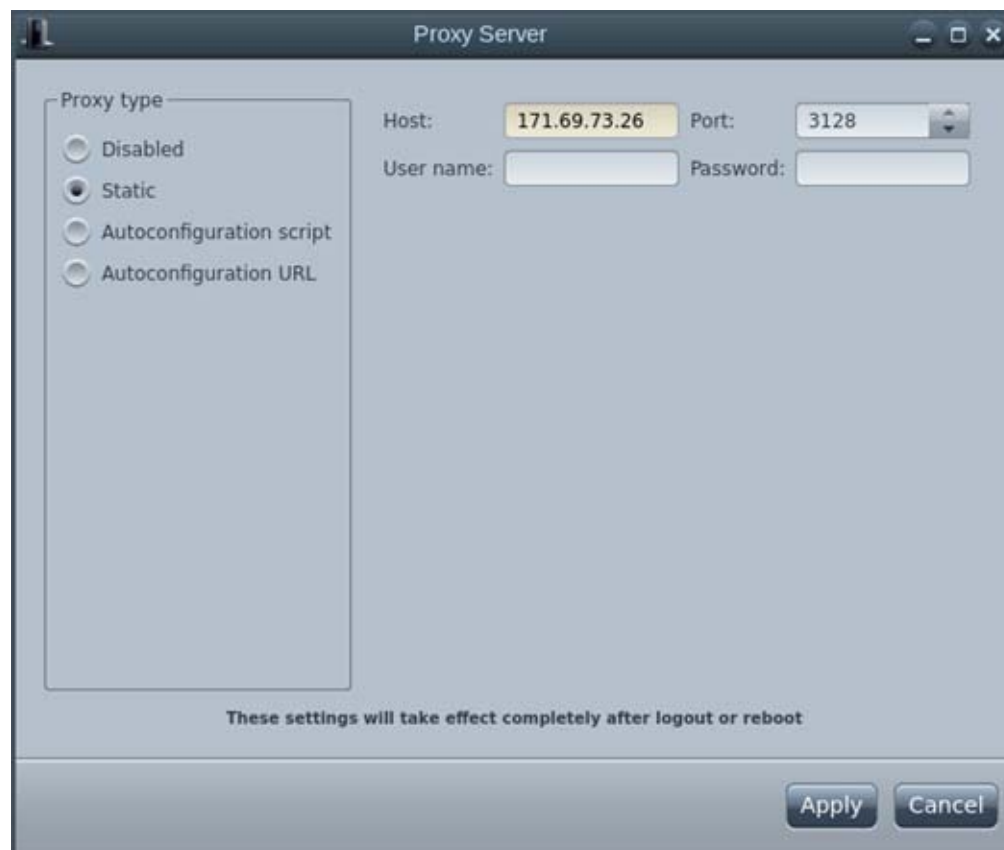
## Static Option

Follow these steps to enable a proxy server using the static option:

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** If the IEC is managed by an IEM, enter its maintenance code.
- Step 3** Click the **Proxy Server** icon.

**Figure 3-24** Proxy Server Icon in System Settings Window

**Step 4** In the Proxy Server dialog box, choose the **Static** radio button as proxy type.

**Figure 3-25** Proxy Server Dialog Box

**Step 5** Enter the host address in the Host field.



- Step 6** Set the port number by using the arrows or entering a value in the Port field.
- Step 7** Enter the user name in the User name field.
- Step 8** Enter the password in the Password field.
- Step 9** When you complete the selections in this window, click **Apply**.
- Step 10** To exit the Proxy Server window, click **Close**.
- Step 11** In the System Settings window, click **Reboot**.

**Figure 3-26** Reboot Icon in the System Settings Window



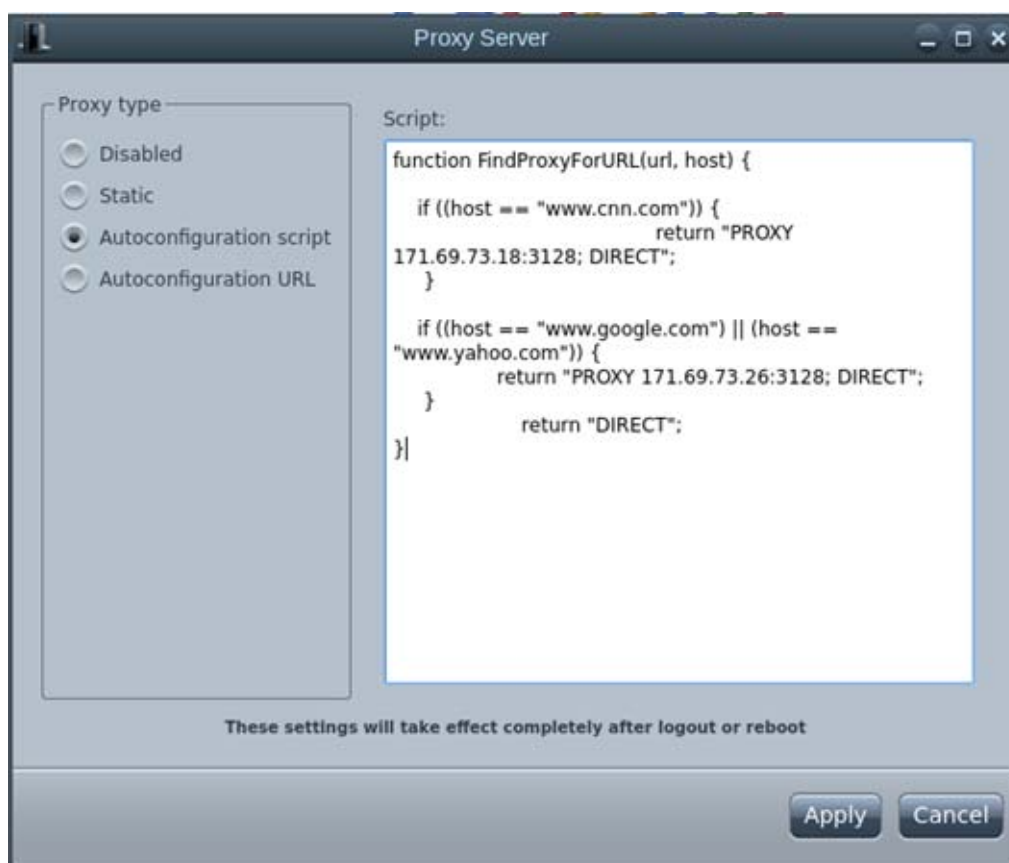
## Autoconfiguration Script Option

Follow these steps to enable a proxy server using an autoconfiguration script:

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** If the IEC is managed by an IEM, enter its maintenance code.
- Step 3** Click the **Proxy Server** icon.

**Figure 3-27** Proxy Server Icon in System Settings Window

**Step 4** In the Proxy Server dialog box, choose the **Autoconfiguration script** radio button as proxy type.

**Figure 3-28** Proxy Server Dialog Box

**Step 5** Enter the proxy script in the Script field.

- Step 6** Click **Apply**.
- Step 7** To exit the Proxy Server window, click **Close**.
- Step 8** In the System Settings window, click **Reboot**.

**Figure 3-29** Reboot Icon in the System Settings Window



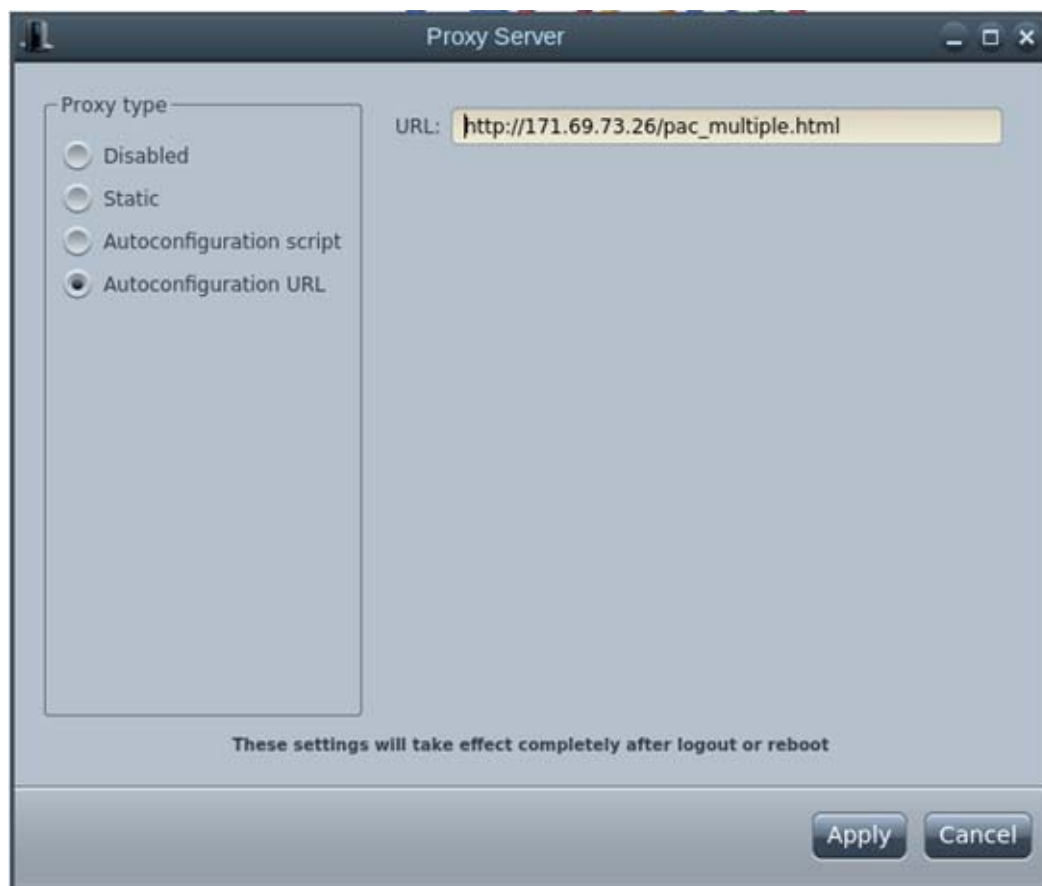
## Autoconfiguration URL Option

Follow these steps to enable a proxy server using an autoconfiguration URL:

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** If the IEC is managed by an IEM, enter its maintenance code.
- Step 3** Click the **Proxy Server** icon.

**Figure 3-30** Proxy Server Icon in System Settings Window

**Step 4** In the Proxy Server dialog box, choose the **Autoconfiguration URL** radio button as proxy type.

**Figure 3-31** Proxy Server Dialog Box

- Step 5** Enter the URL of the PAC file or web server in the URL field.
- Step 6** Click **Apply**.
- Step 7** To exit the Proxy Server window, click **Close**.
- Step 8** In the System Settings window, click **Reboot**.

**Figure 3-32** Reboot Icon in the System Settings Window



## System Settings

There are three tabs in the System settings window: Server, Device, and LAN. To configure the system, you will need the Cisco IEM URL. If you do not know the URL, contact the administrator in your company who installed and configured the Cisco IEM.

## Setting Management Mode

In managed mode, the IEC 4600 Series is configured and controlled remotely. Managed mode facilitates consistency and is the recommended (and default) mode.

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **System** icon.

**Figure 3-33** System Icon in System Settings Window

Now you will configure the system to connect the Cisco IEC 4600 Series device to the Cisco IEM.

- Step 3** Enter the device name in the **Device name** field. The name you choose will be used in the Cisco IEM to identify this device.

**Figure 3-34** System Dialog Box

- Step 4** Enter the device description in the **Device Description** field.

- Step 5** Enter the device location in the **Device Location** field.

- Step 6** Enter the Cisco IEM address in the **IEM URL** field.
- Step 7** Click the **Managed by Cisco IE Manager (IEM)** radio button. The Account Details dialog box opens. The information entered here will be used to access the Cisco IEM. If you do not know this information, obtain it from the administrator who installed and configured the Cisco IEM.
- Step 8** Enter the account name in the **Account** field.

**Figure 3-35** Account Details Dialog Box



The screenshot shows a dialog box titled "Account Details". It has a standard window title bar with minimize, maximize, and close buttons. The dialog contains three input fields: "Account:" with the text "myaccount", "User name:" with the text "myusername", and "Password:" with masked characters (dots). Below the password field is a checkbox labeled "Show password" which is currently unchecked. At the bottom right of the dialog is a button labeled "Register".

- Step 9** Enter the user name in the **User name** field.
- Step 10** Enter the password in the **Password** field. To verify that you entered the correct password, check the **Show password** check box to see the characters entered.
- Step 11** Click **Register**.
- Step 12** Once the account is registered, you will see the word "Success".

**Figure 3-36** Registration Successful Notification



**Step 13** Click **Reboot now**.

---

## Setting Stand-Alone Mode

If you will not use the Cisco IEM to manage the kiosk, configure the Cisco IEC 4600 Series using the stand-alone mode.



### Warning

**If you have already registered a Cisco IEM account, choosing stand-alone will unregister that account.**

---

**Step 1** Press **Ctrl-Alt-S** to display the System Settings window.

**Step 2** Click the **System** icon.



**Figure 3-37** System Icon in System Settings Window

**Step 3** Enter the device name in the **Device name** field.

**Figure 3-38** System Dialog Box

**Step 4** Enter the device description in the **Device Description** field.

**Step 5** Enter the device location in the **Device Location** field.

**Step 6** Click the **Stand-alone** radio button.

- Step 7** Enter the account name in the **Account** field.
- Step 8** Enter the user name in the **User name** field.
- Step 9** Enter the password in the **Password** field. To verify that you entered the correct password, check the **Show password** check box to see the characters entered.
- Step 10** Click **Unregister**.
- Step 11** To exit the System window, click **Close**.
- Step 12** In the System Settings window, click **Reboot**.

**Figure 3-39** *Reboot icon in the System Settings Window*



## Changing the IEM's URL

There may be times when you need to change the IEM's URL in the IEC to a different IEM URL such as when the IEC is used for demos that use multiple instances of IEMs. If you need to change the IEM's URL in the IEC, follow the steps below.

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **System** icon.

**Figure 3-40** System Icon in System Settings Window

**Step 3** Click the **Stand-alone** radio button.

**Figure 3-41** System Dialog Box

**Step 4** Enter the account name in the **Account** field.

**Step 5** Enter the user name in the **User name** field.

**Step 6** Enter the password in the **Password** field. To verify that you entered the correct password, check the **Show password** check box to see the characters entered.

- Step 7** Click **Unregister**.
- Step 8** Enter the new IEM address in the **IEM URL** field.
- Step 9** Click the **Managed by Cisco IE Manager (IEM)** radio button.  
The Account Details dialog box opens.
- Step 10** Enter the account name for the new IEM in the **Account** field.

**Figure 3-42** Account Details Dialog Box



- Step 11** Enter the user name in the **User name** field.
- Step 12** Enter the password in the **Password** field. To verify that you entered the correct password, check the **Show password** check box to see the characters entered.
- Step 13** Click **Register**.
- Step 14** Once the account is registered, you will see the word "Success".

**Figure 3-43** Registration Successful Notification



- Step 15** Click **Reboot now**.
- Step 16** To exit the System window, click **Close**.
- Step 17** In the System Settings window, click **Reboot**.

**Figure 3-44** Reboot Icon in the System Settings Window



## Resetting the Device

The Cisco IEC 4600 Series can be reset to factory settings at any time.

There are two methods for resetting the device to factory settings:

1. Insert a pin in the Reset hole on the side of the IEC and hold it for five seconds.
2. Click the **Reset to defaults** button in the Device tab. Follow the steps below to reset the device to factory settings using this option.

**Step 1** Press **Ctrl-Alt-S** to display the System Settings window.

**Step 2** Click the **System** icon.

**Figure 3-45** System Icon in System Settings Window



**Step 3** Click the **Device** tab.

**Figure 3-46**      **Device Tab**

**Step 4**      Click **Reset to defaults**. The Reset dialog box opens.

**Step 5**      Click **Yes**.

**Figure 3-47**      **Reset Dialog Box**

## System Logs

The System Logs window displays all the data collected since the device was last powered on. The Cisco IEC 4600 Series is a stateless device so if the device is unplugged or loses power, the data is lost.

You can sort data five ways:

- **Severity** – You can sort by level of severity from highest to lowest: critical, error, warning, notice, information, debug.

- Time – You can sort by when the data was collected.
- Application – You can sort by the type of component.
- Process identifier (PID) – You can sort by the process identifier (PID), the unique number assigned to every process running in the system.
- Message – You can sort by message types.

## Sorting Logs

Follow these steps to sort the log entries:

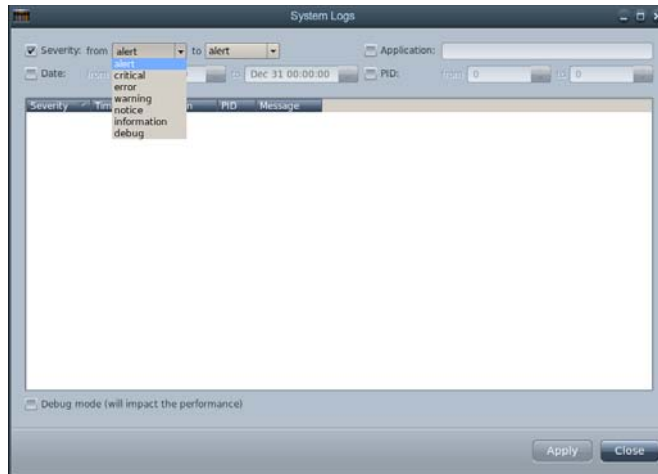
- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **System Logs** icon.

**Figure 3-48** System Logs Icon in System Settings Window



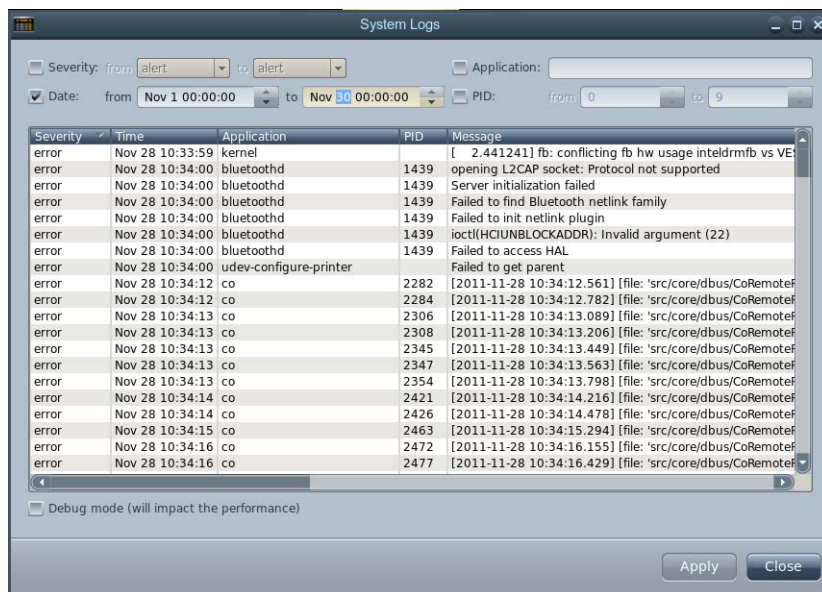
- Step 3** Click on check boxes and enter required values or information to sort the log entries.
- To sort by severity:
    - Check the **Severity** check box.
    - From the Severity from drop-down list, choose the highest level of severity desired.
    - From the Severity to drop-down list, choose the lowest level of severity desired.



**Figure 3-49** Severity Check Box and Drop-Down Lists**Tip**

If you want the three highest levels of severity, choose Alert for the “from” drop down and choose Error for the “to” drop down. If you reversed the choices and choose Error for the “from” drop down and choose Alert for the “to” drop down nothing would display. If no logs display after you have chosen levels of severity, make sure that you are choosing from highest level to lowest level not lowest level to highest level. If no logs still display, there may not be logs yet for those levels. To clear the entry, uncheck the **Severity** check box. Scroll through the list of data to see if anything was logged for those levels. If not, you can reset those levels. If the levels are logged, reset those levels in reverse order.

- To sort by Date:
  - Check the **Date** check box.
  - From the Date from drop-down, choose the earlier date in the “from” field by either pressing the **Up Arrow** or **Down Arrow** to pick a value or manually entering the date and time.
  - Choose the later date in the “to” field.

**Figure 3-50** Date Check Box and Fields

- The majority of applications that you can sort by are daemon processes in Linux. If you are familiar with Linux, follow these steps to sort by applications:
  - Check the **Application** check box.
  - Enter one of the application names below in the **Application** field. Make sure that you are entering it exactly as shown here; the names are case-sensitive.

/usr/sbin/cron

CRON

acpid

avahi-daemon

bluetoothd

co

dhclient

dmmd

kernel

management-daemon-system

ntpd

ntpd\_intres

ntpddate

replicator

rsyslogd

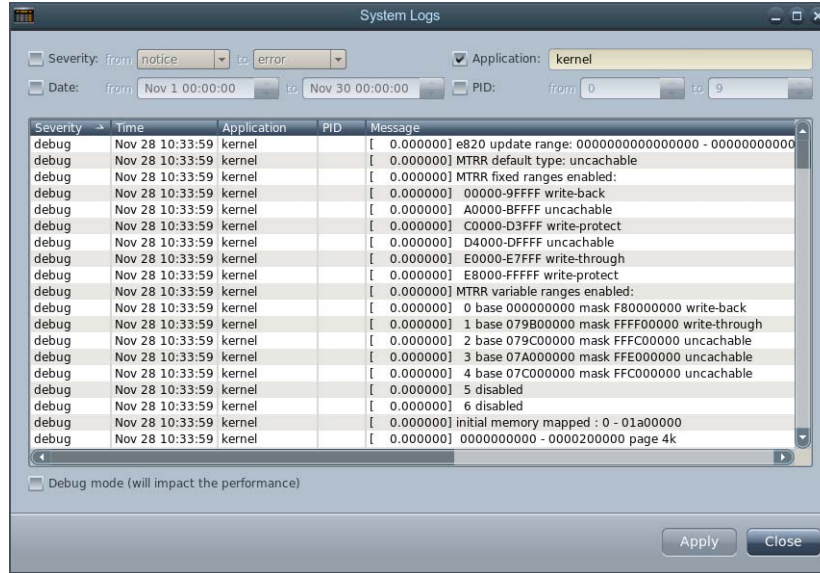
sconsole

scrmon

sshd

udev-configure-printer  
wpa\_supplicant

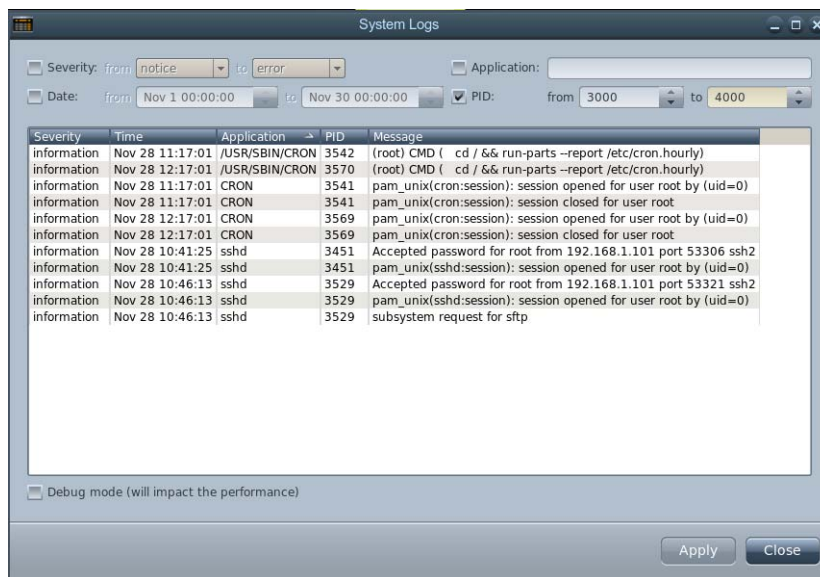
**Figure 3-51 Application Check Box and Field**



**Tip**

If no logs appear after you have entered one of the above application names, uncheck the **Application** check box and search for a log event of that application type. If there are log events for that application, check the **Application** check box and re-enter the application name making sure that you are entering it exactly as shown in the log.

- To sort by PID:
  - Check the **PID** check box.
  - Enter the lowest PID number desired into the “from” field by either pressing the **Up Arrow** or **Down Arrow** to pick a value or manually entering the date and time.
  - Enter the highest PID number desired into the “to” field.

**Figure 3-52** PID Check Box and Fields

- Step 4** If you want to keep how the entries are sorted for the next time you access the logs, click **Close**. If you want all entries to display the next time you access the logs, uncheck all the check boxes and then Click **Close**.

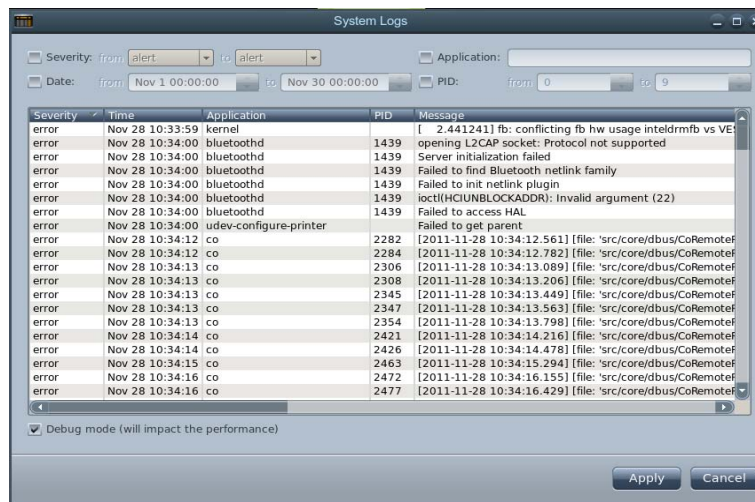
## Enabling the Debug Mode

The Debug mode can be enabled. Since debugging is an application that runs in the background, it will affect performance of the Cisco IEC 4600 Series if it is enabled. To enable the Debug mode, follow these instructions:

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **System Logs** icon.

**Figure 3-53** System Logs Icon in System Settings Window

**Step 3** Check the **Debug mode** check box.

**Figure 3-54** Debug Mode Check Box

**Step 4** Click **Apply**.

**Step 5** To exit the System Logs window, click **Close**.

## Reboot

The **Reboot** icon is used to reboot the Cisco IEC 4600 Series after any changes to settings.

**Step 1** Press **Ctrl-Alt-S** to display the System Settings window.

**Step 2** In the System Settings window, click **Reboot**.

**Figure 3-55** *Reboot Icon in the System Settings Window*





## CHAPTER 4

# Off-Line Caching

---

Revised: January 29, 2014, OL-26457-05

## Chapter Overview

This chapter identifies how to enable aggressive caching on an IEC.

Topics in this chapter include:

- [Off-Line Caching, page 4-1](#)
  - [Configuring Property Settings in the IEM to Enable Aggressive Caching, page 4-1](#)

## Off-Line Caching

The user can set properties within a device profile or applied policy that enables aggressive caching on an IEC. As a result, content is cached by the IEC so that if the IEC becomes off-line (connection to the startup URL is lost), it can still display content that users previously had interacted with before going off-line.



### Note

Content that was not interacted with before the IEC goes off-line will not be cached and thus not visible to users. For example, if users only move an interactive map to the east and to the north of the central coordinates, after the IEC goes off-line, the west and south portions of the map will not be visible to users.

Only static page content is cached. Images and embedded videos are also cached. Dynamic page content is NOT cached. For example, news ticker content may not display at some point if the news ticker is being constantly updated.

In order to activate aggressive caching, you must first configure the media and web property settings in the IEC's device profile or an applied policy within the IEM. Videos played on the video player are cached in the media cache. Web page content is cached in the web cache.

## Configuring Property Settings in the IEM to Enable Aggressive Caching

Follow the steps below to configure property settings.

- Step 1** Log into the IEM.
- Step 2** If you want to configure property settings just for one IEC, go to the IEC's profile. Otherwise, create a new policy or access an existing policy that is applied to the IECs that you want to enable aggressive caching.
- Step 3** In the profile or policy, find the **browser** property and expand it to show the cache property within it.

**Figure 4-1 Browser Property**

Property	Compatibility	Value	Description
▶ application			
▶ audio			
▼ browser	•		
▶ appearance	•		
▶ application			
▶ cache			

- Step 4** Expand the **cache** property to show the media and web properties within it.

**Figure 4-2 Cache Property**

Property	Compatibility	Value	Description
▶ appearance	•		
▶ application			
▼ cache			
▶ maximum			
▶ media			
▶ web			

- Step 5** Expand the **media** property to show the enabled and mode properties within it.

**Figure 4-3 Media Property**

Property	Compatibility	Value	Description
▶ maximum			
▼ media			
▶ clear		false	Clear media cache
▶ enabled		true	Enable media cache
▶ mode		Check if content is expired	Media content caching mode
▶ size		2048	Media cache size in megabytes

- Step 6** Set the enabled property to **true** to enable media caching.
- Step 7** Set the mode property to **Content never expires**.
- Step 8** (Optional) Set the cache size for media.
- Step 9** Expand the **web** property to show the enabled and mode properties within it.



**Figure 4-4 Web Property**

▼ web			
enabled		false	Enable web cache
mode		Prefer cache	Web content caching mode
size		1024	Web cache size in megabytes

**Step 10** Set the enabled property to **true** to enable web caching.

**Step 11** Choose either **Prefer cache** or **Always cache** for the mode property.

**Note**

If you did not cache all the content that your application requires, when in off-line mode the content will not be loaded from the network when your application requests it. Instead you will see the “Service temporarily unavailable” error message.”

**Note**

If you need to cache web content to be able to use it later in the off-line mode, you must load that content with the web cache mode set to any value except **Always cache**. Afterwards, set this value to **Always cache** or **Prefer cache**.

**Step 12** (Optional) Set the web cache size.

**Step 13** Click **Apply**.

**Step 14** If you created a new policy for aggressive caching, apply it to the devices.





## CHAPTER 5

# Upgrading the IEC

---

Revised: January 29, 2014, OL-26457-05

## Chapter Overview

This chapter identifies how to upgrade the firmware.

Both methods of upgrading explained here are intended for incremental upgrades. The IEC's settings will not be modified using either method.

Topics in this chapter include:

- [IEC Firmware Upgrade Using the IEM, page 5-1](#)
  - [Saving XML Files, page 5-8](#)
- [IEC Firmware Upgrade Using the Terminal Utility, page 5-10](#)



**Warning**

---

**Before upgrading an IEC to version 2.1.1, ensure that the software version of the IEM is 2.1.1.**

---

## IEC Firmware Upgrade Using the IEM

You will need the following files that can be downloaded from [www.cisco.com](http://www.cisco.com):

- System file
- Application file
- Specification file



**Tip**

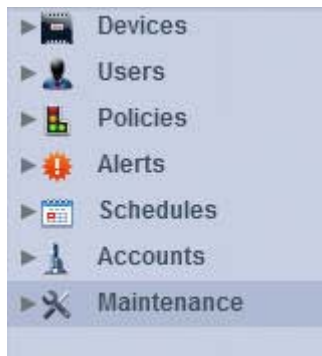
---

It is recommended that only one version is active.

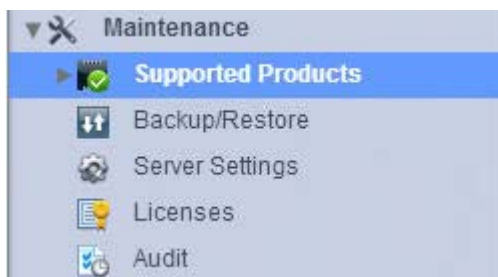
---

**Step 1**

In the left pane of the IEM, click **Maintenance**.

**Figure 5-1 Maintenance Button**

**Step 2** Click **Supported Products**

**Figure 5-2 Supported Products Button**

**Step 3** Click **IEC**.

**Figure 5-3 Product Name in the Left Pane**

**Step 4** Click **4600**.

**Figure 5-4 Model Name in the Left Pane**

**Step 5** Go to the Edit menu in the right pane and click **Versions**.

**Figure 5-5** Versions Button in the Edit Menu

A list of versions is displayed in the center pane.

**Figure 5-6** List of Versions

Version	Build	System Image	Applications Image	Specification	Active
2.1.0	5.40.55	Wed Aug 14 2013	Wed Aug 14 2013	Wed Aug 14 2013	Yes

If the version (build) listed is the desired version, proceed to the “Administrators” section of this chapter. If a different or newer version should be loaded or no versions are listed, continue this step set.

You will need the following files:

- System file
- Application file
- Specification file

**Step 6** Click **New Firmware** in the Edit menu.

The Add firmware dialog box opens.

**Figure 5-7** Add Firmware Dialog Box

**Step 7** In the New firmware version fields, enter the latest version number.

**Step 8** Click **Ok**.

**Step 9** Make sure that you have the following files available on your desktop:

- System file
- Application file
- Specification file

**Note**

If specification file is incorrectly saved to your desktop, it will report 'Specification is not found' when uploading to the IEM. See "Saving XML Files" in this chapter to learn how to save this XML file to your desktop correctly.

**Step 10** In the System Image column, click +.

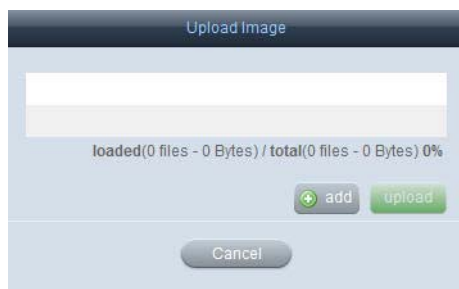
**Figure 5-8 Add Image Button**

Version	System Image
4.96.180	Wed Jul 27 2011  
4.97.187	Tue Aug 2 2011  
4.97.188	Tue Aug 2 2011  
4.98.191	 

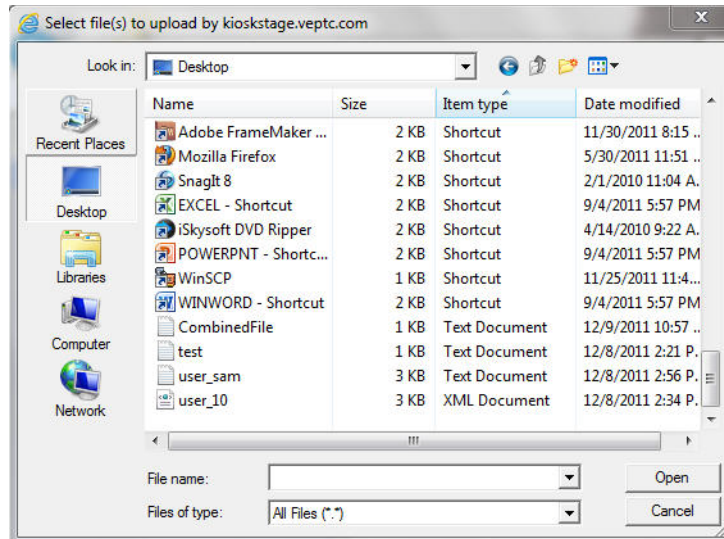
The Upload Image dialog box opens.

**Step 11** Click +add.

**Figure 5-9 Upload Image Dialog Box**



**Step 12** Find the file on your desktop and click **Open**.

**Figure 5-10** *Select Files Dialog Box*

The file appears in the Upload Image dialog box.

**Figure 5-11** *System File in Upload Image Dialog Box*

**Step 13** Click **upload**.

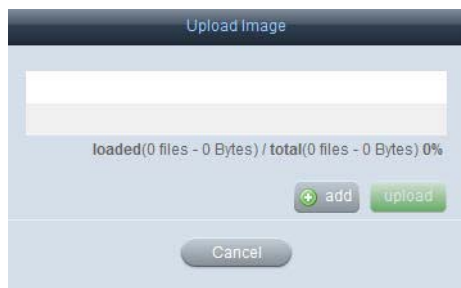
The file will appear in the System Image list.

**Step 14** In the Application column, click **+**.

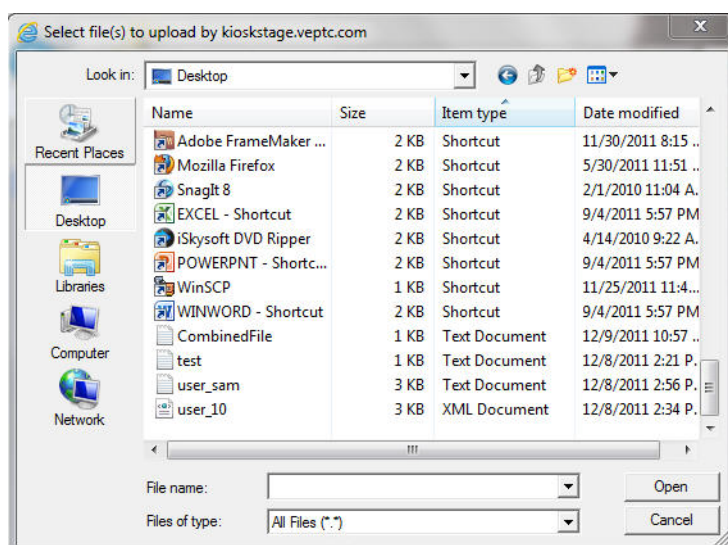
**Figure 5-12** *Add Image Button*

The Upload Image dialog box opens.

**Step 15** Click **+add**.

**Figure 5-13 Upload Image Dialog Box**

**Step 16** Find the file on your desktop and click **Open**.

**Figure 5-14 Select Files Dialog Box**

The file appears in the Upload Image dialog box.

**Figure 5-15 Application File in Upload Image Dialog Box**

**Step 17** Click **upload**.

The file will appear in the Applications Image list.

**Step 18** In the Specification column, click +.



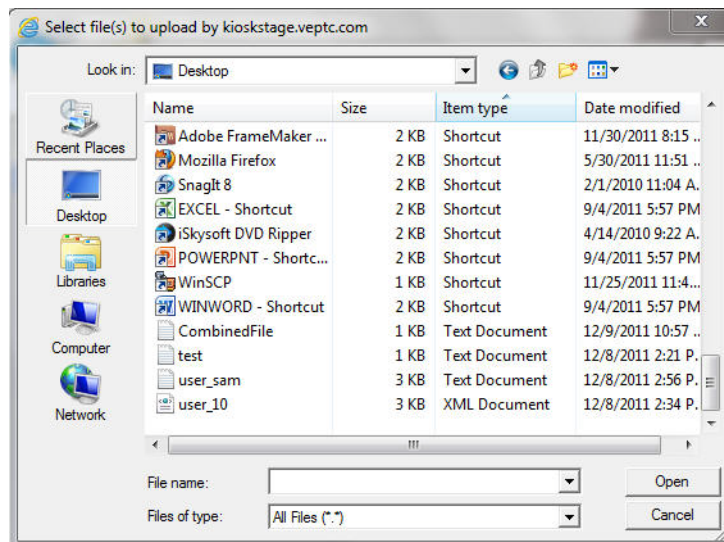
**Figure 5-16 Add Image Button**

The Upload Image dialog box opens.

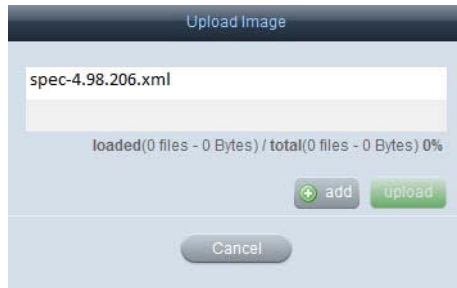
**Step 19** Click **+add**.

**Figure 5-17 Upload Image Dialog Box**

**Step 20** Find the file on your desktop and click **Open**.

**Figure 5-18 Select Files Dialog Box**

The file appears in the Upload Image dialog box.

**Figure 5-19** Specification File in Upload Image Dialog Box**Step 21** Click **upload**.

The file will appear in the Specification list.

All three files should now be uploaded.

**Step 22** In the right pane, click **enable**.

The version is now active. In the Active column, the word “Yes” appears.

**Figure 5-20** Active Column

Version	System Image	Applications Image	Specification	Active
4.98.206	Sat Aug 6 2011	Thu Sep 1 2011	Thu Sep 1 2011	Yes

The images will become available for pushing to the IECs that are registered and active in the IEM.

Deactivate the previous version if one was already activated. You do not need to delete older versions.

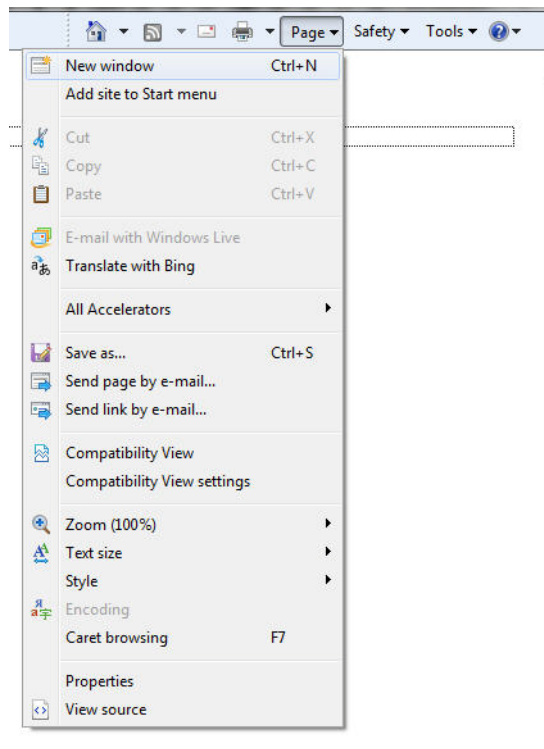
## Saving XML Files

The specification file is an XML file. If it is incorrectly saved, it will report ‘Specification is not found’ when uploading to the IEM. Follow the steps below to save the file correctly to avoid the error message.

**Step 1** Open a recommended browser on your computer.**Step 2** Enter the specification file URL.

**Figure 5-21** Specification File

**Step 3** Click **page** to expand the drop-down list.

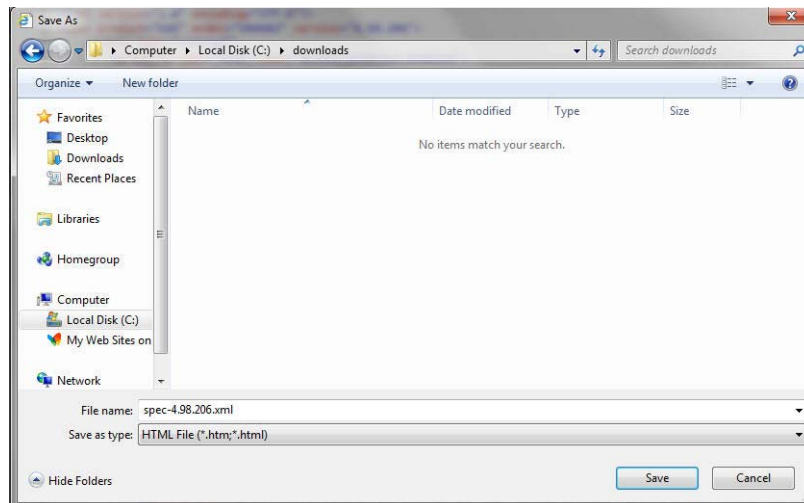
**Figure 5-22** Page Menu

**Step 4** Click **View source**.

The file opens in a Notepad window.

**Figure 5-23 XML File in Notepad Window**

- Step 5** Click **File** to open the File menu.
- Step 6** Click **Save**.
- Step 7** In the Save As dialog box, choose a location on your computer.

**Figure 5-24 Save As Dialog Box**

- Step 8** In the Save as type drop-down list, choose **All Files** to save the file with the xml extension.
- Step 9** Click **Save**.

## IEC Firmware Upgrade Using the Terminal Utility

In this method you will use the debugging console to upgrade the firmware. The unloaders command switches from the old partition to the new partition. The old partition then become available for future upgrades.

You will need the following files that can be downloaded from [www.cisco.com](http://www.cisco.com):

- System file
- Application file
- Specification file

You will also need the URL of where you placed these files.

To upgrade the firmware, follow these steps:

---

**Step 1** Press Ctrl-Alt-S to open the System Settings menu.

**Figure 5-25** System Settings Menu



**Step 2** Click the **Terminal** icon.

The console window opens with the password prompt.

**Step 3** Type the DMC for the password and press the Enter key.

**Figure 5-26** Console Window

```

+=====+
|                COBALT SHELL                |
+=====+
| Unauthorized access is prohibited. |
|   Violators will be prosecuted.   |
+=====+

Type 'help' to print usage information.

=> █

```

**Step 4** To view a list of commands, type **help** and press the Enter key.

**Step 5** Locate the upgrade commands in the list.

**Figure 5-27** Upgrade Commands

```

=> help
USAGE: command [option(s)]

General
=====
    help                - Show this help.
    exit | quit         - Quit the shell.
    sn                  - Show device serial number.
    dmc                  - Show Device Maintenance Code (DMC) for this device.
    reboot              - Reboot the device (no confirmation will be asked).
    reset               - Reset the device to factory defaults and reboot (no confirmation will be asked).

Upgrade
=====
    version             - Show firmware version.
    usys <url>          - Upgrade system firmware from URL.
    uapps <url>         - Upgrade applications firmware from URL.
    uloaders            - Upgrade loaders.

Debugging
=====

```

**Step 6** Enter the **usys <url>** command where the URL is the location of the system firmware file.

**Step 7** Enter the **uapps <url>** command where the URL is the location of the applications firmware file.

**Step 8** Enter the **uloaders** command.



# CHAPTER 6

## Debugging Console

---

Revised: January 29, 2014, OL-26457-05

### Chapter Overview

This chapter explains how to use the debugging console of the Cisco IEC 4600 Series.

Topics in this chapter include:

- [Debugging Console, page 6-1](#)
  - [General Commands, page 6-3](#)
  - [Upgrade Commands, page 6-4](#)
  - [Debugging Commands, page 6-4](#)
  - [Management Commands, page 6-6](#)
  - [Properties Commands, page 6-7](#)

### Debugging Console

The IEC has a custom debug shell that provides command line interface for running diagnostics commands and other debugging and troubleshooting activities.

You will need the Device Maintenance Code (DMC) to access the debugging console. The DMC is found on the General tab of the IEC's Device screen in the IEM.

**Figure 6-1** DMC in the General Tab

General Member Of Profile Policies Status Events Performance Effect.Prof.

Device Name \* Touch\_center

Serial Number 656015320016

Maintenance Code b9f33f Hide Copy

Product IEC

Family 4600

Version 1.0.3

Build 4.176.413

User

Status ON

Uptime 34m 45s

Location

Description

To access the debugging console, follow these steps:

- Step 1** Press Ctrl-Alt-S to open the System Settings menu.

**Figure 6-2** System Settings Menu

- Step 2** Click the **Terminal** icon.
- The console window opens with the password prompt.



**Step 3** Type the DMC for the password and press the Enter key.

**Figure 6-3** Console Window

```

+=====+
|          COBALT SHELL          |
+=====+
| Unauthorized access is prohibited. |
|   Violators will be prosecuted.   |
+=====+

Type 'help' to print usage information.

=> █

```

**Step 4** To view a list of commands, type **help** and press the Enter key.

**Figure 6-4** Command List

```

=> help

USAGE: command [option(s)]

General
=====
    help                - Show this help.
    exit | quit         - Quit the shell.
    sn                  - Show device serial number.
    dmc                  - Show Device Maintenance Code (DMC) for this device.
    reboot              - Reboot the device (no confirmation will be asked).
    reset               - Reset the device to factory defaults and reboot (no confirmat
n will be asked).

Upgrade
=====
    version              - Show firmware version.
    usys <url>           - Upgrade system firmware from URL.
    uapps <url>          - Upgrade applications firmware from URL.
    uloaders             - Upgrade loaders.

Debugging
=====

```

**Step 5** Type the command you desire and press the Enter key.

**Step 6** To close the console window, click the X in the upper left corner of the window.

## General Commands

Enter the following commands to show general information about this utility and the IEC such as the list of commands, the IEC's serial number, and Device Maintenance Code. General commands also include those that reboot and reset the IEC to factory default settings.

**Table 6-1 General Commands**

Command	Description
help	Show the help screen containing the list of commands
exit	Quit the shell
quit	
sn	Show device's serial number
dmc	Show the Device Maintenance Code (DMS)
reboot	Reboot the device (note that no confirmation to reboot will be asked)
reset	Reset the device to factory default settings and reboot (note that no confirmation will be asked)

## Upgrade Commands

Enter the following commands to upgrade the firmware of the device.

**Table 6-2 Upgrade Commands**

Command	Description
version	Show firmware version
usys <url>	Upgrade system firmware from URL
uapps <url>	Upgrade applications firmware from URL
uloaders	Upgrade loaders

**Note**

The angle brackets (<>) indicates a required value. The square brackets ([]) indicate an optional value.

To upgrade the firmware:

1. Enter the **usys** <url> command where the URL is the location of the system firmware file.
2. Enter the **uapps** <url> command where the URL is the location of the applications firmware file.
3. Enter the **uloaders** command to switch to the new partition.

## Debugging Commands

Enter the following commands to debug the device and view system statistics.

**Warning**

**Only run the debug command when troubleshooting the IEC. By default, debugging is turned off. When the debug command is turned on, every event is collected and sent to the IEM's Events tab. The act of collecting and sending the events will use processing power and may impact the performance of the IEC. When you are not troubleshooting an issue on the IEC, make sure that debugging has been turned off by running the release command.**

**Table 6-3**      **Debugging Commands**

Command	Description
debug	Switch the device to debug mode to generate log messages. Since this mode can generate many messages, it might compromise device performance. The device must be rebooted to start all the applications in debug mode.
release	Switch the device to release mode to stop debug level logging. The device must be rebooted to start all the applications in release mode.
memstat	Print memory statistics
cpustat	Print CPU statistics
iostat	Print I/O statistics
dstat	Print local storage statistics
lsusb	List connected USB devices
lsinput	List connected input devices
httphead <url>	Send HEAD request to URL url. Response header will be printed.
ifconfig	Show network interfaces configuration.
traceroute <host address>	Track the route packets taken from an IP network on their way to a given host.
nslookup <host fqdn>	Query Internet domain name servers to find out host's IP addresses.

**Note**

The angle brackets (<>) indicates a required value. The square brackets ([]) indicate an optional value.

The figure below shows the output when the administrator entered the **memstat** command.

**Figure 6-5**      **memstat Command Output**

```
=> memstat
      total      used      free      shared      buffers      cached
Mem:   1971100    972952    998148         0       215224     600796
-/+ buffers/cache:    156932    1814168
Swap:         0         0         0
=>
```

The figure below shows the output when the administrator entered the **lsusb** command.

**Figure 6-6** *Isusb Command Output*

```

=> isusb
Bus 006 Device 002: ID 13d3:3314 IMC Networks
Bus 006 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 005 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 004 Device 003: ID 0d3d:0040 Tangtop Technology Co., Ltd
Bus 004 Device 002: ID 04e7:0020 Elo TouchSystems Touchscreen Interface (2700)
Bus 004 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
=>

```

## Management Commands

Enter the following commands to manage the device.



### Note

These management commands were not designed to configure the device but to aid troubleshooting.

**Table 6-4** *Management Commands*

Command	Description
mng	Show IEM's URL
setmng <url>	Set IEM's URL (note that the prefix will be ignored; it always should be 'https')
compression <on off>	Turn management protocol compression on or off
dload	Load device's profile from the IEM
diload	Load device's information (name and description) from the IEM
dsave	Save device's entire profile on the IEM
disave	Save device's information (name and description) on the IEM
esave	Save events on the IEM (note that the saved events will be removed from the local event database)
dsync	Save unsaved properties from the device's profile on the IEM
ping	Update device's status on the IEM
ismanaged	Check if the device is in managed mode
isreg	Check if the device is registered in the IEM
reg <account> <user> [password]	Register device in the IEM
ureg <user> [password]	Unregister device in the IEM



### Note

The angle brackets (<>) indicates a required value. The square brackets ([ ]) indicate an optional value.

The figure below shows the output when the administrator entered the **mng** command.

**Figure 6-7** *mng Command Output*

```
=> mng
https://172.25.26.103
=>
```

## Properties Commands

The properties commands display and set values and parameters.

**Table 6-5** *Properties Commands*

Command	Description
rm [wildcard]	Remove persistent properties' values (note that if no wildcard ('*') is provided, the entire storage will be cleared)
ls [wildcard]	List properties' values
lsp <name>	List persistent property's value
set <name> <value>	Set properties' values
lsc <wildcard>	List configuration parameters
setc <name> <value>	Set configuration parameters


**Note**

The angle brackets (<>) indicates a required value. The square brackets ([]) indicate an optional value.





## CHAPTER 7

# Locally Configuring the IEC

---

Revised: January 29, 2014, OL-26457-05

## Chapter Overview



### Note

The IEC 4600 Series should be configured from the IEM by applying policies and configuring its profile. This chapter is only for configuration of a single IEC that is not connected to an IEM such as for demo purposes.

---

This chapter explains how to configure the IEC 4600 Series settings for demos or special deployment situations.

The topics in this chapter include the following:

- [Setting Stand-Alone Mode, page 7-2](#)
- [Audio Settings, page 7-4](#)
  - [Specifying the Audio Input Device, page 7-4](#)
  - [Specifying the Audio Output Device, page 7-6](#)
- [Date and Time Settings, page 7-7](#)
  - [Selecting the Time Zone, page 7-9](#)
  - [Selecting the Time Zone, page 7-9](#)
- [Display Settings, page 7-11](#)
  - [Adjusting the Rotation, page 7-11](#)
  - [Selecting the Master Video Display, page 7-13](#)
- [Keyboard Settings, page 7-14](#)
  - [Adjusting the Keyboard Parameters, page 7-14](#)
  - [Specifying the Keyboard Layout, page 7-16](#)
- [Kiosk Settings, page 7-18](#)
  - [Displaying the Navigational Panel and Content Title, page 7-19](#)
  - [Displaying a Website using the Kiosk URL feature, page 7-21](#)
  - [Specifying the Scrolling Mode, page 7-23](#)

- [Mouse Settings, page 7-25](#)
  - [Changing the Mouse Button Order, page 7-25](#)
  - [Changing the Mouse Acceleration and Threshold, page 7-27](#)
  - [Displaying the Mouse Cursor, page 7-28](#)

## Setting Stand-Alone Mode

If you will not use the Cisco IEM to manage the kiosk, configure the Cisco IEC 4600 Series using the stand-alone mode.



### Warning

**If you have already registered a Cisco IEM account, choosing stand-alone will unregister that account.**

**Step 1** Press **Ctrl-Alt-S** to display the System Settings window.

**Step 2** Click the **System** icon.

**Figure 7-1** System Icon in System Settings Window



**Step 3** If the Server tab is not displayed, click the **Server** tab.



**Figure 7-2 Server Tab**

The screenshot shows a window titled "System" with a "Server" tab selected. The window contains the following fields and options:

- Ethernet MAC: 00:21:11:00:20:6C
- Serial number: 656015030192
- Device name: SN656015030192
- Device Description: (empty field)
- Device Location: (empty field)
- Management mode:
  - ☒ Managed by Cisco IE Manager (IEM)
    - IEM URL: (empty field)
    - ☒ Get IEM server address from DHCP
  - ☐ Stand-alone
  - ☐ Managed by Cisco Digital Media Manager (DMM)
    - DMM URL: (empty field)

At the bottom of the window are "Apply" and "Close" buttons.

- Step 4** Enter the device name in the **Device name** field.
- Step 5** Enter the device description in the **Device Description** field.
- Step 6** Enter the device location in the **Device Location** field.
- Step 7** Click the **Stand-alone** radio button.
- Step 8** Enter the account name in the **Account** field.
- Step 9** Enter the user name in the **User name** field.
- Step 10** Enter the password in the **Password** field. To verify that you entered the correct password, check the **Show password** check box to see the characters entered.
- Step 11** Click **Unregister**.
- Step 12** To exit the System window, click **Close**.
- Step 13** In the System Settings window, click **Reboot**.

**Figure 7-3** Reboot Icon in the System Settings Window



## Audio Settings

The Audio setting controls the input and output devices.

### Specifying the Audio Input Device

The default setting for audio input is Analog. There are three types of input audio possible: Analog, Camera, and USB headset. If you want to change this setting, follow the steps below.

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Audio** icon.

**Figure 7-4** Audio Icon in the System Settings window



**Step 3** If the input audio is an USB headset or a camera with an USB cable, connect the USB cable to an USB port on the Cisco IEC 4600 Series. If the input audio is a camera with a TRS connector, connect the TRS connector to the microphone port or RS232 port on the Cisco IEC 4600 Series.

**Figure 7-5** The TRS audio connectors on the Cisco IEC 4600 Series



**Step 4** From the Input drop-down list, choose **Camera** or **USB headset**.

**Figure 7-6** Audio Input Drop-Down List



**Step 5** When you complete the selections in this window, click **Apply**.

**Step 6** To exit the Audio window, click **Close**.

## Specifying the Audio Output Device

The default setting for audio output is Analog. The other options are HDMI, USB headset, and USB speaker.



**Note**

The audio mode falls back to 'Analog' when the audio output is configured as 'USB headset' or 'USB speaker' but a USB headset or speaker is not connected to the IEC.

**Step 1** Press **Ctrl-Alt-S** to display the System Settings window.

**Step 2** Click the **Audio** icon.

**Figure 7-7** Audio Icon in the System Settings window

- Step 3** Connect the cable from the output device to a port (HDMI, USB, TRS headphone, or IR) on the Cisco IEC 4600 Series.

**Figure 7-8** TRS audio connectors on the Cisco IEC 4600 Series

- Step 4** From the drop-down list, choose the type of output.
- Step 5** Click **Apply**.
- Step 6** To exit the Audio window, click **Close**.

## Date and Time Settings

The date, time, and time zone are automatically set by default but can be manually changed if they are incorrect.

### Setting the Date and Time

Follow the steps below to change the date and time.

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Date and Time** icon.

**Figure 7-9** *Date and Time Icon in the System Settings window*

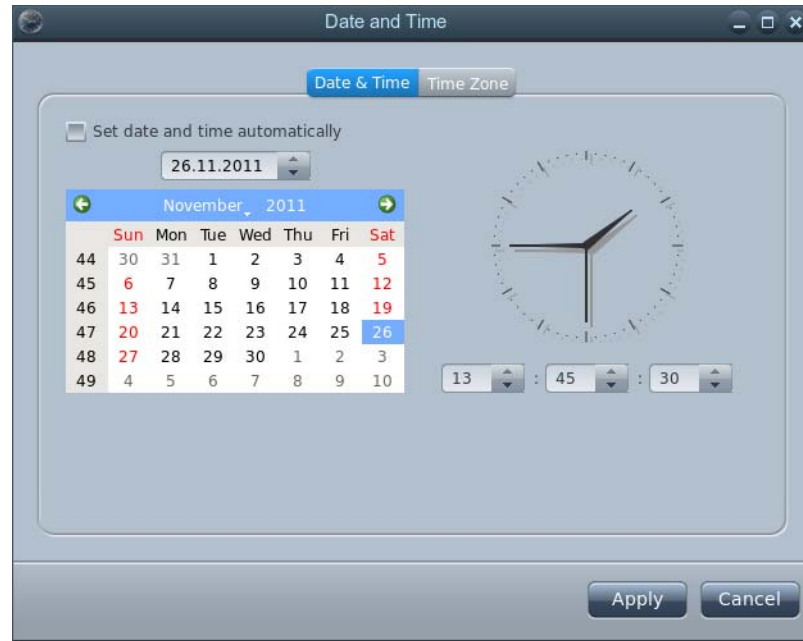


- Step 3** Click the **Date & Time** tab.

**Figure 7-10** *Date & Time Tab*



- Step 4** To change the date and time, uncheck the **Set date and time automatically** check box.
- Step 5** In the date field, enter the month, day, and year.

**Figure 7-11**      **Setting the Date and Time Manually**

**Step 6**      In the time field, enter the hour, minute, and second.

**Step 7**      Click **Apply** to set the new date and time.

**Step 8**      To exit the Date and Time window, click **Close**.

## Selecting the Time Zone

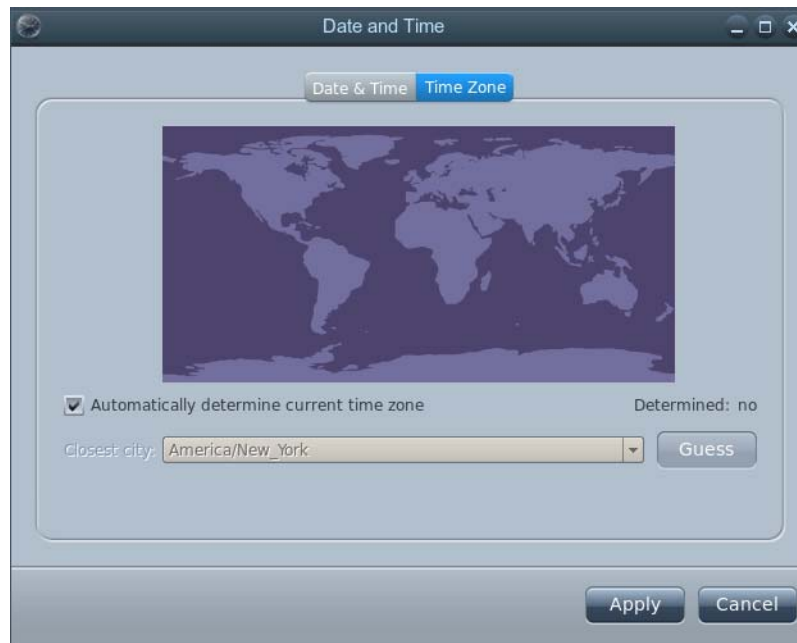
The time zone is automatically determined by default. If the time zone is incorrect or you want to change it, follow the steps below.

**Step 1**      Press **Ctrl-Alt-S** to display the System Settings window.

**Step 2**      Click the **Date and Time** icon.

**Figure 7-12** Date and Time Icon in the System Settings window

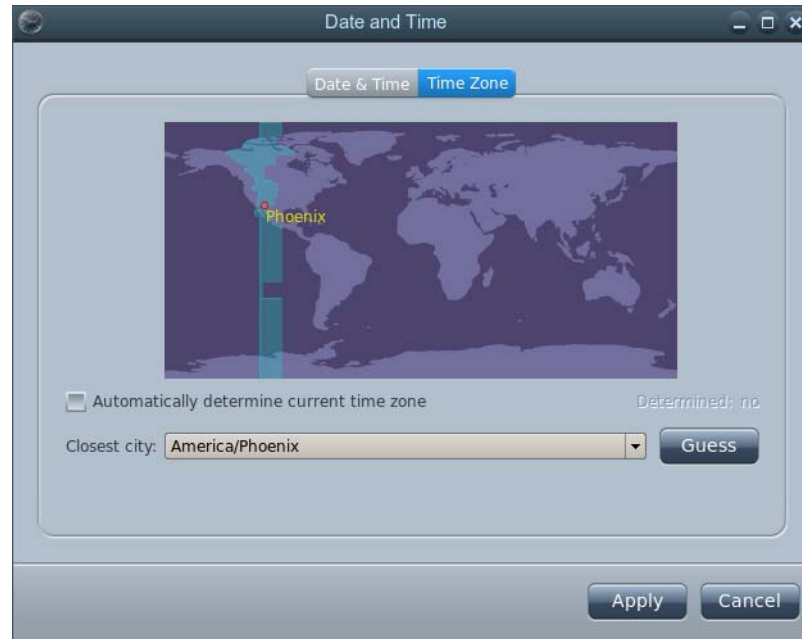
**Step 3** .Click the **Time Zone** tab

**Figure 7-13** Time Zone Tab

**Step 4** Uncheck the **Automatically determine current time zone** check box.

**Step 5** From the Closest city drop-down list, choose a city.



**Figure 7-14** *Choosing the Closest City*

- Step 6** Click **Apply** to set the time zone.
- Step 7** To exit the Date and Time window, click **Close**.
- 

## Display Settings

There are three tabs in the Display settings window. The Information tab lists the display resolution, size, and depth. The General tab indicates the rotation of the display and type of master input used to connect the Cisco IEC 4600 Series to the video display.

### Adjusting the Rotation

The rotation is determined by the IEM policy that is applied. The rotation is set to Normal by default. To change the rotation in standalone mode, follow these steps:

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Display** icon.

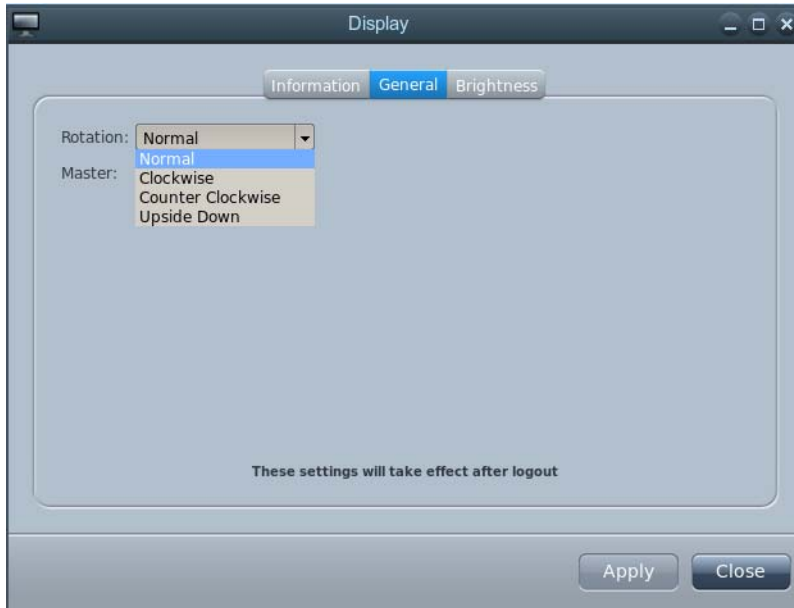
**Figure 7-15** Display Icon in the System Settings window



**Step 3** .Click the **General** tab.

**Step 4** From the Rotation drop-down list, choose a setting (Normal, Clockwise, Counter Clockwise, or Upside Down) that will display the startup URL right-side up.

**Figure 7-16** Rotation Drop-Down List



**Step 5** Click **Apply**.

**Step 6** To exit the Display window, click **Close**.

## Selecting the Master Video Display

The Master setting indicates the input method that is used to connect the video display to the IEC 4600 Series if more than one display has been connected. The two choices are VGA and HDMI. Choose the display connection that you want as the master video display by following these steps.

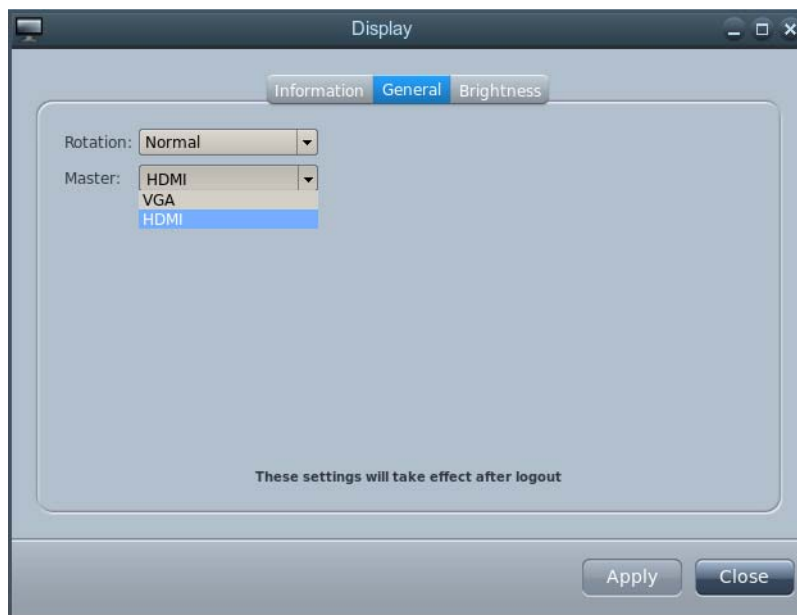
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Display** icon.

**Figure 7-17** *Display Icon in the System Settings window*



- Step 3** Click the **General** tab.
- Step 4** From the Master drop-down list, choose the type of connection used for the video display.

**Figure 7-18** Master Drop-Down List



- Step 5** Click **Apply** to set the master input.
- Step 6** To exit the Display window, click **Close**.
- 

## Keyboard Settings

The Keyboard settings can be changed. Follow these steps to view and change the keyboard settings.

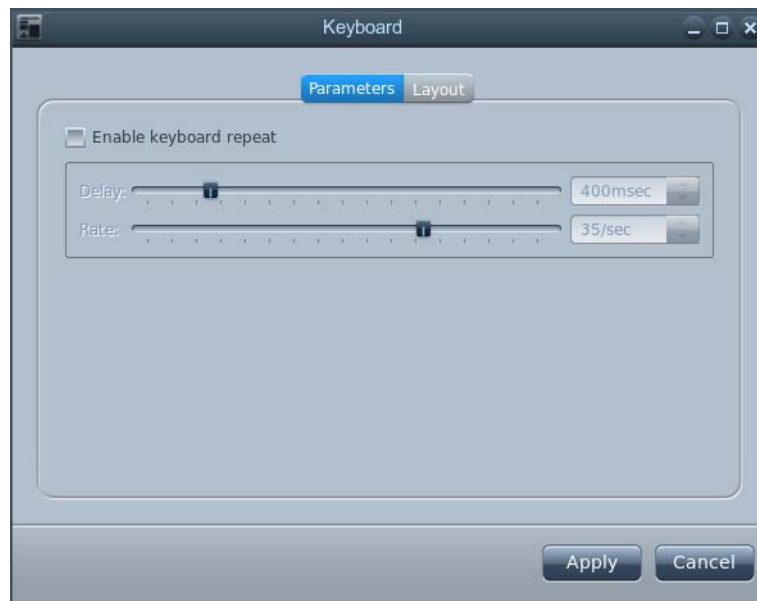
### Adjusting the Keyboard Parameters

The keyboard parameters are by default set to a 400 millisecond delay and at a rate of 35 per second. To change the parameters, follow these steps:

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window
- Step 2** Click the **Keyboard** icon.

**Figure 7-19** Keyboard Icon in System Settings Window

**Step 3** Check the **Enable keyboard repeat** check box

**Figure 7-20** Parameters Tab

- Step 4** To change the delay, slide the delay bar, enter a number between 100 and 2000, or press the **Up Arrow** or **Down Arrow** to pick a value.
- Step 5** To change the rate, slide the rate bar, enter a number between 1 and 50, or press the **Up Arrow** or **Down Arrow** to pick a value.
- Step 6** When you complete the selections in this window, click **Apply**.
- Step 7** To exit the Keyboard window, click **Close**.

## Specifying the Keyboard Layout

Keyboards are available in different languages. The layout for keyboards can be different to accommodate the different characters in languages. In order for the IEC 4600 Series to work with your keyboard, make sure the correct language keyboard has been chosen.

The default keyboard is for the U.S.A. If the keyboard you are using is for a different country, follow these steps:

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window
  - Step 2** Click the **Keyboard** icon.

**Figure 7-21** Keyboard Icon in System Settings Window



- Step 3** Click the **Layout** tab of the Keyboard window.

**Figure 7-22**      **Layout Tab**

**Step 4** Find the country, language, and keyboard type within the Available layouts list.

**Step 5** Click the **Right Arrow** to move that keyboard layout to the Configured layouts list.

**Figure 7-23**      **Available Layouts**

**Step 6** Click on the layout choice that you want to apply.

**Note**

If the USA layout is not needed, you can move it to the Available layouts. Click the layout name and then click the **Left Arrow**.

- Step 7** Click **Apply** to change the layout. Note that the Current layout at the bottom of the window has now changed.

**Figure 7-24** *Current Layout Has Changed*



- Step 8** To exit the Keyboard window, click **Close**.

## Kiosk Settings

If you are using standalone mode, the Kiosk window allows you to modify how the kiosk display appears and interacts with the user. Once the IEC 4600 Series is restored to management mode, the Cisco IEM policy with override these local settings.

You can modify the following in the Kiosk settings screen:

- Title that appears on the top of the screen
- Navigational panel that appears on the top of the screen
- Web page that will display on the browser



**Tip** Only enter a URL if you are not using the IEM to manage the startup URL.



**Note** The URL should not be used for the Remote Expert.



## Displaying the Navigational Panel and Content Title

**Note**

If the navigational panel and content title are to be displayed on the kiosk, they should be configured in the Cisco IEM policy.

To display the navigational panel and the content title on the kiosk when in standalone mode, follow these steps:

**Step 1** Press **Ctrl-Alt-S** to display the System Settings window

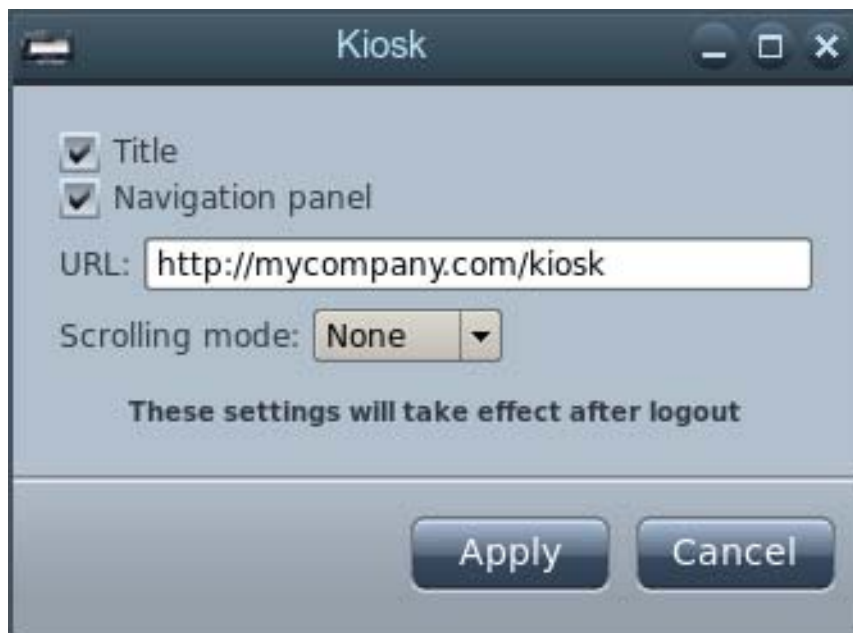
**Step 2** Click the **Kiosk** icon.

**Figure 7-25** Kiosk Icon in System Settings Window



**Step 3** Check the **Title** check box to display a title.

**Figure 7-26** Navigational Panel Check Box

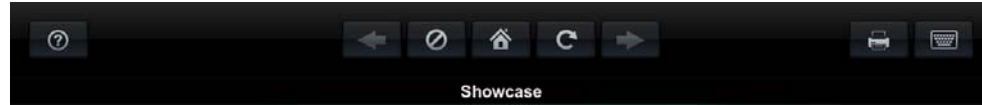


- Step 4** Check the **Navigational panel** check box to display the navigational panel.
- Step 5** Click **Apply**.
- Step 6** To exit the Kiosk window, click **Close**.
- Step 7** In the System Settings window, click **Reboot**.

**Figure 7-27** Reboot Icon in the System Settings Window



The navigational panel and content title now appear at the top of the kiosk display.

**Figure 7-28**      **Navigational Panel and Title on Kiosk**

When the Navigational panel is enabled, the following buttons appear on the kiosk:

- Question/Help button
- Go back one page button
- Stop loading this page button
- Go to startup URL button
- Reload current page button
- Go forward one page button
- Print currently loaded page button
- Show virtual keyboard button

## Displaying a Website using the Kiosk URL feature

If the IEC 4600 Series is in standalone mode, you can display a web page on the kiosk. This feature is available for demos of the unit or when the connection to the IEM has been lost temporarily and it is imperative for the monitor to display content while the connection is fixed.



---

**Tip** Only enter a URL if you are not using the IEM to manage the startup URL.

---



---

**Note** Remote Expert implementations should not use this feature.

---

Follow these steps to configure the Kiosk settings to display a web page:

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window
- Step 2** Click the **Kiosk** icon.

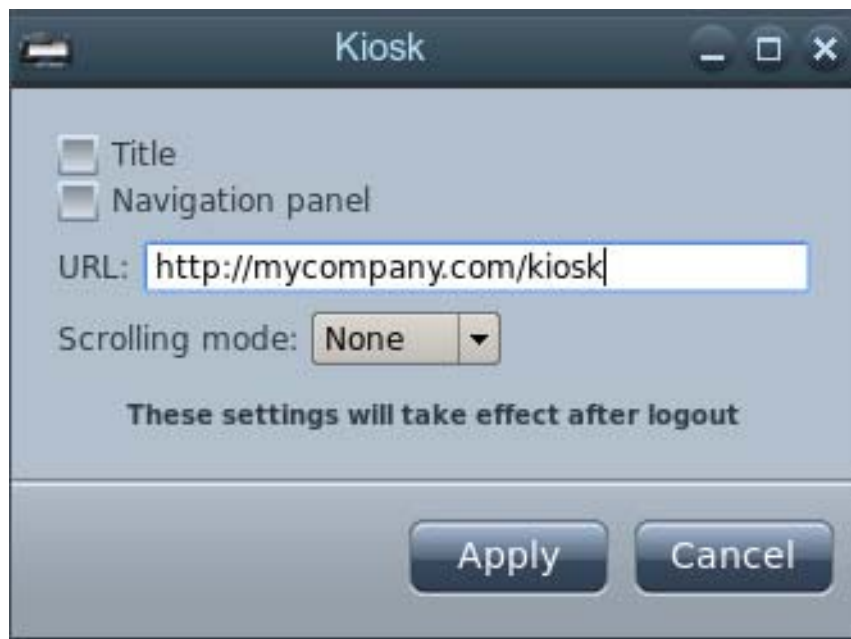
**Figure 7-29** Kiosk Icon in System Settings Window



**Step 3** Enter the website address in the **URL** field.

**Step 4** If the navigational panel should be displayed on the kiosk display, check the **Navigational panel** check box.

**Figure 7-30** URL Field



**Step 5** Click **Apply**.

**Step 6** To exit the Kiosk window, click **Close**.

**Step 7** In the System Settings window, click **Reboot**.

**Figure 7-31** Reboot Icon in the System Settings Window

## Specifying the Scrolling Mode

If scrolling is enabled, customers can scroll through the content on a page. When flicking is chosen as the scrolling method, customers can use the mouse or their finger (if the screen is a touchscreen) to push the page content up, down, right, or left. When “Panels” is the scrolling method, four panes appear on the screen to allow customers to push scroll bars up, down, right, or left. Follow these steps to set the scrolling mode:

- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
  - Step 2** Click the **Kiosk** icon.

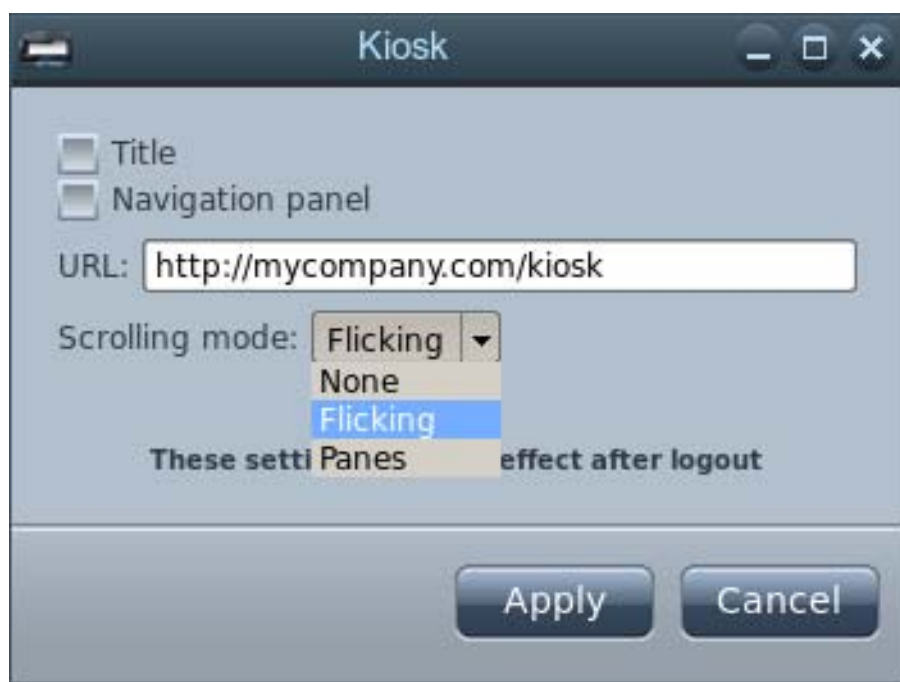
**Figure 7-32** Kiosk Icon in System Settings Window



**Step 3** Enter the website address in the **URL** field.

**Step 4** From the Scrolling mode drop-down list, choose a scrolling mode.

**Figure 7-33** Scrolling Mode Drop-Down List



**Step 5** Click **Apply**.

**Step 6** To exit the Kiosk window, click **Close**.

**Step 7** In the System Settings window, click **Reboot**.

**Figure 7-34** Reboot Icon in the System Settings Window



## Mouse Settings

The mouse settings can be changed. By default, the mouse has the following settings:

- Button order: Right handed
- Acceleration: 2.0
- Threshold: 4
- Mouse cursor: Automatically

## Changing the Mouse Button Order

Follow these steps to change the order of buttons on the mouse:

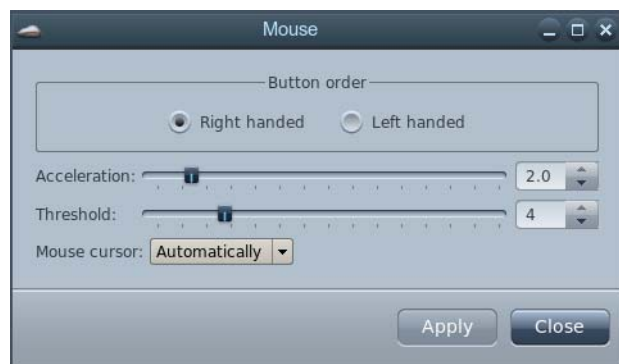
- 
- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Mouse** icon.

**Figure 7-35** Mouse Icon in System Settings Window



**Step 3** To change the button order from right handed to left handed, click the **Left handed** radio button.

**Figure 7-36** Button Order Radio Buttons



**Step 4** Click **Apply**.

**Step 5** To exit the Mouse window, click **Close**.

**Step 6** In the System Settings window, click **Reboot**.



**Figure 7-37** Reboot Icon in the System Settings Window

## Changing the Mouse Acceleration and Threshold

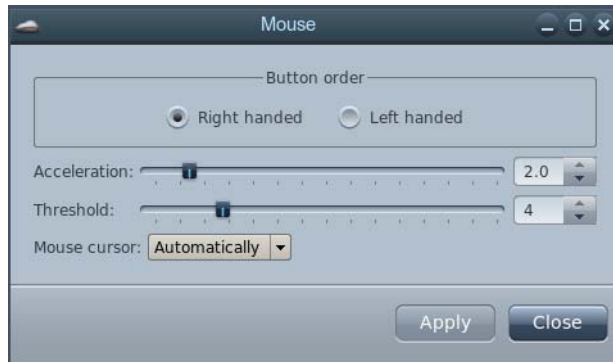
To change the mouse acceleration and threshold settings, follow the steps below.

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Mouse** icon.

**Figure 7-38** Mouse Icon in System Settings Window

- Step 3** To change the acceleration, slide the acceleration bar, enter a value between 0.0 and 20.0, or press the **Up Arrow** or **Down Arrow** to pick a value.

**Figure 7-39** Acceleration and Threshold Slide Bars



- Step 4** To change the threshold, slide the threshold bar, enter a value between 0 and 20, or press the **Up Arrow** or **Down Arrow** to pick a value.
- Step 5** When you complete the selections in this window, click **Apply**.
- Step 6** To exit the Mouse window, click **Close**.
- Step 7** In the System Settings window, click **Reboot**.

**Figure 7-40** Reboot Icon in the System Settings Window



## Displaying the Mouse Cursor

If you want the mouse cursor to appear on the kiosk screen, follow these steps.

- Step 1** Press **Ctrl-Alt-S** to display the System Settings window.
- Step 2** Click the **Mouse** icon.
- Step 3** From the drop-down list, choose **Show** or **Hide** to change the mouse cursor setting.

**Figure 7-41** Mouse Cursor Drop-Down List



- Step 4** To exit the Mouse window, click **Close**.
- Step 5** In the System Settings window, click **Reboot**.

**Figure 7-42** Reboot Icon in the System Settings Window







# APPENDIX **A**

## Compatible Peripherals

---

Revised: January 29, 2014, OL-26457-05

### Appendix Overview

This appendix identifies which peripherals are compatible with the IEC 4600 Series. Topics in this appendix include:

- [Compatible Peripherals, page A-1](#)
- [Configure the NEC MultiSync V552 to Work on a Linux Platform, page A-6](#)

### Compatible Peripherals

Table A-1 contains a list of peripherals that have been deployed with the Cisco Interactive Experience Client 4600 Series devices without incidence. Other models may also be compatible.

**Table A-1**      **Compatible Peripherals**

Peripheral	Type Supported	Reference Peripherals
Touch Screen and Touch Screen Overlay	Linux supported, HID compliant	<p>ELO Optical 4600L and 5500L</p> <p>ELO Intellitouch including 4200L, 4600L, 5500L, ET1928L (see Table A-2 for a complete list of compatible ELO touchscreens)</p> <p>Horizon Display HD47C22VA67-ABIO</p> <p>NEC MultiSync X461S and V552 (see next section for instructions on how to configure this touchscreen to work on a Linux platform)</p> <p>ViewSonic ePoster EP5502T</p> <p>3M DST overlay 3M Micro Touch System DST2270DX (works with LG LD470EUD-SDA1 LED TV)</p> <p>3M Touch Systems, Inc. C4667PW</p> <p>Panasonic TH-42LF30U display with multi touch panel MTP-42LF30</p> <p>Panasonic TH-47LF30U display with multi touch panel MTP-47LF30</p>
Monitor	VGA or HDMI (It is recommended to use a 1920 x 1080 resolution.)	<p>ASUS LCD Monitor VE2208</p> <p>Samsung LN32B650T1FXZA</p> <p>Insignia NSL26Q10A</p> <p>LG LD470EUD-SDA1 LED TV (HDMI recommended)</p>
Remote Control	Cisco IEP-IR-K9	Cisco Remote Control IEP-IR-K9
Wireless Keyboard and Mouse	Wireless USB	<p>Logitech USB wireless K260</p> <p>Logitech Wireless Combo mk520</p>
Wired Mouse	Wired USB	<p>Targus AMU81USZ</p> <p>inland Optical USB Mouse</p>
Wired Keyboard	Wired USB	<p>Moderro Keyboard KB-M3200-311B1</p> <p>Microsoft Keyboard 600 1366</p> <p>Logitech USB Keyboard K120 and K200</p>
Analog Speaker		DAEWOO SMS-010X
Digital Speaker	USB	<p>Altec Lansing Orbit USB speaker</p> <p>Logitech USB speaker S-0155A</p> <p>Logitech USB speaker S-150 (Volume control on the device does not take effect. The volume needs to be controlled from the IEC.</p>
Analog Headset		Plantronics 326 Analog Headset

Peripheral	Type Supported	Reference Peripherals
Analog Microphone		Ihome analog mic IH-H413UN
Digital Microphone	USB	NADY USB condenser mic USB1C
Webcam	HID compliant, USB	Cisco PrecisionHD USB Firmware 1.5 Logitech C110 Logitech C920 camera
Document Camera		Vaddio CeilingVIEW HD-18 DocCAM with DVI/HDMI Quick-Connect
Video Encoder Dongle		System Dimensions AVS 2610 Portable Adaptive Video Streamer for Live Events
Printer	CUPS compliant <sup>1</sup>  HP printers should have HP Linux Imaging and Printing (HPLIP) 3.1 drivers (see <a href="http://hplipopensource.com/hplip-web/supported_devices/index.html">http://hplipopensource.com/hplip-web/supported_devices/index.html</a> )	HP LaserJet P3015n HP LaserJet P2035 HP P1606dn (The network feature is not supported. It can only print via a direct USB connection.) HP LaserJet P1102w (Wireless printing was not tested.)
Optical Scanner		HP 5590 Workgroup Scanner Canon CanoScan Lide 110
Barcode Scanner	Keyboard emulation, USB	Honeywell USB Fixed Position Bar Code Scanner Cypress
Magnetic Card Reader	Keyboard emulation, USB	MagTek 21040146 or 21040108
HDMI Switch		Gefen 4x1 Switcher for HDMI with RS232 switches Extron HDMI Switcher
Wi-Fi: 3G USB Mobile Broadband		Sierra Wireless Aircard 597E Cisco 881G Ethernet Sec Router w/3G B/U

<sup>1</sup>Please consult [www.openprinting.org](http://www.openprinting.org) for printer compatibility. Review the level of support for a printer, which is indicated in the printer's record. Consumer-grade printers where the models change frequently are less likely to be supported. Cisco recommends the use of more mature commercial-grade printers with longer lifespans.


**Tip**

The IEC4610 and IEC4632 models each have four USB ports. If you need to connect more than four USB peripherals, connect a USB hub to one of the USB ports.

**Table A-2**      **Compatible ELO Touchscreens**

<b>Family Name</b>	<b>Type of Enclosure</b>	<b>Size (Inches)</b>	<b>Aspect Ratio</b>	<b>Part Number</b>
1215L	Desktop	12	4:3	E432532
1215L	Desktop	12	4:3	E991639
1247L	Open Frame	12	4:3	E655204
1509L	Desktop	15	16:9	E534869
1515L	Desktop	15	4:3	E344320
1515L	Desktop	15	4:3	E882593
1515L	Desktop	15	4:3	E399324
1517L	Desktop	15	4:3	E144246
1517L	Desktop	15	4:3	E590483
1517L	Desktop	15	4:3	E829550
1517L	Desktop	15	4:3	E342516
1519L	Desktop	15.6	16:9	E175716
1519L	Desktop	15.6	16:9	E114849
1519L	Desktop	15.6	16:9	E264492
1522L	Desktop	15	4:3	E993389
1522L	Desktop	15	4:3	E407449
1522L	Desktop	15	4:3	E518492
1522L	Desktop	15	4:3	E136451
1522L	Desktop	15	4:3	E889598
1522L	Desktop	15	4:3	E664329
1522L	Desktop	15	4:3	E467495
1522L	Desktop	15	4:3	E626377
1528L	Desktop	15	4:3	E338457
1528L	Desktop	15	4:3	E606958
1529L	Desktop	15	4:3	E587776
1529L	Desktop	15	4:3	E785333
1529L	Desktop	15	4:3	E619005
1529L	Desktop	15	4:3	E582772
1529L	Desktop	15	4:3	E564135
1529L	Desktop	15	4:3	E659634
1529L	Desktop	15	4:3	E229149
1529L	Desktop	15	4:3	E641269
1529L	Desktop	15	4:3	E926109
1529L	Desktop	15	4:3	E101984
1529L	Desktop	15	4:3	E273617
1529L	Desktop	15	4:3	E733714



Family Name	Type of Enclosure	Size (Inches)	Aspect Ratio	Part Number
1537L	Open Frame	15	4:3	E731919
1537L	Open Frame	15	4:3	E701210
1537L	Open Frame	15	4:3	E512043
1541L	Open Frame	15.6	16:9	E805638
1541L	Open Frame	15.6	16:9	E606625
1715L	Desktop	17	5:4	E603162
1715L	Desktop	17	5:4	E719160
1717L	Desktop	17	5:4	E649473
1717L	Desktop	17	5:4	E679434
1717L	Desktop	17	5:4	E179069
1717L	Desktop	17	5:4	E227652
1729L	Desktop	17	5:4	E763885
1729L	Desktop	17	5:4	E274975
1729L	Desktop	17	5:4	E461870
1729L	Desktop	17	5:4	E629992
1739L	Open Frame	17	5:4	E734455
1739L	Open Frame	17	5:4	E607940
1739L	Open Frame	17	5:4	E012584
1900L	Desktop	19	16:10	E500662
1915L	Desktop	19	5:4	E607608
1915L	Desktop	19	5:4	E266835
1919L	Desktop	18.5	16:9	E706956
1919L	Desktop	18.5	16:9	E876321
1919L	Desktop	18.5	16:9	E015447
1919L	Desktop	18.5	16:9	E120415
1919L	Desktop	18.5	16:9	E803857
1928L	Desktop	19	5:4	E522556
1928L	Desktop	19	5:4	E935808
1928L	Desktop	19	5:4	E188117
1928L	Desktop	19	5:4	E897317
1937L	Open Frame	19	5:4	E679610
1937L	Open Frame	19	5:4	E896339
1938L	Open Frame	19	16:10	E965017
1939L	Open Frame	19	5:4	E779866
1939L	Open Frame	19	5:4	E945445
1939L	Open Frame	19	5:4	E215546
1940L	Open Frame	19	16:9	E855244

Family Name	Type of Enclosure	Size (Inches)	Aspect Ratio	Part Number
2200L	Desktop	22	16:10	E808372
2201L	Desktop	22	16:9	E107766
2201L	Desktop	22	16:9	E382790
2239L	Open Frame	22	16:10	E846997
2240L	Open Frame	22	16:10	E186354
2242L	Open Frame	22	16:10	E667969
2243L	Open Frame	22	16:9	E059181
2244L	Open Frame	22	16:9	E469590
2400L	Desktop	24	16:10	E100905
2400L	Desktop	24	16:10	E964424
2400L	Desktop	24	16:10	E178661
2639L	Open Frame	26	16:9	E864190
3200L	IDS	32	16:9	E994558
3239L	Open Frame	32	16:9	E162387
4200L	IDS	42	16:9	E841203
4200L	IDS	42	16:9	E505459
4600L	IDS	46	16:9	E960985
4600L	IDS	46	16:9	E536712
5500L	IDS	55	16:9	E053414
5500L	IDS	55	16:9	E891542

**Note**

If an Elo Touchscreen 2216 (1537L) is connected to an IEC in an account that is being exported, the import of that account's XML file will fail. Garbage characters are produced in the name of the touchscreen field when using this Elo touchscreen. There are a number of workarounds if you need to import an account that contains IECs connected to this touchscreen: 1) Disconnect the monitor before exporting the account. 2) Delete the monitor block from exported XML and then import the file. 3) Delete the entire device block from exported XML and then import the file.

## Configure the NEC MultiSync V552 to Work on a Linux Platform

To configure the NEC MultiSync V552 touchscreen to work on a LINUX platform, follow these steps:

- Step 1** Install the C.T.M. application on a WIN OS platform.
- Step 2** Plug in the USB connector.
- Step 3** Log into CTM.
- Step 4** Navigate to Administrator > Functional Settings.
- Step 5** Select the **ProDrive** radio button in the Protocol field.

- Step 6** Configure the following values in the Communication field:
- a. Configure the Touch Type as **Single Touch**.
  - b. Configure the Communications as **Mouse**.
  - c. Configure the Identification as **Manual**.
- Step 7** Select the Operating System as **Linux** from the Touch Type field drop down menu.
- Step 8** Select **Back** and then select **Yes** to save settings.
-





# APPENDIX **B**

## Printers

---

Revised: January 29, 2014, OL-26457-05

## Appendix Overview

This appendix identifies how to implement printers at kiosks to allow end users to print documents.

Topics in this appendix include:

- [Printer Compatibility, page B-1](#)
- [Printer Implementation, page B-2](#)
  - [global.printer Object, page B-2](#)
  - [PrintJob, page B-4](#)
  - [Example Usage of the global.printer Object, page B-5](#)
  - [Best Practices and Tips, page B-6](#)
  - [Testing the Printer Widget, page B-7](#)

## Printer Compatibility

Refer to Appendix A for a list of printers that have been tested with the IEC 4600 Series.



**Note**

---

Other printers may also be compatible.

---

## Printer Implementation

### global.printer Object

The global.printer object implements a printer interface which allows control of the printer connected to the IEC 4600 Series either locally or via the network. This object allows end users to print PDF files, images, plain text documents and HTML documents. Plain text and HTML documents must be UTF-8 encoded in order to be printed correctly.

**Note**

While printing HTML documents, the end user will not be able to print external resources referred by that document such as images, flash clips or plugins.

The following is the `global.printer` object code:

```
interface Printer
{
    attribute bool collateCopies;
    readonly attribute int colorCount;
    attribute ColorMode colorMode;
    attribute int copyCount;
    attribute bool doubleSidedPrinting;
    attribute DuplexMode duplex;
    attribute bool fontEmbeddingEnabled;
    attribute int fromPage;
    attribute bool fullPage;
    readonly attribute int widthMM;
    readonly attribute int heightMM;
    readonly attribute bool isValid;
    readonly attribute string name;
    attribute Orientation orientation;
    attribute PageOrder pageOrder;
    attribute PaperSize paperSize;
    attribute PaperSource paperSource;
    readonly attribute PrinterState state;
    attribute int resolution;
    readonly attribute list<int> supportedResolutions;
    readonly attribute bool supportsMultipleCopies;

    slot bool abort();
    slot bool newPage();

    void getPageMargins(out real left, out real top,
        out real right, out real bottom,
        int Unit unit) const;
    void setPageMargins(in real left, in real top, in real right, in real bottom, in
        Unit unit);
    QSizeF paperSize(Unit unit) const;
    bool print(in string url);

    signal void finished(in bool ok);
    signal void pagePrinted(in int pageNumber);
};
```

**Table B-1** *global.printer Variables*

Variable	Description
<code>collateCopies</code>	Contains true if collation is turned on when multiple copies is selected. Contains false if it is turned off when multiple copies is selected. When collating is turned off, the printing of each individual page will be repeated the <code>numCopies</code> amount before the next page is started. With collating turned on, all pages are printed before the next copy of those pages is started.
<code>colorCount</code>	Contains the number of different colors available for the printer.
<code>colorMode</code>	Contains the current color mode.

Variable	Description
copyCount	Contains the number of copies that will be printed. The default value is 1.
doubleSidedPrinting	Contains true if double side printing is enabled.
duplex	Contains the current duplex mode.
fontEmbeddingEnabled	Contains true if font embedding is enabled.
fromPage	Contains the number of the first page in a range of pages to be printed (the "from page" setting). Pages in a document are numbered according to the convention that the first page is page 1. By default, this function returns a special value of 0, meaning that the "from page" setting is unset.
fullPage	Contains true if the origin of the printer's coordinate system is at the corner of the page and false if it is at the edge of the printable area.
widthMM	Contains the width of printing area in millimeters.
heightMM	Contains the height of printing area in millimeters.
isValid	Contains true if the printer currently selected is a valid printer in the system.
name	Contains the printer name.
orientation	Contains the orientation setting.
pageOrder	Contains the current page order.
paperSize	Contains the printer paper size.
paperSource	Contains the printer's paper source.
printerState	Contains the current state of the printer. This may not always be accurate (for example if the printer doesn't have the capability of reporting its state to the operating system).
resolution	Contains the current assumed resolution of the printer.
supportedResolutions	Contains a list of the resolutions (a list of dots-per-inch integers) that the printer says it supports.
supportsMultipleCopies	Returns true if the printer supports printing multiple copies of the same document in one job; otherwise false is returned. On most systems this function will return true.
abort()	Aborts the current print run. Returns true if the print run was successfully aborted and <code>printerState</code> will return "Printer::Aborted;" otherwise returns false. It is not always possible to abort a print job. For example, all the data has gone to the printer but the printer cannot or will not cancel the job when asked to.
newPage()	Tells the printer to eject the current page and to continue printing on a new page. Returns true if this was successful; otherwise returns false.
getPageMargins()	Returns the page margins for this printer for the left, top, right, and bottom margins. The unit of the returned margins are specified with the unit parameter.
setPageMargins()	This function sets the left, top, right and bottom page margins for this printer. The unit of the margins are specified with the unit parameter.
paperSize()	Returns the paper size unit.

Variable	Description
print()	Prints document given by its URL. The url can be local file system path or an HTTP URL. Returns zero in case of success and error code in case of failure.
finished()	Fired when printing job is finished. ok is true in case of success and false in case of failure.
pagePrinted()	Fired when PDF document page is printed.
pageNumber	Indicates the page number that was just printed.

## PrintJob

All global.printer methods related to performing actual printing return objects implementing the PrintJob interface.

```
interface PrintJob {
    readonly attribute JobState state;
    readonly attribute string errorString;
    readonly attribute string printerName;
    readonly attribute bool isFinished;

    void cancel();
    void remove();

    signal void finished();
    signal void error();
    signal void stateChanged();
}
```

**Table B-2** *PrintJob Variables*

Variable	Description
state	Contains current state of the print job and has one of the following values:  'Downloading' — document is being downloaded from remote server 'Held' — job is held for printing 'Pending' — job is waiting to be printed 'Processing' — job is currently printing 'Completed' — job has completed successfully 'Stopped' — job has been stopped 'Aborted' — job has aborted due to an error
errorString	Contains string describing the error that has occurred
printerName	Contains name of a printer performing the job
isFinished	Contains 'true' if printer finished processing the job regardless if it was successful or not or 'false' if printer has not finished processing the job



Variable	Description
cancel()	Instructs the printer to cancel processing the print job. Returns 'true' on success or 'false' on failure. Note that it is not always possible to stop printing immediately if this process already started.
remove()	Instructs the browser to remove job object. Information about all processed and finished jobs are kept in memory. If application uses printing extensively, it may be necessary to free resources associated with finished jobs manually using this method. Job object should never be used after the call of this method.
finished()	Returns when the job is finished processing regardless if it was successful or not
error()	Returns when error related to the job occurs
stateChanged()	Returns every time job state changes

## Example Usage of the global.printer Object

The following HTML document contains an example of global.printer usage.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>

<head>

<title>...: global.printer test :...</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">

<style>

body
{
margin: 20px;
background-color: #000000;
color: #ffffff;
font-weight: bold;
font-family: Arial;
font-size: 20px;
color: #ffffff;
}

</style>

<script type="text/javascript">

var pageNumber;

function onFinish(ok)
{
document.getElementById("jobState").innerHTML = ok ? "Successfully" :
"Unsuccessfully";
}

function onPagePrinted(number)
{
pageNumber.innerHTML = number;
}
```

```

function init()
{
document.getElementById("name").innerHTML = global.printer.name;
document.getElementById("resolution").innerHTML = global.printer.resolution;
document.getElementById("state").innerHTML = global.printer.state;

pageNumber = document.getElementById("pageNumber");

global.printer.finished.connect(onFinished);
global.printer.pagePrinted.connect(onPagePrinted);

// global.printer.print("http://www2.lauterbach.com/doc/rtosqnx.pdf");
//
global.printer.print("http://is1.vladstudio.com/jpg_low/1600x1200/vladstudio_gecko_160
0x1200
.jpg");
global.printer.print("http://lenta.ru/news/2011/09/20/c27j/");
}

</script>

</head>

<body onload="init()">

<table cellpadding="2" cellspacing="0" border="1" align="center" width="50%">
<tr>
<td>Printer name</td>
<td id="name"></td>
</tr>
<tr>
<td>Resolution</td>
<td id="resolution"></td>
</tr>
<tr>
<td>State</td>
<td id="state"></td>
</tr>
<tr>
<td>Page printed</td>
<td id="pageNumber"></td>
</tr>
<tr>
<td>Job finished</td>
<td id="jobState"></td>
</tr>
</table>

</body>

</html>

```

## Best Practices and Tips

- Make sure to have the location of the file as a URL.
- Change the URL in the above HTML to print another file.
- Copy the above contents to an HTML file and transfer the file to a web server from where it can be accessed.

- The printer must be connected to the IEC. Reboot the IEC after connecting the printer.

## Testing the Printer Widget

There are two ways to test the printer widget:

1. Using the policy:
  1. Create a policy with startup URL as the URL of the printer HTML and apply the policy  
As a result, the IEC boots up with the printer policy loaded.
2. Using the Kiosk menu:
  1. On the IEC, press Ctl + Alt + S and then choose Kiosk
  2. Enter the printer widget URL
  3. Reboot the IEC  
As a result, the IEC boots up with the printer URL loaded.





# APPENDIX C

## Optical Scanners

---

Revised: January 29, 2014, OL-26457-05

### Appendix Overview

An optical scanner can be connected to the IEC to allow end users to scan a document at the kiosk.

This appendix explains how to implement optical scanners connected to the IECs.

Topics in this appendix include:

- [Optical Scanner Compatibility, page C-1](#)
- [Optical Scanner Implementation, page C-1](#)
  - [global.scanner Object, page C-1](#)
  - [Best Practices and Tips, page C-3](#)
  - [Testing the Scanner Widget, page C-3](#)

### Optical Scanner Compatibility

Refer to Appendix A for the list of optical scanners that have been tested with the IEC.



**Note**

---

Other scanner models may also be compatible.

---

### Optical Scanner Implementation

#### global.scanner Object

The global.scanner object implements an interface for optical scanners allowing an application displayed on a kiosk to scan and manipulate a document. The scanner library used is from SANE and the list of compatible devices can be found here: <http://www.sane-project.org/sane-supported-devices.html>

The global.scanner object code is:

```
interface Scanner
```

```

{
    attribute uint dpiX;
    attribute uint dpiY;
    attribute bool color;
    attribute string source;
    readonly attribute List<String> devices;
    readonly attribute List<String> sources;
    readonly attribute string lastError;
    readonly attribute string base64Data;
    readonly attribute bool busy;

    void setCurrentScanner(in string deviceName);

signals:
    void finished();
    void error(out string error);

slots:
    start();
    stop();
    shutdown();
};

```

**Table C-1** *global.scanner Object Variables*

Variable	Description
dpiX	DPI X of the selected scanner
dpiY	DPI Y of the selected scanner
color	Is selected scanner in color mode
source	Document source
devices	List of available scanners
sources	List of available document sources
lastError	Last error occurred
base64Data	Scanned image as base64 JPEG data
busy	Check if the scanner is busy
setCurrentScanner(in string deviceName)	Set the current scanner to use. You need to call this method before scanning.
finished()	The scanner has finished scanning
error(out string error)	An error has occurred
start()	Start scanning from the selected scanner and document source
stop()	Stop scanning
shutdown()	Shutdown scanning subsystem and reset all internal caches

## Best Practices and Tips

- Make sure to have the location of the file as a URL.
- Copy the above contents to an HTML file and transfer the file to a web server from where it can be accessed.
- The scanner must be connected to the IEC. Reboot the IEC after connecting the scanner.

## Testing the Scanner Widget

There are two ways to test the scanner widget:

1. Using the policy:
  1. Create a policy with startup URL as the URL of the scanner HTML and apply the policy  
As a result, the IEC boots up with the scanner policy loaded.
2. Using the Kiosk menu:
  1. On the IEC, press Ctrl + Alt + S and then choose Kiosk
  2. Enter the scanner widget URL
  3. Reboot the IEC  
As a result, the IEC boots up with the scanner URL loaded.







## APPENDIX **D**

# Magnetic Card Readers and Barcode Scanners

---

Revised: January 29, 2014, OL-26457-05

## Appendix Overview

This appendix explains how to implement magnetic card readers and barcode scanners to allow end users to swipe their credit cards, customer loyalty cards, or gift cards or scan a barcode on a product.

Topics in this appendix include:

- [Magnetic Card Reader and Barcode Scanner Compatibility, page D-1](#)
- [Magnetic Card Reader and Barcode Scanner Implementation, page D-1](#)
  - [Magnetic Card Reader or Barcode Scanner Name, page D-2](#)
  - [global.magstripe Object, page D-3](#)
  - [Implement the global.magstripe Object, page D-4](#)

## Magnetic Card Reader and Barcode Scanner Compatibility

HID or keyboard emulation-type magnetic card readers and barcode scanners are supported by IEC 4600 Series devices. Refer to Appendix A for a list of magnetic card readers and barcode scanners that have been tested with the IEC 4600 Series.

## Magnetic Card Reader and Barcode Scanner Implementation

To enable the magnetic card reader or barcode scanner, you will perform the following:

1. Retrieve the name of the peripheral that the IEC recognizes
2. Replace the `deviceName` variable in the `global.magstripe` object with the name of the peripheral that the IEC recognizes
3. Implement the `global.magstripe` object in your application
4. Configure the key and value in the device's profile or an applied property in the IEM

## Magnetic Card Reader or Barcode Scanner Name

You need the exact name of the card reader or barcode scanner by which the IEC recognizes the peripheral. Follow these steps to retrieve that name:

- Step 1** Plug the magnetic card reader or barcode scanner into the USB port of the IEC.
- Step 2** Reboot the IEC so that the IEC will recognize the new peripheral.
- Step 3** Run the **lsinput** command at the shell prompt to get a list of connected input devices.

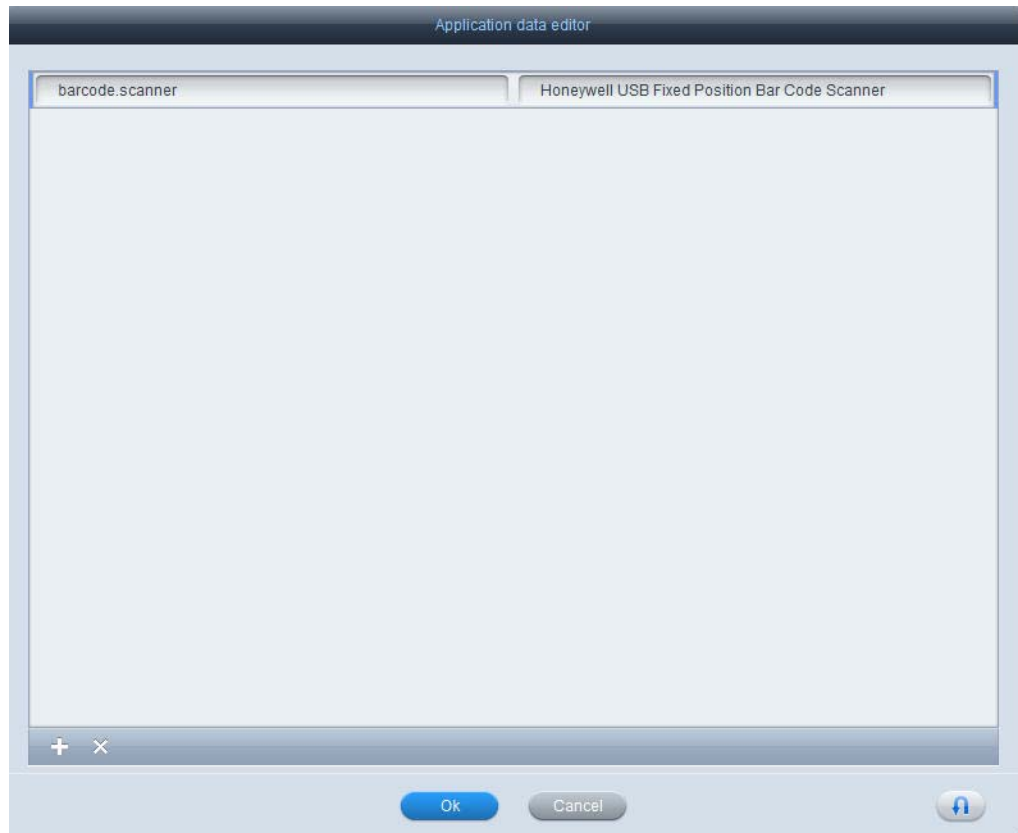


**Note** Alternatively, you can get the name from the Cisco Interactive Experience Manager (IEM). Go to the device and click the Status tab.

- Step 4** Find the name of the magnetic card reader or barcode scanner. In the example below, the magnetic card reader is shown in red:

```
Virtual core pointer id=2[master pointer (3)]
  Virtual core XTEST pointer id=4[slave pointer (2)]
  Microsoft Microsoft® Digital Media Keyboardid=12[slave pointer (2)]
  Filtered Elo TouchSystems, Inc. Elo TouchSystems 2700 IntelliTouch(r) USB
  Touchid=14[slave pointer (2)]
  MCE IR Keyboard/Mouse (ite-cir) id=15[slave pointer (2)]
  Elo TouchSystems, Inc. Elo TouchSystems 2700 IntelliTouch(r) USB Touchmonitor
  Interfaceid=9[slave pointer (2)]
Virtual core keyboard id=3[master keyboard (2)]
  Virtual core XTEST keyboard id=5[slave keyboard (3)]
  Power Button id=6[slave keyboard (3)]
  Video Bus id=7[slave keyboard (3)]
  Power Button id=8[slave keyboard (3)]
  PWC snapshot button id=10[slave keyboard (3)]
  Microsoft Microsoft® Digital Media Keyboardid=11[slave keyboard (3)]
  Mag-Tek USB Swipe Reader id=13[slave keyboard (3)]
  ACPI Virtual Keyboard Device id=16[slave keyboard (3)]
  ITE8704 CIR transceiver id=17[slave keyboard (3)]
```

- Step 5** Replace the `deviceName` variable in the `global.magstripe` object with the name of the peripheral that the IEC recognizes.
- Step 6** In the device's profile or a property applied to that device within the IEM, configure the application data property with "barcode.scanner" or "magstripe.scanner" for the key and the name of the peripheral that the IEC recognizes for the value.

**Figure A-1** Barcode Scanner Entered in the Application Data Editor

**Step 7** Click **Ok**.

**Step 8** Click **Apply**.

## global.magstripe Object

The global.magstripe object is a widget that provides an interface to magnetic card readers or barcode scanners.

In the case of a card reader, the widget reacts to a scan of a card and returns the value of the data that is recorded on the magnetic stripe. For credit cards, the data returned is typically cardholder's name, card number, and expiration date. The widget returns the data in an unparsed form, so it is the responsibility of the developer to decrypt if necessary and parse the data.

For a barcode reader, the widget registers a scanned event and returns the string that represents the barcode.

The global.magstripe object code is:

```
interface Magstripe {  
    void open(in string deviceName);  
    void close();  
  
signals:  
    void opened();
```

```

void scanning();
void scanned(out string data);
void error(out string error);
}

```

**Table D-2** *global.magstripe Object Variables*

Variable	Description
open(in string deviceName)	Open the device for reading data. If deviceName is not empty, use this device name, and browser.magstripe.scanner property otherwise.
close()	Close the device.
opened()	The device has been open successfully.
scanning()	The device has started data scanning.
scanned(out string data)	The device has finished scanning, read the scanned data from deviceName.
error(out string error)	Error has occurred.

## Implement the global.magstripe Object

- 
- Step 1** Open your application's code.
- Step 2** Insert the global.magstripe object code.
- Step 3** Replace the deviceName variable with the name of the device that you retrieved from the IEC.
-



## APPENDIX **E**

# Infrared Remote Controls

---

Revised: January 29, 2014, OL-26457-05

## Appendix Overview

An Infrared (IR) Cisco Remote Control can be connected to the Cisco Interactive Experience Client 4600 (IEC 4600) Series device so that the end user can control applications and remote playback without touching the screen or using a mouse.

This appendix explains which Cisco Remote Control is supported and how to configure applications to allow use of the remote control.

Topics in this appendix include:

- [Cisco Remote Control IEP-IR-K9, page E-1](#)
  - [Battery, page E-2](#)
  - [Infrared Sensor, page E-3](#)
- [Remote Control Buttons, page E-4](#)
- [Remote Control Implementation, page E-9](#)
  - [global.ir Object, page E-10](#)
  - [Usage of global.ir Object, page E-10](#)

## Cisco Remote Control IEP-IR-K9

The Cisco Remote Control IEP-IR-K9 is the remote control model that is supported with the IEC.

Figure A-1 Cisco Remote Control IEP-IR-K9



## Battery



### Warning

Lithium Batteries are used in this module. Do not try to charge, discharge, or replace these batteries.

<b>Waarschuwing</b>	Er worden lithiumbatterijen gebruikt in deze module. Probeer deze batterijen niet te laden, ontladen of vervangen.
<b>Varoitus</b>	Moduulissa käytetään litiumparistoja. Älä yritä ladata, purkaa tai vaihtaa näitä paristoja.
<b>Attention</b>	Ce module requiert des piles au lithium. N'essayez pas de les recharger, les décharger ou de les remplacer.
<b>Warnung</b>	In diesem Modul werden Lithium-Batterien eingesetzt. Versuchen Sie nicht, diese Batterien aufzuladen, zu entladen oder zu ersetzen.
<b>Avvertenza</b>	Questo modulo utilizza batterie al litio. Non tentare di caricare, scaricare o sostituire le batterie.

<b>Advarsel</b>	<b>Det brukes litiumbatterier i denne modulen. Forsøk ikke å lade, utlade eller skifte ut disse batteriene.</b>
<b>Aviso</b>	<b>Este módulo utiliza baterias de Lítio. Não tente recarregar, descarregar ou substituir essas baterias.</b>
<b>Advertencia!</b>	<b>Este módulo funciona con pilas de litio. No intente cargarlas, descargarlas ni recambiarlas.</b>
<b>Varning!</b>	<b>Litiumbatterier används i denna modul. Försök inte att ladda upp, ladda ur eller byta ut dessa batterier.</b>

The Cisco remote control is battery-powered. It uses a standard, 3V CR2025 lithium battery, manufactured by a well-known supplier such as Panasonic or Toshiba. The name of the actual manufacturer is etched into the face of the battery.

When the battery loses its charge or when you remove the battery, the remote control will not work until the battery is replaced.

You should always recycle or dispose of the battery in accordance with:

- Its manufacturer guidelines.
- Regulations in your locale for disposal and recycling.



#### Note

Remote control settings are not lost when you remove or replace the battery.

To replace the battery in the remote control, follow these steps:

- Step 1** Place the remote control on a flat surface, button-side down.
- Step 2** To unlock the battery clip and remove it, pinch the locking mechanism and slide the clip out of the remote control.
- Step 3** To remove the old battery from the clip, pivot the battery so that it touches only the opening of the clip.
- Step 4** Insert a new battery so that positive charge (+) symbols are visible simultaneously on the battery and the clip.
- Step 5** Slide the clip back in to the remote control.

## Infrared Sensor

The IEC is equipped with an infrared (IR) sensor that receives, recognizes, and reacts to the signals from this Cisco remote control.

The way that you mount an IEC can limit how well it responds to these signals. The mounting method might block the IR sensor.





It is recommended to use an IR extender with the remote control. With the IR extender, the range of the remote control is approximately up to 15 feet (4.57m).

The IR sensor of the extender (or the IR sensor of the IEC if you are not using the extender) must be in the line of sight of the end user. The remote control will not work if the IR sensor is behind the touchscreen or blocked by another peripheral.




## Remote Control Buttons

All the buttons can be programmed. The functions listed in the tables below are standard functions for the keys.




**Table E-2 System Control Buttons**

Function	Button	IR Signal Frequency
Power		0xff 00 0090
Input		0xef 10 0090
Information		0xe0 1f 0090
Help		0xf6 09 0090

**Table E-3 Playback Control Buttons**

Function	Button	IR Signal Frequency
Play		0xf9 06 0090
Pause		0xfd 02 0090
Stop		0xfc 03 0090






Function	Button	IR Signal Frequency
Rewind		0xfb 04 0090
Fast forward		0xfa 05 0090
Live		0xf7 08 0090



**Note**

The Live button is usually used to jump to the next channel or track.

**Table E-4 Audio Control Buttons**

Function	Button	IR Signal Frequency
volume up		0xbf 40 0090
volume down		0xbe 41 0090
mute		0xfe 01 009

**Table E-5 Channel Control Buttons**

Function	Button	IR Signal Frequency
Channel down		0xbc 43 0090
Channel up		0xbd 42 0090












Function	Button	IR Signal Frequency
Return to previous		0xe3 <b>1c</b> 0090
1		0xf2 <b>0d</b> 0090
2		0xf1 <b>0e</b> 0090
3		0xf0 <b>0f</b> 0090
4		0xe1 <b>1e</b> 0090
5		0xe8 <b>17</b> 0090
6		0xe7 <b>18</b> 0090
7		0xe6 <b>19</b> 0090
8		0xe5 <b>1a</b> 0090
9		0xe4 <b>1b</b> 0090
0		0xe2 <b>1d</b> 0090

Table E-6 Menu Control Buttons







Function	Button	IR Signal Frequency
Menu		0xb8 47 0090
Up		0xea 15 0090
Left		0xec 13 0090
OK		0xed 12 0090
Right		0xeb 14 0090
Down		0xe9 16 0090

Table E-7 Guide Control Buttons









Function	Button	IR Signal Frequency
Guide		0xf5 <b>0a</b> 0090
Page up		0xea <b>15</b> 0090
Page down		0xf3 <b>0c</b> 0090
Exit		0xee <b>11</b> 0090

Table E-8 Soft Keys

Function	Button	IR Signal Frequency
		0xa9 <b>56</b> 0090
		0xaf <b>50</b> 0090
		0xad <b>52</b> 0090
		0xab <b>54</b> 0090

The following is an example of programming for the remote control in an application:

```
if(!filterIR){
    filterIR = true;
    document.getElementById("trace").innerHTML = "IR pressed key code: "+key+"
    (" +skey+ ")";
    switch(skey){
        case "play":
            HUD("play");
            playVideo();
            break;
        case "pause":
            HUD("pause");
            togglePause();
            break;
        case "fastforward":
            HUD("fwd");
            playNextTrack();
            break;
        case "rewind":
            HUD("rewind");
            playPrevTrack();
            break;
        case "stop":
            HUD("stop");
            stopVideo();
            break;
        case "right":
            HUD("right");
            selectNext();
            break;
        case "left":
            HUD("left");
            selectPrevious();
            break;
        case "okay":
            HUD("play");
            playSelected();
            break;
        case "power":
            window.location = "index.html";
            default:
            break;
    }
    irFilterTimeout = setTimeout(function(){filterIR=false}, 750);
}
```

## Remote Control Implementation

The IR port is active by default. No additional configuration is required.

You will need to embed the global.ir object into your application code in order for your applications to perform the expected action when the end user presses a button on the remote control.

## global.ir Object

The global.ir object implements the IR interface. It allows an application to receive signals from the infrared remote control.

The global.ir object code is:

```
interface Ir {
    readonly attribute string lastError;
    List <String> availableControls() const;
    bool setCurrentControl(in string device);
signals:
    event(in uint key, in string skey, in string configName) const;
    error(in string err) const;
}
```

**Table E-9**      *global.ir Object Variables*

Variable	Description
lastError	Last error occurred
availableControls()	Returns the list of the supported remote controls
setCurrentControl(in string device)	Sets the current remote control to use.  The device name must be obtained from availableControls() list.  Leave the device name empty to use browser.ir.configuration. In this case you should set browser.ir.configuration.enabled to <b>true</b> and browser.ir.configuration to the valid LIRC configuration.
event(in uint key, in string skey, in string configName)	Remote control event <ul style="list-style-type: none"> <li>The event control code is set to <b>key</b>.</li> <li>The control name (such as "poweroff", "ch1", "up", etc.) is set to <b>skey</b>.</li> <li>The configuration name, which is rarely needed, is set to <b>configName</b>.</li> </ul>

## Usage of global.ir Object

The following HTML code contains an example of global.ir usage.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/
loose.dtd">
<html>

<head>

<title>...: global . ir test :... </title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

```

<style>

    body
    {
        margin: 20px;
        background-color: #111111;
        color : #eeeeee;
        font-weight: bold;
        font-family: Arial;
        font-size: 18px;
        color : #eeeeee;
    }

</style>

<script type="text/javascript">

    var errorId ;
    var eventId;
    var controlId ;
    var timer;

    function init ()
    {
        errorId = document.getElementById("error");
        eventId = document.getElementById("event");
        controlId = document.getElementById("control");

        global . ir . error .connect(onError);
        global . ir . event.connect(onEvent);

        var ctrls = global. ir . availableControls ;

        for (var i = 0;i < ctrls .length; i++)
        {
            controlId .options.add(new Option(ctrls[i ], i )) ;
        }
    }

    function onError(err)
    {
        errorId .innerHTML = err;
    }

    function onEvent(key, skey, config)
    {
        eventId.innerHTML = "" + key + ' ' + skey + ' ' + config;

        clearTimeout(timer);
        timer = setTimeout(function() { eventId.innerHTML = ""; }, 750);
    }

    function setControl()
    {
        {
            try
            {
                global . ir .setCurrentControl(controlId.options[ controlId .selectedIndex ]. text) ;

                /*
                * In order to use the browser property, you should set 'browser.ir . configuration
                .enabled'

```

```

    * to 'true' and 'browser.ir . configuration ' to the valid LIRC config in the device
    profile .
    * Then you will be able to set the control from the browser property:
    *
    * global . ir .setCurrentControl(); // leave the device name empty
    */
    }
    catch(ex)

{
    alert ("Exception: " + ex);
}
}

</script>

</head>

<body onload="init()">
    Control: <select size="1" id="control"></select><input type="button" value="Apply"
onclick="
setControl()" /><br><br>
    Event: <span id="event"></span><br><br>
    Error log : <span id="error"></span>
</body>

</html>

```





## APPENDIX **F**

# Video Conferencing Using the Session Initiation Protocol Client

---

Revised: January 29, 2014, OL-26457-05

## Appendix Overview

The Session Initiation Protocol (SIP) client enables a customer at the kiosk to make a SIP audio and video call with a remote assistant.

Topics in this appendix include:

- [SIP Recommendations, page F-1](#)
- [SipPhone Widget, page F-2](#)
  - [Sample Test Code, page F-4](#)
- [IEC Preparation, page F-12](#)
- [SIP Client, page F-12](#)
- [Cisco IP Phone Set Up on the CUCM, page F-12](#)
  - [Finding The IP Phone's MAC Address, page F-23](#)
- [Cisco IEC Set Up on the CUCM, page F-24](#)
- [Configuring Call Manager Information, page F-36](#)
  - [Using a Policy on the IEM, page F-36](#)
  - [Using the SipPhone Widget, page F-42](#)
- [SIP DTMF, page F-43](#)
  - [Sample usage of sendDtmf\(\) API, page F-44](#)

## SIP Recommendations

The following are recommendations when using SIP:

- SIP video quality is dependent on the available network link. At least 1Mbps of available bandwidth between the end-points is recommended for HD-quality video call.

- Since HD quality is affected greatly by poor network design, it is recommended that the network link is not congested.
- When using the SIP widget with another video application such as the video player, ensure that all videos have stopped when SIP receives an incoming signal.
- Use an USB external microphone and USB speakers to get the best result for echo cancellation.
- Use a recommended camera for HD quality video such as the Cisco PrecisionHD camera or Logitech C920 camera.

## SipPhone Widget

Cobra provides several proprietary widgets to simplify developer's life. Those widgets can be configured and controlled from JavaScript. The sipphone widget allows you to make SIP phone calls to another SIP endpoint. This plugin acts like a True SIP endpoint and supports both audio and video calls. Both SD (g711) and HD (g7221) audio codecs are supported. For video, it supports H.263 and H.264 codecs.

The sipphone interface declaration is:

```
interface SipPhone
{
    attribute int height;
    attribute int width;
    attribute string backgroundColor;
    attribute string idleImage;
    attribute bool videoEnabled; // Is true by default.
    attribute string status;

slots:

    int start (in string username,
               in string password,
               in string domain,
               in string transport);
    void call(in string sipUri);
    void hangup();
    void sendDtmf(in string dtmfkey);
    bool setidleImage(in string imgurl, in bool stretchFlag);
    bool changeidleImage(in string imgurl, in bool stretchFlag);

signals:

    void ready();
    void registered();
    void placingCall();
    void incomingCall();
    void established();
    void ring();
    void disconnected();
    void error(in int code, in string explanation);
};
```

**Table F-1** *sipphone Variables*

<code>start(in string username, in string password, in string domain, in string transport)</code>	This method call is to be used to set the SIP credentials that are needed to get registered with the SIP Registrar (or Call Manager). The needed credentials are Username, Password, Domain (IP Address or Domain Name of the SIP Registrar) and the transport to be used (UDP or TCP).
<code>call(in string sipUri)</code>	This method should be used only after the <code>start(...)</code> method is called. This method initiates the call to the sipUri (called party).
<code>hangup()</code>	This method, when called, disconnects the existing call.
<code>sendDtmf(in string dtmfkey)</code>	This method sends DTMF tones to the SIP proxy. Valid DTMF keys are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, *, and #.
<code>setIdleImage(in string imgUrl, in bool stretchFlag)</code>	This method can be used to display an image, like logo or some graphic when the SIP widget is registered and not in a call. This method provides a mechanism for the widget to display an image when it is not in a call. The parameters are imgUrl, the URL for the image to be displayed, and stretchFlag, which indicates whether to auto resize or not the image to the given frame.
<code>changeIdleImage(in string imgUrl, in string sipUri)</code>	This method is similar in functionality to <code>setIdleImage</code> . You could use this method to change the appearance of the widget like coding it in javascript to change the idleimage to create the sense of screen saver for the widget.
<code>ready()</code>	This signal is indicative that values given for initializing the sipphone are accepted.
<code>registered()</code>	This signal means that the sipphone is now registered with the SIP Registrar (or Call Manager) and you can make and receive calls from the widget.
<code>placingCall()</code>	This signal means the widget is trying to place the call to the called party of interest.
<code>incomingCall()</code>	This signal means the widget is receiving an incoming call request from another SIP peer.
<code>established()</code>	This signal is indicative that the call is in progress.
<code>ring()</code>	This signal means that the called party has been notified about the incoming call.
<code>disconnected()</code>	This signal means that the call has been terminated.
<code>error(in int code, in string explanation)</code>	This signal is indicative of any errors whilst the widget operation. The signal has a code and an explanation about the error that was encountered.

## Sample Test Code

```
<!-- IEC-4.155.393 -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>SIP phone</title>
    <style type="text/css">
      html, body {padding:0; margin:0; width:100%; height:100%}
      body {background: #1e2024; color: #ffffff; font:normal 12px Arial, Helvetica,
      sans-serif;}
      body {background: -webkit-gradient(linear, left top, left bottom,
      color-stop(0%,rgba(180,180,177,1)), color-stop(32%,rgba(214,213,212,1)),
      color-stop(100%,rgba(255,255,255,1))); background: -webkit-linear-gradient(top,
      rgba(180,180,177,1) 0%,rgba(214,213,212,1) 32%,rgba(255,255,255,1) 100%);}
      ul, ol, li {padding:0; margin:0;}
      .vbox, .hbox {
        display: -webkit-box;
        display: box;
        -webkit-box-pack: justify;
        box-pack: justify;
        text-align:justify;
        text-align:center;
      }
      .vbox {
        -webkit-box-orient: vertical;
        box-orient: vertical;
      }
      .hbox {
        -webkit-box-orient: horizontal;
        box-orient: horizontal;
      }
      .fullwindow {
        height:100%; width:100%;
        display: -webkit-box;
        display: box;
        -webkit-box-orient: horizontal;
        box-orient: horizontal;
        -webkit-box-pack: justify;
        box-pack: justify;
      }
      /*===== SIP =====*/
      .LED_red, .LED_green, .LED_white, .LED_off {width:44px; height:24px;
      background:transparent url('img/LED_off.png') center center no-repeat;}
      .LED_red {background-image:url('img/LED_red.png');}
      .LED_green {background-image:url('img/LED_green.png');}
      .LED_white {background-image:url('img/LED_white.png');}
      .topPanel {background:#0e1014 url('img/top_panel_bg.png') top left repeat-x;
      color:#4c5058; text-shadow:0 -1px 1px #000; font:normal 14px Arial, Helvetica,
      sans-serif; height:41px;}
      .status {color:#848d9d; text-shadow:0 -1px 1px #000; font:normal 14px Arial,
      Helvetica, sans-serif; padding:0 20px}
      .bottomPanel {background:#0e1014 url('img/bottom_panel_bg.png') top left repeat-x;
      color:#4c5058; text-shadow:0 -1px 1px #000; font:normal 14px Arial, Helvetica,
      sans-serif; height:80px;}
      .calltime {color:#b1b6c3; font:normal 14px Arial, Helvetica, sans-serif;
      height:41px; text-shadow:0 -1px 1px #000;}
      .buttons {text-align:center; display:inline-block; padding:0 30px 0 30px;}
      .greenButton, .redButton, .callButton, .endCallButton, .hangupButton,
      .acceptButton, .rejectButton {width:170px; height:56px; background:transparent;
      -webkit-border-image: url('img/greenButton_disabled.png') 1 10 1 10 stretch
```

```

stretch; border-width:1px 10px 1px 10px; color:rgba(255,255,255,.9); font:normal
22px Arial, Helvetica, sans-serif; padding-top:6px; text-shadow:0 -1px 1px
rgba(0,0,0,.6)}
.greenButton, .callButton, .acceptButton {-webkit-border-image:
url('img/greenButton_idle.png') 1 10 1 10 stretch stretch;}
.greenButton:hover, .callButton:hover, .acceptButton:hover {-webkit-border-image:
url('img/greenButton_hover.png') 1 10 1 10 stretch stretch;}
.greenButton:active, .callButton:active, .acceptButton:active
{-webkit-border-image: url('img/greenButton_pressed.png') 1 10 1 10 stretch
stretch;}
.greenButton:disabled, .callButton:disabled, .acceptButton:disabled
{-webkit-border-image: url('img/greenButton_disabled.png') 1 10 1 10 stretch
stretch; color:#51565d}
.redButton, .endCallButton, .hangupButton, .rejectButton {-webkit-border-image:
url('img/redButton_idle.png') 1 10 1 10 stretch stretch;}
.redButton:hover, .endCallButton:hover, .hangupButton:hover, .rejectButton:hover
{-webkit-border-image: url('img/redButton_hover.png') 1 10 1 10 stretch stretch;}
.redButton:active, .endCallButton:active, .hangupButton:active,
.rejectButton:active {-webkit-border-image: url('img/redButton_pressed.png') 1 10
1 10 stretch stretch;}
.redButton:disabled, .endCallButton:disabled, .hangupButton:disabled,
.rejectButton:disabled {-webkit-border-image: url('img/redButton_disabled.png') 1
10 1 10 stretch stretch; color:#51565d}
.view {background:#000; border:solid 1px #3b3d40; text-align:center; width:640px;
height:380px;}
.timerOn, .timerOff {color:#b1b6c3; font:normal 36px Arial, Helvetica, sans-serif;
height:41px; text-shadow:0 -1px 1px #000;}
.timerOff {color:#292e33}
.dialpad_disabled {width:43px; height:43px; background:transparent
url('img/dialpad_disabled.png') center center no-repeat; border:none}
</style>
<script>
var sipphone, sipButton, sipRejectButton, sipTimer, sipStatus, sipRegistered;
var callInProgress;
var sip_target = "133";
var sip_username = "vep1";
var sip_password = "user132resu";
var sip_domain = "192.168.0.108";
var sip_transport = "udp";
var useApplicationData = true;
function initSIP(){
writeLog('Starting SIP widget:');
callInProgress = false;
sipphone = document.getElementById("sipphone");
sipbutton = document.getElementById("CallButton");
//sipRejectButton = document.getElementById("RejectButton");
sipTimer = document.getElementById("callTimer");
sipRegistered = document.getElementById("registeredLED");
sipStatus = document.getElementById("SIPstatus");
var default_target = sip_target;
var default_username = sip_username;
var default_password = sip_password;
var default_domain = sip_domain;
var default_transport = sip_transport;
if(useApplicationData){
writeLog('Using application data.');
```

// These are the Credentials for the SIP endpoint

// It is recommended that you use the

// Application Data at the IEM profile to set these

// Values and get them via the global.applicationData.value() API.

```

sip_target = global.applicationData.value("sip.target", default_target);
sip_username = global.applicationData.value("sip.username", default_username);
sip_password = global.applicationData.value("sip.password", default_password);
sip_domain = global.applicationData.value("sip.domain", default_domain);

```

```

sip_transport = global.applicationData.value("sip.transport", default_transport)
}
writeLog("username = "+sip_username+"<br>"+"password = "+sip_password+"<br>"+"domain = "+sip_domain+"<br>"+"transport = "+sip_transport+"<br>"+"target = "+sip_target+"<br>");
sipbutton.disabled = true;
sipRegistered.className = "LED_off";
countDown(0);
sipStatus.innerHTML = "Connecting to server...";
writeLog("Starting SIP daemon...");
sipphone.start(sip_username, sip_password, sip_domain, sip_transport);
writeLog("Connecting signals...");
sipphone.ready.connect(onReady); writeLog("onReady() connected to sipphone.ready");
sipphone.registered.connect(onRegistered); writeLog("onRegistered() connected to sipphone.registered");
sipphone.placingCall.connect(onPlacingCall); writeLog("onPlacingCall() connected to sipphone.placingCall");
sipphone.established.connect(onEstablished); writeLog("onEstablished() connected to sipphone.established");
sipphone.disconnected.connect(onDisconnected); writeLog("onDisconnected() connected to sipphone.disconnected");
sipphone.ring.connect(onRing); writeLog("onRing() connected to sipphone.ring");
sipphone.incomingCall.connect(onIncomingCall); writeLog("onIncomingCall() connected to sipphone.incomingCall");
sipphone.error.connect(onError); writeLog("onError() connected to sipphone.error");
writeLog("SIP widget started, all signals are connected.");
}
function onReady(){
writeLog("sipphone.status = "+sipphone.status);
sipbutton.disabled = true;
sipbutton.className="callButton";
sipbutton.innerHTML="Call";
sipStatus.innerHTML = "Ready";
sipTimer.className = "timerOff";
//sipRegistered.className = "LED_white";
writeLog('onReady() READY');
}
var checkRegistrationStatusTimeout;
function onRegistered(){
clearTimeout(checkRegistrationStatusTimeout);
writeLog("sipphone.status = "+sipphone.status);
var success = (sipphone.status=="register successful"); // CHECK REGISTRATION STATUS
if(success){
sipbutton.disabled = false;
sipbutton.className="callButton";
sipbutton.innerHTML="Call";
sipStatus.innerHTML = "Ready";
sipTimer.className = "timerOff";
sipRegistered.className = "LED_green";
writeLog('onRegistered() REGISTERED');
} else {
sipbutton.disabled = true;
sipbutton.className="callButton";
sipbutton.innerHTML=" ";
sipStatus.innerHTML = "Connecting to server...";
sipTimer.className = "timerOff";
sipRegistered.className = "LED_off";
writeLog('Waiting for server...');
checkRegistrationStatusTimeout = setTimeout("onRegistered()", 15000);
}
}
}

```

```

function onPlacingCall(){
writeLog("sipphone.status = "+sipphone.status);
sipbutton.className="hangupButton";
sipbutton.innerHTML="Cancel";
sipStatus.innerHTML = "Placing call...";
sipTimer.className = "timerOn";
writeLog('onPlacingCall()');
}

function onIncomingCall(){
writeLog("sipphone.status = "+sipphone.status);
sipbutton.disabled = false;
sipbutton.className="acceptButton";
sipbutton.innerHTML="Accept Call";
sipStatus.innerHTML = "Incoming call";
sipTimer.className = "timerOn";
writeLog('onIncomingCall()');
}

function onEstablished(){
writeLog("sipphone.status = "+sipphone.status);
callInProgress = true;
sipbutton.disabled = false;
sipbutton.className="hangupButton";
sipbutton.innerHTML="End Call";
sipStatus.innerHTML = "In Call";
sipTimer.className = "timerOn";
countDown(1);
writeLog("onEstablished()");
writeLog("callInProgress = "+callInProgress);
}

function onRing(){
writeLog("sipphone.status = "+sipphone.status);
sipbutton.disabled = false;
sipbutton.className="hangupButton";
sipbutton.innerHTML="Cancel";
sipStatus.innerHTML = "Calling...";
sipTimer.className = "timerOn";
writeLog('onRing()');
}

function onDisconnected(){
writeLog("sipphone.status = "+sipphone.status);
callInProgress = false;
sipbutton.disabled = false;
sipbutton.className="callButton";
sipbutton.innerHTML="Call";
sipStatus.innerHTML = "Ready";
sipTimer.className = "timerOff";
countDown(0);
writeLog('onDisconnected()');
}

var t1;
function onError(code, explanation){
writeLog("sipphone.status = "+sipphone.status);
callInProgress = false;
sipbutton.disabled = true;
sipbutton.className="callButton";
sipbutton.innerHTML="Call";
sipTimer.className = "timerOff";
countDown(0);
switch(code){
case 404:
sipStatus.innerHTML = "<span style='color:#ff0000;'>No answer</span>";
break;
case 401:
sipStatus.innerHTML = "<span style='color:#ff0000;'>Registration failed</span>";

```

```

break;
default:
sipStatus.innerHTML = "<span style='color:#ff6920;'>Error</span>";
break;
}
t1 = setTimeout(function(){
sipbutton.disabled = false;
sipStatus.innerHTML = "Ready";
}, 30000);
writeLog("onError() " + explanation + " (SIP code = " + code + ")");
}
function makeCall(targetID){
writeLog("sipphone.status = "+sipphone.status);
sipbutton.disabled = true;
var uri = targetID ? targetID : sip_target;
uri = uri.indexOf("sip:")<0 ? "sip:" + uri : uri;
if(callInProgress){
callInProgress = false;
sipphone.hangup();
writeLog("hangup(); callInProgress = "+callInProgress);
} else {
callInProgress = true;
sipphone.call(uri);
writeLog("calling " + uri+" / callInProgress = "+callInProgress);
}
}
// For Timing to be shown
var sip_sec = 00; // set the seconds
var sip_min = 00; // set the minutes
var sip_hrs = 00; // set the Hours
var sip_OneSecond;
function countdown(flag){
var calltime;
if (flag) {
sip_sec++;
if (sip_sec == 59) {
sip_sec = 00;
sip_min = sip_min + 1;
}
if (sip_min == 59) {
sip_min = 00;
sip_hrs = sip_hrs + 1;
}
if (sip_sec <= 9){
sip_sec = "0" + sip_sec;
}
calltime = (sip_hrs<1 ? "" : ((sip_hrs<=9 ? "0" + sip_hrs : sip_hrs) + ":")) +
(sip_min<=9 && sip_hrs>0 ? "0" + sip_min : sip_min) + ":" + sip_sec;
sipTimer.innerHTML = calltime;
sipTimer.title = "Last call duration: "+calltime;
sip_OneSecond = setTimeout("countDown(1)", 1000);
} else {
sipTimer.innerHTML = "0:00";
clearTimeout(sip_OneSecond);
sip_sec = 00;
sip_min = 00;
}
}
function isDebugMode(){
var l=String(window.location);
var qs=l.substring(l.indexOf("?")+1, l.length);
if(qs.indexOf("debug", 0)>=0){
document.getElementById('appDebugInfo').style.visibility = "visible";
} else {

```



```

document.getElementById('appDebugInfo').style.visibility = "hidden";
}
}
function init(){
isDebugMode();
initSIP();
}
</script>
</head>
<body onLoad="init()">
<div class="fullwindow hbox">
<div class="vbox" style="-webkit-box-flex: 1; box-flex: 1; -webkit-box-pack:
center; box-pack: center;" >
<table border="0" cellpadding="0" cellspacing="0" width="100%" height="100%">
<tr>
<td align="center">
<table border="0" cellpadding="0" cellspacing="1" align="center"
bgcolor="#000000">
<tr>
<td class="topPanel">
<table border="0" cellpadding="0" cellspacing="0" width="100%" height="100%"
style="width:100%; max-width:640px">
<tr>
<td width="49%" style="min-width:160px" align="left"><span class="status"
id="SIPstatus">&nbsp;</span></td>
<td align="center">
<div style="min-width:162px">
<table border="0" cellpadding="0" cellspacing="0" height="100%">
<tr>
<td width="44"><div style="width:44px">&nbsp;</div></td>
<td width="74" align="center" style="width:74px"></td>
<td width="44"></td>
</tr>
</table>
</div>
</td>
<td width="49%" style="min-width:160px" align="right">&nbsp;</td>
</tr>
</table>
</td>
<td class="view">
<object id="sipphone" type="application/x-qt-plugin" classid="sipphone"
width="640" height="380" backgroundColor="#333333"></object>
</td>
</tr>
<tr>
<td class="bottomPanel">
<table border="0" cellpadding="0" cellspacing="0" width="100%" height="100%"
style="width:100%; max-width:640px">
<tr>
<td align="right" width="49%" style="min-width:160px"><span class="timerOff"
id="callTimer" title="">&nbsp;</span></td>
<td align="center"><div class="buttons"><button id="CallButton" class="callButton"
onclick="makeCall();" disabled="disabled">Call</button></div></td>
<td width="49%" style="min-width:160px; text-align:right"><div
style="display:inline-block; padding:0 20px; width:80%; text-align:left"><input
type="button" value="" id="dialpad" class="dislpad_disabled" /></div></td>
</tr>
</table>
</td>

```

```

</tr>
</table>
</td>
</tr>
</table>
</div>
</div>
<div style="display:none; visibility:hidden">
<!-- chaching images -->















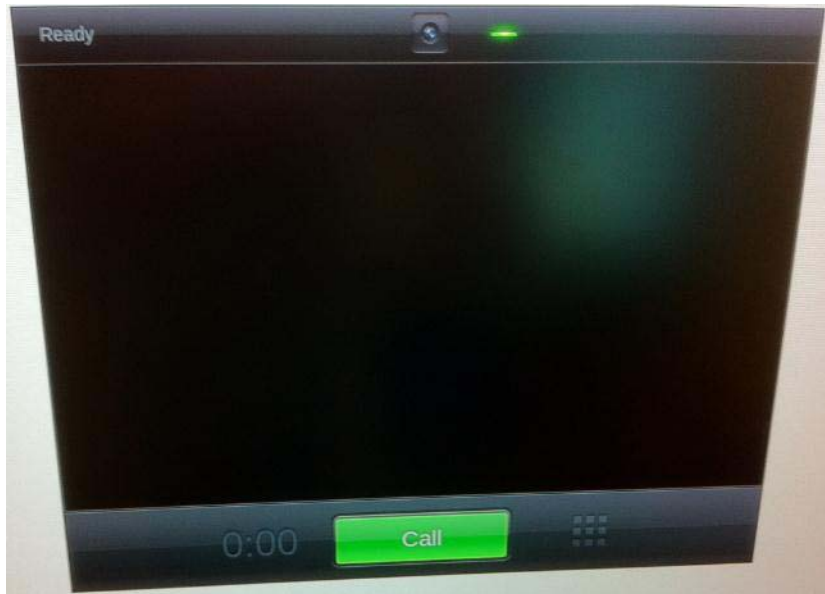

</div>
<!-- This part of code is used for tracing application states -->
<div id="appDebugInfo" style="visibility:hidden; background:rgba(0,0,0,.75);
position:absolute; top:0; left:0; width:300px; overflow-x:hidden;
overflow-y:scroll; color:white; padding:20px; font:normal 10px/12px
sans-serif"></div>
<script>
function writeLog(msg){
var c = document.getElementById('appDebugInfo');
if(c){
c.innerHTML=c.innerHTML + msg + "<br><br>";
}
}
document.getElementById('appDebugInfo').style.height =
document.body.offsetHeight-100+"px";
</script>
</body>
</html>

```

The above HTML code creates a sample widget to test SIP.

1. Copy the above contents to an HTML file and transfer the file to a web server from where it can be accessed. Make sure to have the location of the file as a URL.
2. Register the IEC and the other endpoint on CUCM (see instructions below)
3. Create a policy with startup URL as the URL of the above script. Make changes to the application->data property in the policy. Apply the policy. (see instructions below)

**Figure F-2**      **Sample Result - Ready State on Kiosk**



**Figure F-3**      **Sample Result - Call State on Kiosk**



**Note**

The resolution of the video call from a Cisco video IP phone is fixed. It cannot be adjusted.

# IEC Preparation

The following steps must be done before setting up the SIP client.

- 
- Step 1** Make sure that the IEC is installed, registered, configured, and up and running. Confirm that the startup URL is displaying.
- Step 2** Connect a webcam using a USB cable to a USB port on the IEC.
- Step 3** Connect a microphone to the IEC. You can connect the microphone to either a USB port or the MIC-in port (shown on the figure below as the pink port with the microphone icon).

**Figure F-4** MIC-in Port on the IEC



## SIP Client

In order for the SIP to work, the Cisco IEC 4600 Series device and Cisco IP Phone will need to be configured on the Cisco Unified Communications Manager (CUCM) and then configured on the Cisco IEM.

To install the SIP Client, you will need the following:

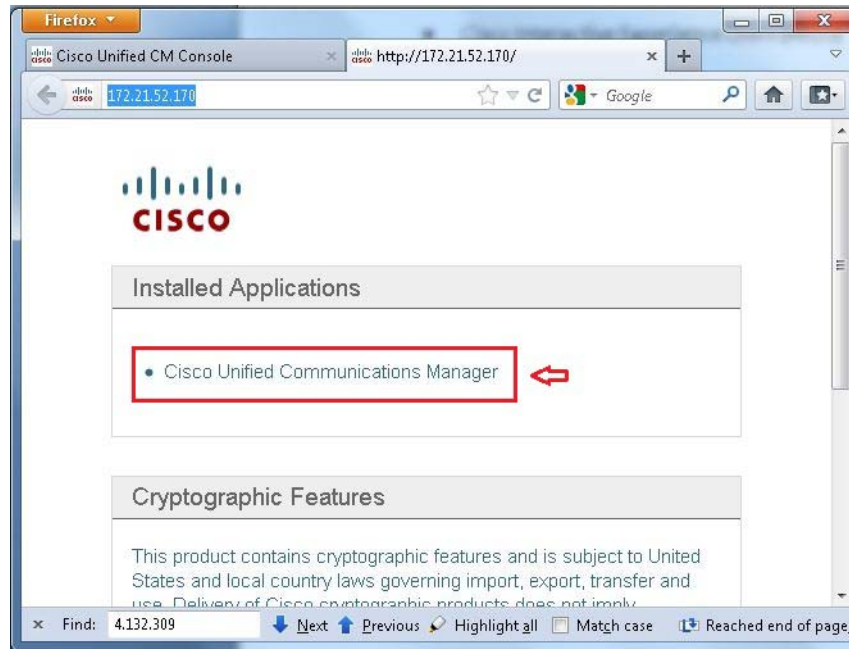
- CUCM v8.6.2 or 9.0
- Cisco IEC4610 or IEC4632
- Cisco Unified IP Phone 9951
- Cisco TelePresence PrecisionHD USB Camera

## Cisco IP Phone Set Up on the CUCM

The following steps will set up a Cisco Unified IP Phone 9951 on the CUCM. Modify the values entered if you are setting up a different phone, Tandberg, or TelePresence.

- Step 1** Enter the IP address of your CUCM in your browser.
- Step 2** Press the **Enter** button.
- Step 3** In the CUCM main page, select **Cisco Unified Communications Manager**.

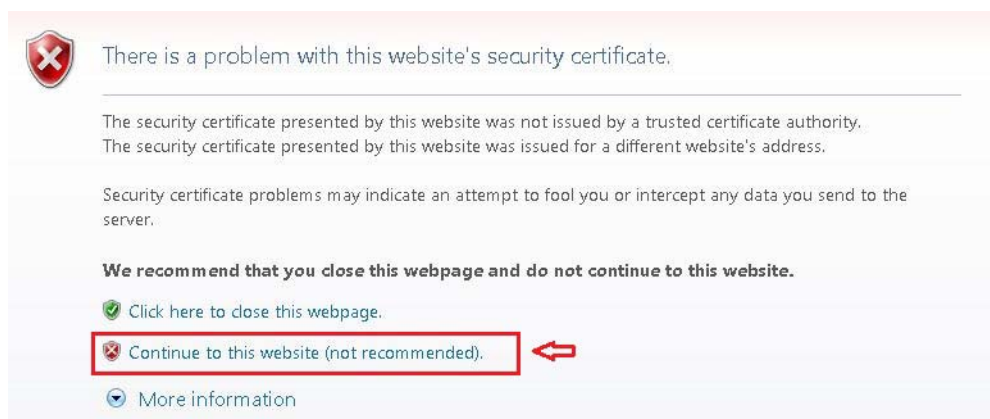
**Figure F-5** CUCM Main Page



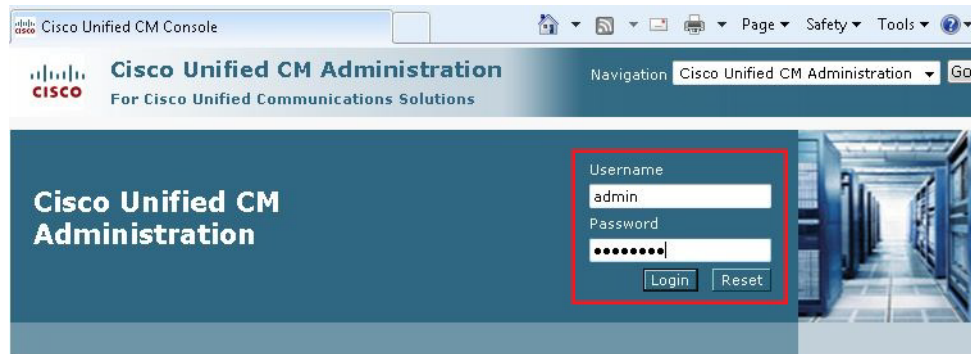
You will be prompted to the Website's Security Certificate page.

- Step 4** On the Website's Security Certificate page, click **Continue to this website (Not Recommended)**.

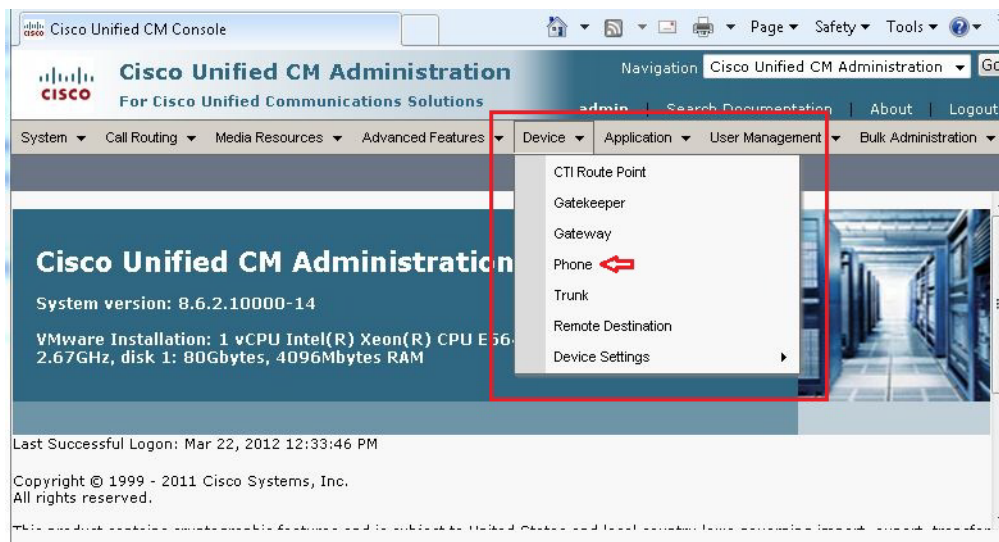
**Figure F-6** Website's Security Certificate Page



- Step 5** Enter **admin** in the Username field of the Cisco Unified CM Administration page.

**Figure F-7** Cisco Unified CM Administration Page

- Step 6** Enter the password in the Password field.
- Step 7** Click **Login** button.
- Step 8** From the Device drop-down menu, choose **Phone**.

**Figure F-8** Device Drop-Down Menu

- Step 9** Click the **Find** button.

**Figure F-9 Find and List Phones Screen**

The screenshot shows the 'Find and List Phones' interface in the Cisco Unified CM Administration console. The page title is 'Find and List Phones'. Below the navigation bar, there's a section for 'Find Phone where' with a dropdown menu set to 'Device Name' and a search input field. A red box highlights the 'Find' button. To the right of the 'Find' button are 'Clear Filter', '+', and '-' buttons. Below the search input field, it says 'Select item or enter search text'. At the bottom of the search section, it says 'No active query. Please enter your search criteria using the options above.' and there is an 'Add New' button.

All the devices registered on the CUCM will be listed.

**Step 10** To add a new phone, click **Add New**.

**Figure F-10 Add New Phone Button**

The screenshot shows the 'Find and List Phones' interface with a list of phones. The 'Add New' button is highlighted with a red box. The list shows 50 records found. The table has columns: Device Name(Line), Description, Device Pool, Device Protocol, Status, IP Address, Copy, and Super Copy. The first four rows are highlighted.

Device Name(Line)	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
CTI_7654	Unified CM Telephony Group #0-1	Default	SCCP	Registered with 172.21.52.170	172.21.52.171	Copy	Super Copy
CTI_7655	Unified CM Telephony Group #0-1	Default	SCCP	Registered with 172.21.52.170	172.21.52.171	Copy	Super Copy
CTI_7656	Unified CM Telephony Group #0-1	Default	SCCP	Registered with 172.21.52.170	172.21.52.171	Copy	Super Copy
CTI_7657	Unified CM	Default	SCCP	Registered	172.21.52.171	Copy	Super Copy

**Step 11** From the Phone Type drop-down menu, choose **Cisco 9951**.

**Figure F-11** Add a New Phone Screen

add New Phone

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

**Add a New Phone**

Next

**Status**  
Status: Ready

**Select the type of phone you would like to create**

Phone Type\*  
 Cisco 9951  
 Cisco 7961G-GE  
 Cisco 7962  
 Cisco 7965  
 Cisco 7970  
 Cisco 7971  
 Cisco 7975  
 Cisco 7985  
 Cisco 8941  
 Cisco 8945  
 Cisco 8961  
 Cisco 9971  
 Cisco ATA 186  
 Cisco ATA 187  
 Cisco Cius  
 Cisco Cius SP  
 Cisco Dual Mode for Android  
 Cisco Dual Mode for iPhone  
 Cisco E20  
 Cisco IP Communicator  
 Cisco TelePresence  
 Cisco TelePresence 1000  
 Cisco TelePresence 1100  
 Cisco TelePresence 1300-47  
 Cisco TelePresence 1300-65

Next

\*- indicate  
 Create  
 to enable template-based phone creation.

**Step 12** Click **Next**.

**Step 13** Enter the IP phone's MAC address in the MAC Address field within the Device Information area.



**Note** If you do not know the IP phone's MAC address, refer to the section "Finding the IP Phone's MAC Address" at the end of this section.



**Figure F-12**      **Device Information Area**

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes 'Cisco Unified CM Administration' and 'For Cisco Unified Communications Solutions'. The 'Phone Configuration' section is active, showing 'Product Type: Cisco 9951' and 'Device Protocol: SIP'. The 'Device Information' section is highlighted with a red box. It contains the following fields:

- ☒ Device is trusted
- MAC Address\* (with a red arrow pointing to the input field)
- Description (with a red arrow pointing to the input field)
- Device Pool\* (with a red arrow pointing to the dropdown menu, currently showing '-- Not Selected --')
- Common Device Configuration (with a red arrow pointing to the dropdown menu, currently showing '< None >')
- Phone Button Template\* (with a red arrow pointing to the dropdown menu, currently showing '-- Not Selected --')
- Common Phone Profile\* (with a red arrow pointing to the dropdown menu, currently showing 'Standard Common Phone Profile')

Below the 'Device Information' section, there are several other fields with dropdown menus:

- Calling Search Space: < None >
- AAR Calling Search Space: < None >
- Media Resource Group List: < None >
- User Hold MOH Audio Source: < None >
- Network Hold MOH Audio Source: < None >
- Location\*: Hub\_None
- AAR Group: < None >
- User Locale: < None >
- Network Locale: < None >

- Step 14** Enter a description of the IP phone to easily distinguish it from others in the CUCM. This field automatically enters the IP phone's MAC Address but can be modified.
- Step 15** From the Device Pool drop-down menu, choose **Default**.
- Step 16** From the Phone Button Template drop-down menu, choose **Standard 9951 SIP**.
- Step 17** From the Device Security Profile drop-down menu within the Protocol Specific Information area, choose **Cisco 9951 - Standard SIP Non-Secure Profile**.

**Figure F-13 Protocol Specific Information Area**

The screenshot shows the Cisco Unified CM Administration web interface. The 'Phone Configuration' section is active, and the 'Protocol Specific Information' area is highlighted with a red box. Within this area, the following fields are visible:

- Packet Capture Mode\*: None
- Packet Capture Duration: 0
- Presence Group\*: Standard Presence group
- SIP Dial Rules: < None >
- MTP Preferred Originating Codec\*: 711ulaw
- Device Security Profile\*: -- Not Selected --
- Rerouting Calling Search Space: < None >
- SUBSCRIBE Calling Search Space: < None >
- SIP Profile\*: < None >
- Digest User: < None >

Below the Protocol Specific Information area, there are checkboxes for:

- Media Termination Point Required
- Unattended Port
- Require DTMF Reception

At the bottom of the form, there is a section for 'Certification Authority Proxy Function (CAPF) Information'.

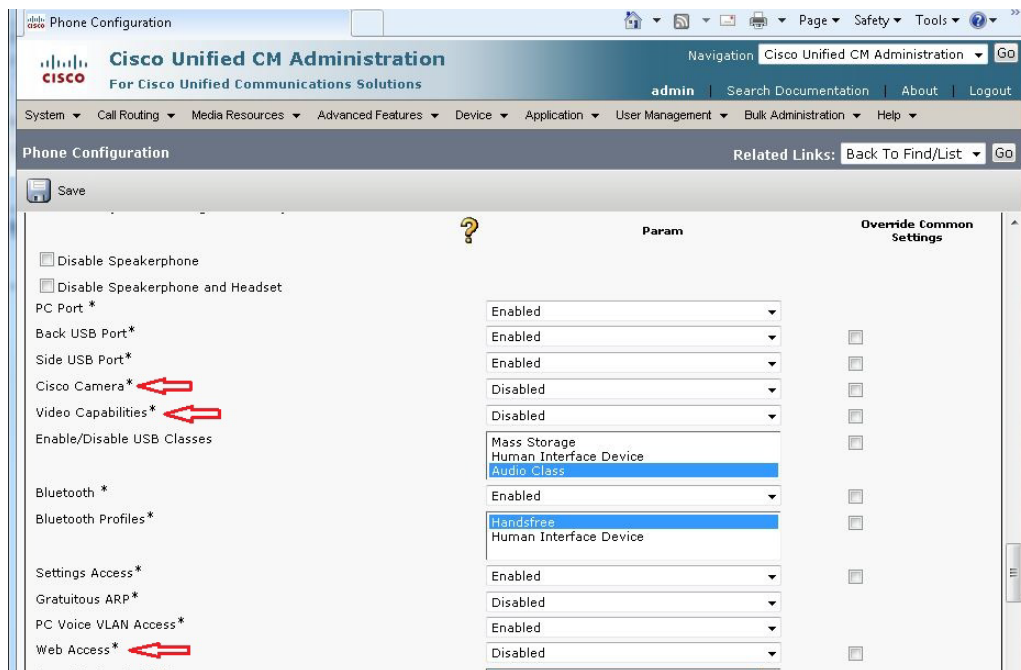
**Step 18** From the SIP Profile drop-down menu, choose **Standard SIP Profile**.

**Step 19** Within the Protocol Specific Information area, go to the Digest User drop-down menu and choose the User ID.

**Figure F-14** Digest User Drop-Down Menu

The screenshot shows the Cisco Unified CM Administration interface. The 'Phone Configuration' page is active, and the 'Protocol Specific Information' section is expanded. The 'Digest User' drop-down menu is open, showing a list of users. The 'None' option is highlighted. The list of users includes: None, 2005, 2006, 2043, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 610, 611, 666, 900, Client1, EnterUsername, John, agent1, agent2, agent3, agentTP1, agentTP3, agentTP4, appadmin, ccx, and lowes.

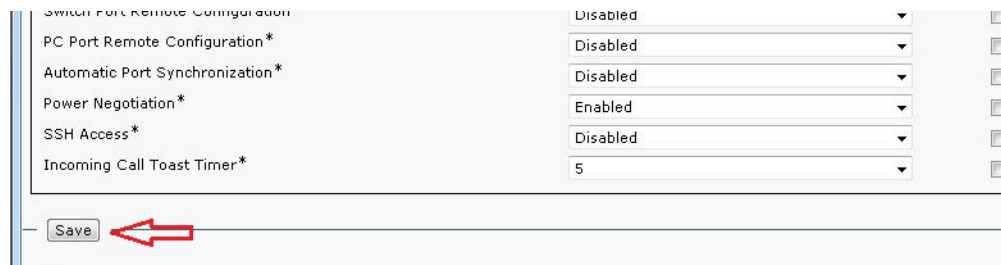
**Step 20** From the Cisco Camera drop-down menu within the Product Specific Configuration Layout, choose **Enabled**.

**Figure F-15 Product Specific Configuration Layout Area**

**Step 21** From the Video Capabilities drop-down menu, choose **Enabled**.

**Step 22** From the Web Access drop-down menu, choose **Enabled**.

**Step 23** Click **Save**.

**Figure F-16 Save Button**

A dialog box appears.

**Step 24** Click **Apply Config**.



**Note** It is important that you first save configurations before applying them. Otherwise, the configurations will be lost.

**Step 25** Click **OK**.

**Step 26** Click **Line [1] – Add a new DN** within the Association Information area.

**Figure F-17 Association Information Area**

Phone Configuration

Find: 5002 Previous Next Options

Cisco Unified CM Administration  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

admin Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

Phone Configuration Related Links: Back To Find/List Go

Save Delete Copy Reset Apply Config Add New

Status  
Add successful

Association Information  
Modify Button Items

1 Line 1 - Add a new DN  
2 Line 2 - Add a new DN  
3 Add a new SD

Phone Type  
Product Type: Cisco 9971  
Device Protocol: SIP

Device Information  
Registration: Unregistered  
IP Address: 10.17.161.18  
Active Inband ID: cin9971-9-2-1

- Step 27** Enter the directory number in the Directory Number field. The directory number must be a number that does not already exist in the CUCM.

**Figure F-18 Directory Number Information Area**

Directory Number Configuration

Find: 5002 Previous Next Options

Cisco Unified CM Administration  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

admin Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

Directory Number Configuration Related Links: Configure Device (SEP64AE0CF66B8C) Go

Save Delete Reset Apply Config Add New

Status  
Status: Ready

Directory Number Information

Directory Number\* 2009  
Route Partition < None >  
Description 2009  
Alerting Name 2009  
ASCII Alerting Name 2009  
☒ Active

Directory Number Settings  
Voice Mail Profile < None > (Choose <None> to use system default)  
Calling Search Space < None >

- Step 28** Enter a description in the Description field. It is good practice to enter the directory number in this field.
- Step 29** Enter a value in the Alerting Name field. It is good practice to enter the directory number in this field too.
- Step 30** Enter a description in the ASCII Alerting Name field. It is good practice to enter the directory number in this field too.
- Step 31** Click **Save**.
- Now that a directory number has been specified, the IP phone must be configured to pick this number and store it. To do so, it has to be linked to the CUCM server.
- Step 32** Go to the IP phone.
- Step 33** Press the System Settings button.

**Figure F-19** System Settings Button on the Cisco Unified IP Phone 9951



**Step 34** Choose the **Administrator Settings** icon, which is button #4 on the Applications screen.

**Figure F-20** Cisco Unified IP Phone 9951 Applications Screen



**Step 35** Choose the Network Setup icon, which is button #1 on the Administrator Settings screen.

**Step 36** Choose the Ethernet Setup icon, which is button #1 on the Network Setup screen.

**Step 37** Choose the IPv4 Setup icon, which is button #1 on the Ethernet Setup screen.

**Step 38** Choose the Alternative TFTP icon, which is button #8 on the IPv4 Setup screen.

**Step 39** In the TFTP Server 1 field, enter the IP Address of the CUCM Server.



## Finding The IP Phone's MAC Address

The Cisco Unified IP phone 9951 has a MAC address, which can be found by one of two methods.

### First Method

There is a label on the bottom of the phone that contains the MAC address.

**Figure F-21**      *MAC Address Label*



### Second Method

**Step 1** Press the System Settings button.

**Figure F-22**      *System Settings Button on the Cisco Unified IP Phone 9951*



**Step 2** Choose the **Administrator Settings** icon, which is button #4 on the Applications screen.

**Tip**

You can either use the touch screen on the display or the numbers on the keypad to navigate the phone settings.

**Figure F-23** Cisco Unified IP Phone 9951 Applications Screen



**Step 3** Choose the Network Setup icon, which is button #1 on the Administrator Settings screen.

**Step 4** Choose the Ethernet Setup icon, which is button #1 on the Network Setup screen.

**Step 5** Choose the MAC Address icon, which is button #2 on the Ethernet Setup screen.

## Cisco IEC Set Up on the CUCM

The Cisco IEC 4600 Series device set up on the CUCM is very similar to the Cisco IP Phone 9951 set up on the CUCM except for a few options. An additional step is also required. This step is the setting up of a User Profile. The User Profile is then linked to the Cisco IEC 4600 Series device after it is set up on the CUCM.

**Step 1** Enter the IP address of your CUCM in your browser.

**Step 2** Press the **Enter** button.

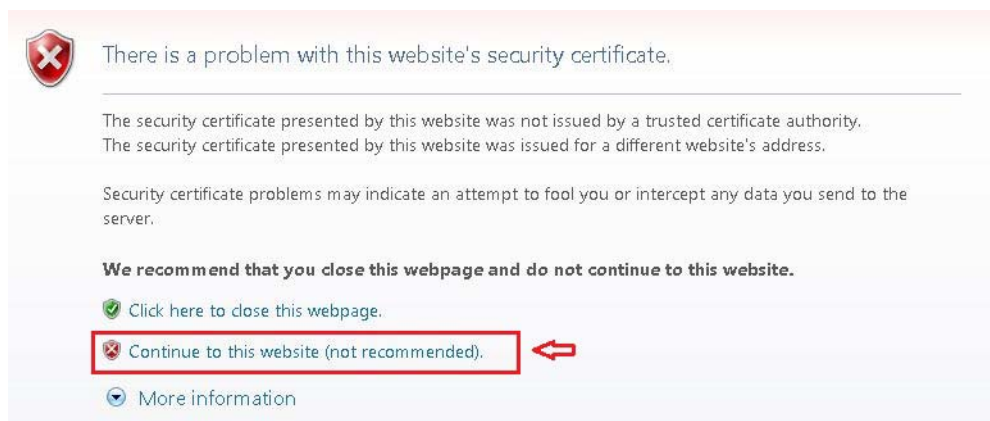
**Step 3** In the CUCM main page, select **Cisco Unified Communications Manager**.



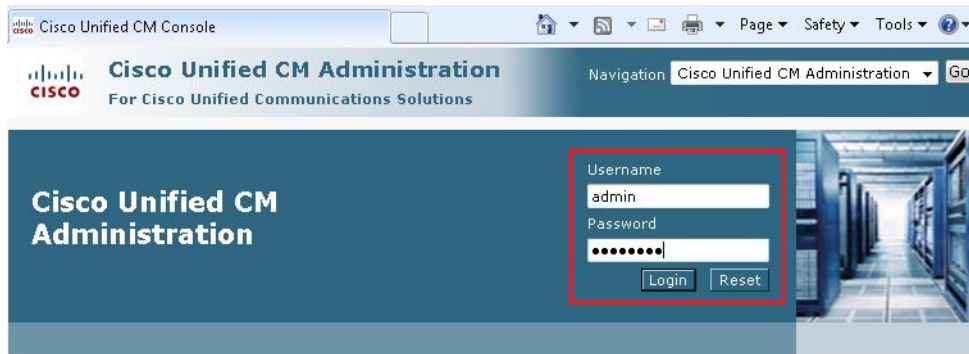
**Figure F-24 CUCM Main Page**

You will be prompted to the Website's Security Certificate page.

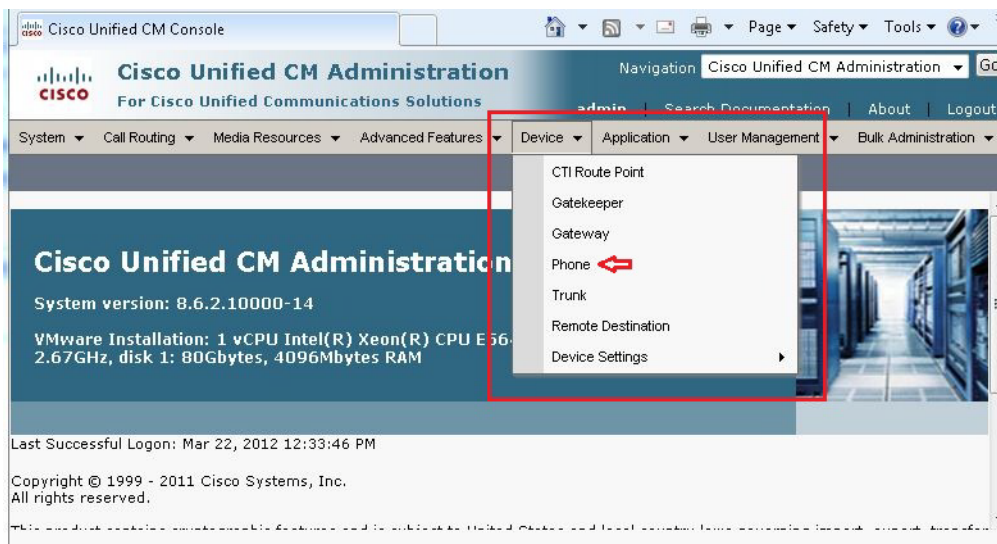
- Step 4** On the Website's Security Certificate page, click **Continue to this website (Not Recommended)**.

**Figure F-25 Website's Security Certificate Page**

- Step 5** Enter **admin** in the Username field of the Cisco Unified CM Administration page.

**Figure F-26 Cisco Unified CM Administration Page**

- Step 6** Enter the password in the Password field.
- Step 7** Click **Login** button.
- Step 8** From the Device drop-down menu, choose **Phone**.

**Figure F-27 Device Drop-Down Menu**

- Step 9** Click the **Find** button.

**Figure F-28 Find and List Phones Screen**

The screenshot shows the 'Find and List Phones' interface in Cisco Unified CM Administration. The page title is 'Find and List Phones'. Below the navigation bar, there's a search section with a dropdown menu set to 'Device Name' and a 'Find' button highlighted with a red box. Other buttons include 'Clear Filter', '+', and '-'. Below the search section, a message states: 'No active query. Please enter your search criteria using the options above.' There is an 'Add New' button at the bottom left.

All the devices registered on the CUCM will be listed.

**Step 10** To add a new phone, click **Add New**.

**Figure F-29 Add New Phone Button**

The screenshot shows the 'Find and List Phones' interface with a list of phones. The 'Add New' button is highlighted with a red box. The list shows 50 records found. The table below lists the first four records:

	Device Name(Line)	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
<input type="checkbox"/>	CTI_7654	Unified CM Telephony Group #0-1	Default	SCCP	Registered with 172.21.52.170	172.21.52.171		
<input type="checkbox"/>	CTI_7655	Unified CM Telephony Group #0-1	Default	SCCP	Registered with 172.21.52.170	172.21.52.171		
<input type="checkbox"/>	CTI_7656	Unified CM Telephony Group #0-1	Default	SCCP	Registered with 172.21.52.170	172.21.52.171		
<input type="checkbox"/>	CTI_7657	Unified CM	Default	SCCP	Registered	172.21.52.171		

**Step 11** From the Phone Type drop-down menu, choose **Third Party SIP Device (Advanced)**.

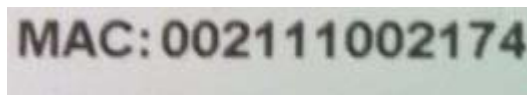
**Figure F-30** *Third-party SIP Device (Advanced) Option*

**Step 12** Click Next.

**Step 13** Enter the Cisco IEC 4600 Series device's MAC address in the MAC Address field within the Device Information area.



**Note** The Cisco IEC 4600 Series device's MAC address is located on the label on the back of the device.

**Figure F-31** *IEC Mac Address Label*

**Step 14** Enter a description of the Cisco IEC 4600 Series device. This field automatically enters "SEP" plus the MAC Address but the field can be modified.

**Figure F-32** Description Field Populated


**Phone Configuration**

 Save

**Status**

 Status: Ready

**Phone Type**

**Product Type:** Third-party SIP Device (Advanced)  
**Device Protocol:** SIP

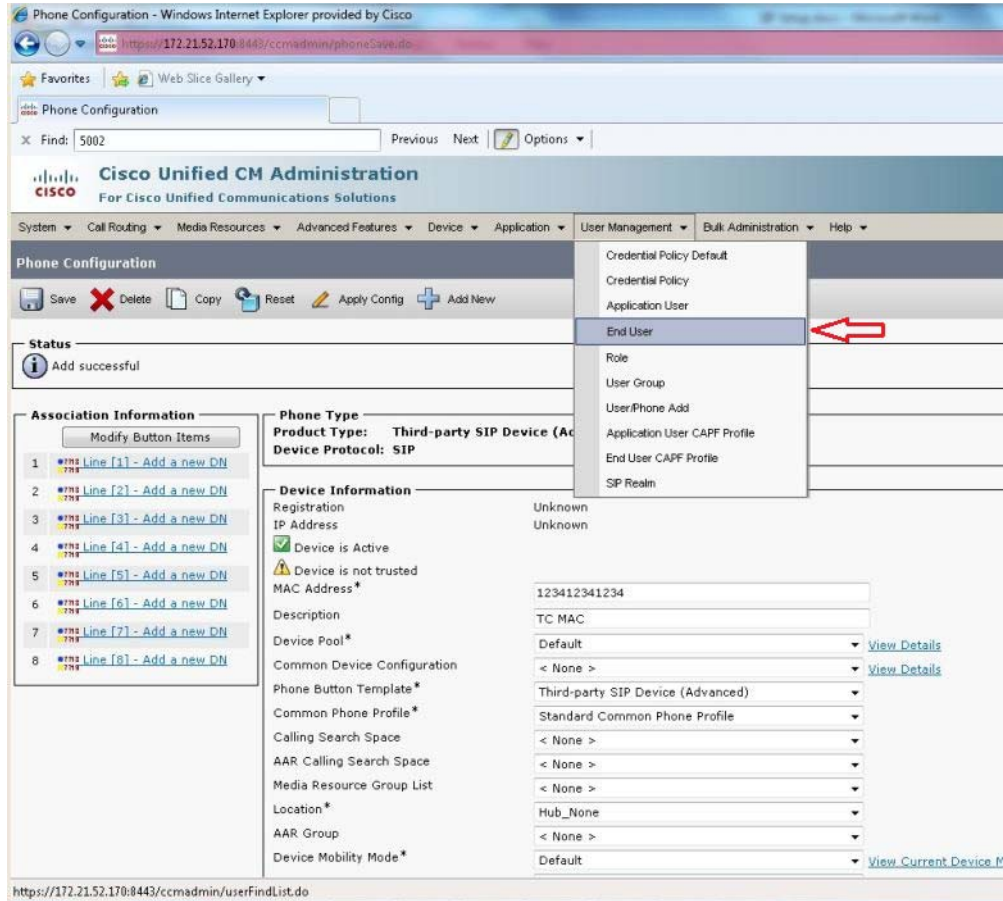
**Device Information**

 Device is not trusted

MAC Address\*

Description

- Step 15** From the Device Pool drop-down menu, choose **Default**.
- Step 16** From the Phone Button Template drop-down menu, choose **Third Party SIP Device (Advanced)**.
- Step 17** From the SIP Profile drop-down menu, choose **Standard SIP Profile**.
- Step 18** From the Device Security Profile drop-down menu, choose **Third-party SIP Device Advanced - Standard SIP Non-secure profile**.
- Step 19** Click **Save**.
- Step 20** Click **Apply Config**.
- In order for the IEC 4600 Series device to be activated, it must be associated with a User Profile.
- Step 21** From the User Management drop-down menu, choose **End User**.

**Figure F-33** User Management Drop-Down Menu

**Step 22** Click **Add New**.

**Step 23** Enter a value in the User ID field. A unique numeric value is required to identify the user. This unique value will be the extension of the SIP device.

**Note**

It is imperative that the value entered in the User ID field is a number. The SIP device will not work if you enter alphabetic characters, punctuation, or spaces.

**Figure F-34** User Information Area

The screenshot shows the 'End User Configuration' page in Cisco Unified CM Administration. The 'User Information' section is highlighted with a red box. Red arrows point to the 'Password', 'Confirm Password', and 'Last name\*' fields. The 'Status' field shows 'Ready'.

- Step 24** Enter a password in the Password field.
- Step 25** Re-enter the password in the Confirm Password field.
- Step 26** Enter the last name of the user in the Last Name field.
- Step 27** Click **Save**.

You will be redirected to a page where you can find the status of your User Profile creation. If all fields have been entered properly the status will indicate 'Add Successful'.

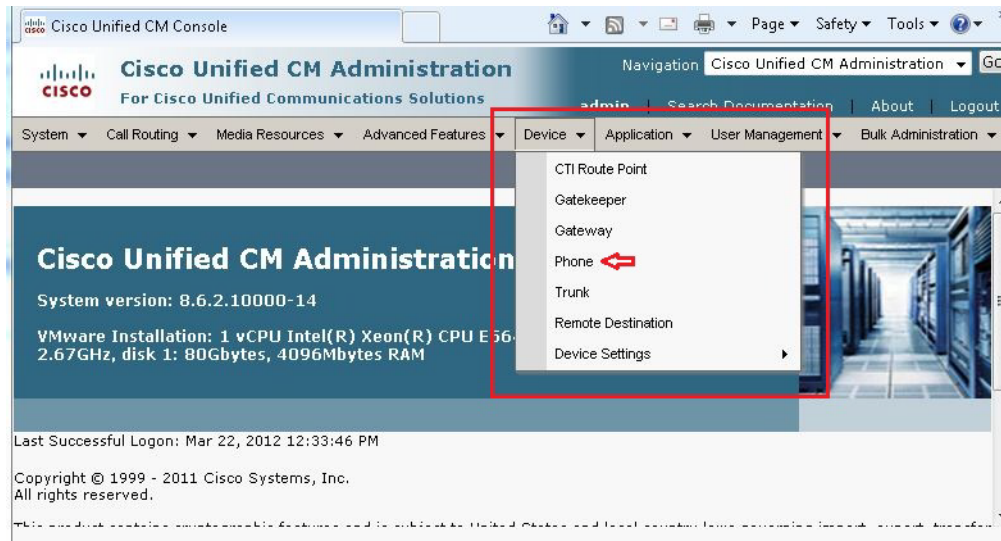
**Figure F-35** Status

The screenshot shows the 'End User Configuration' page after saving. The 'Status' field is highlighted with a red box and shows 'Add successful'. The 'User Information' section is visible below, showing the user ID 'John' and masked password fields with 'Edit Credential' buttons.

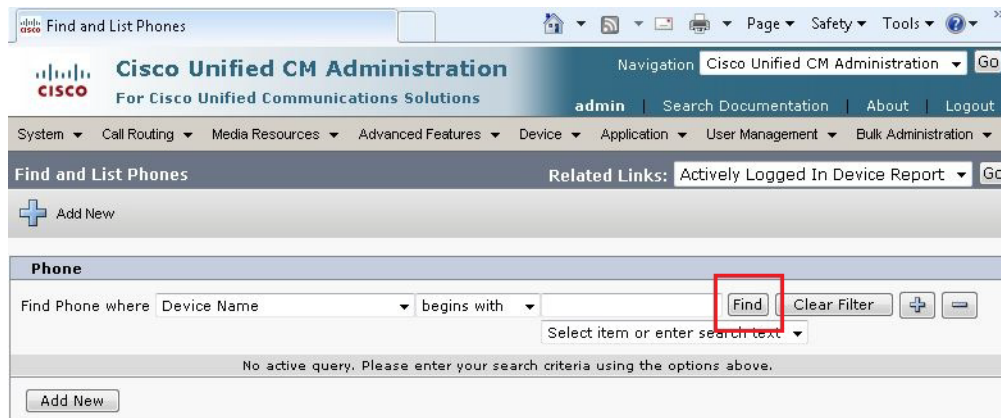
The user profile and the Cisco IEC 4600 Series device on the CUCM must now be linked in order for the phone to work.

- Step 28** From the Device drop-down menu, choose **Phone**.



**Figure F-36** Device Drop-Down Menu

**Step 29** Click the **Find** button.

**Figure F-37** Find Button

All the devices registered on the CUCM will be listed.

**Step 30** Choose the Cisco IEC 4600 Series device, which starts with the letters “SEP” followed by the MAC address.



**Figure F-38** List of Devices

Icon	SEP	Description	Model	Protocol	Status	IP Address
SIP	SEP002145687642	SEP002145687642 (SIP Phone # 610)	Default	SIP	Unregistered	171.6
SIP	SEP0021A02BF2CF	Auto 5001	Default	SIP	Unknown	Unkn
SIP	SEP002233556699	TANDBERG C1700 - QA Guys - (DN 3002)	Default	SIP	Unknown	Unkn
EX60	SEP005060052FFE	Customer - EX60 - DN 2041	Default	SIP	Registered with 172.21.52.170	10.17
EX60	SEP005060058434	Bindu's Cube (3001)	Tandberg	SIP	Registered with 172.21.52.170	10.17
EX60	SEP0050600597A5	Customer - EX90 (2042)	Tandberg	SIP	Registered with 172.21.52.170	10.17
EX60	SEP00506006265A	Frank's Cube (3003)	Tandberg	SIP	Registered with 172.21.52.170	10.17
EX60	SEP00506006265B	EX60 Agent (2043)	Tandberg	SIP	Registered with 172.21.52.170	10.17
EX60	SEP005060068157	Chih's Cube (3000)	Tandberg	SIP	Registered with 172.21.52.170	10.17
EX60	SEP005060068605	EX90 Agent (2044)	Tandberg	SIP	Unknown	Unkn
SIP	SEP012123124155	SEP012123124155 - DN 606	Default	SIP	Unknown	Unkn
SIP	SEP04FE7F6941BD	Auto 5000	Default	SIP	Registered with 172.21.52.170	10.10
SIP	SEP123412341234	TC MAC	Default	SIP	Unknown	Unkn
SIP	SEP1CD0F76F8E7	TP 2004 (Codec)	Default	SIP	Unregistered	10.10
SIP	SEP24B657B04AB9	TP 2004 (Phone)	Default	SIP	Unregistered	10.10
SIP	SEP64AE0CF66BB0	SIP TEST 2009	Default	SIP	Registered with 172.21.52.170	10.17
SIP	SEP64AE0CF6BF16	9971 Phone #2 (2007)	Default	SIP	Unknown	Unkn
SIP	SEP64AE0CF6C00C	9971 Phone #1 (2005)	Default	SIP	Registered with 172.21.52.170	10.17
SIP	SEP68BC0C8181F9	SIP IP Phone - 2010	Default	SIP	Unregistered	10.17

**Step 31** On the Phone Configuration screen, choose **Line [1] – Add a new DN** within the Association Information area.

**Figure F-39** Association Information Area

**Phone Configuration**

Status: Ready

**Association Information**

Modify Button Items

- Line [1] - Add a new DN
- Line [2] - Add a new DN
- Line [3] - Add a new DN
- Line [4] - Add a new DN
- Line [5] - Add a new DN
- Line [6] - Add a new DN
- Line [7] - Add a new DN
- Line [8] - Add a new DN

**Phone Type**

Product Type: Third-party SIP Device (Advanced)

Device Protocol: SIP

**Device Information**

Registration: Unknown

IP Address: Unknown

Device is Active: ☒

Device is not trusted: ☐

MAC Address\*: 123412341234

Description: TC MAC

Device Pool\*: Default [View Details](#)

Common Device Configuration: < None > [View Details](#)

Phone Button Template\*: Third-party SIP Device (Advanced)

The Directory Number Configuration page appears.

**Step 32** Enter a number in the Directory Number field.

**Step 33** Click **Save**.

**Step 34** Click **Associate End Users**.

**Figure F-40 Associate End Users Button**

Users Associated with Line

Full Name	User ID	Permission
EnterLastWam...	EnterUsername	

Associate End Users Select All Clear All Delete Selected

Save Delete Reset Apply Config Add New

\*- indicates required item.  
 \*\*- Changes to Line or Directory Number settings require restart.

Done Internet | Protected Mode: Off 100%

The user list screen appears.

**Step 35** Click **Find**.

**Step 36** Check the check box next to the user that you would like to associate the IEC directory number.

**Figure F-41 List of Users**

Find and List Users - Windows Internet Explorer provided by Cisco

https://172.21.52.170:8443/ccmadmin/userFindList.do?whereClause=pkid not in (select fkenduser fro... Certificate Error

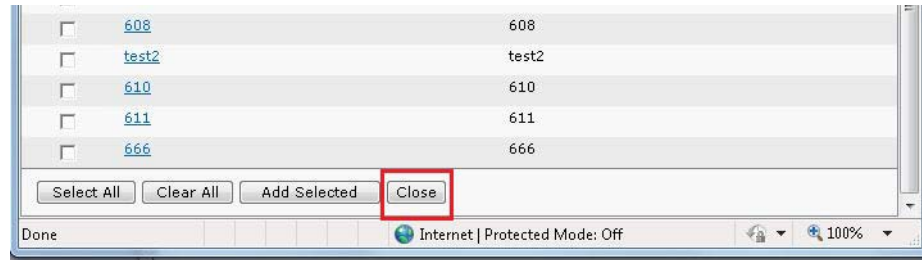
Select All Clear All Add Selected Close

<input type="checkbox"/>	600	600
<input type="checkbox"/>	appadmin	appadmin
<input type="checkbox"/>	agent1	agent1
<input type="checkbox"/>	agentTP3	agentTP3
<input type="checkbox"/>	ccx	ccx
<input type="checkbox"/>	agent2	agent2
<input type="checkbox"/>	agent3	agent3
<input type="checkbox"/>	2043	2043
<input type="checkbox"/>	602	602
<input type="checkbox"/>	603	603
<input type="checkbox"/>	2006	2006
<input type="checkbox"/>	604	604
<input checked="" type="checkbox"/>	John	Smith
<input type="checkbox"/>	900	900
<input type="checkbox"/>	lowes	lowes
<input type="checkbox"/>	Client1	Cisco
<input type="checkbox"/>	605	605
<input type="checkbox"/>	agentTP4	agentTP4
<input type="checkbox"/>	agentTP1	agentTP1
<input type="checkbox"/>	606	606
<input type="checkbox"/>	607	607
<input type="checkbox"/>	608	608

Internet | Protected Mode: Off 100%

**Step 37** Click **Add Selected**.

**Step 38** Click **Close**.

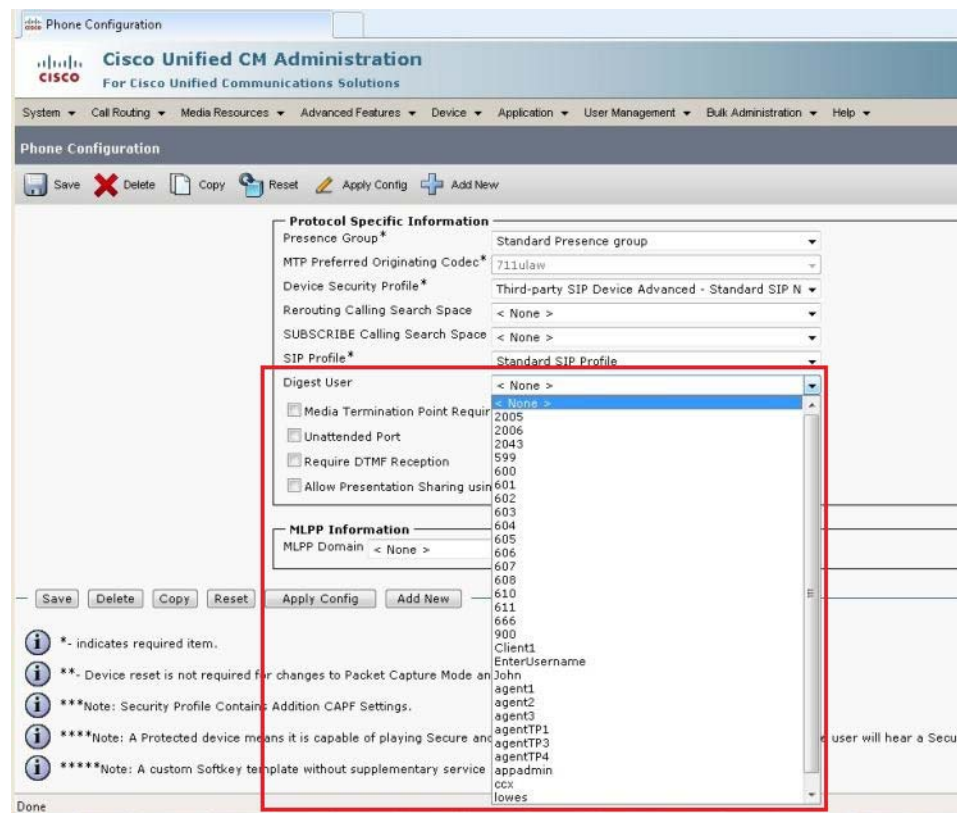
**Figure F-42 Close Button**

**Step 39** From the Device drop-down menu, choose Phone.

**Step 40** Click **Save**.

**Step 41** Click **Apply Config**.

**Step 42** Within the Protocol Specific Information area, go to the Digest User drop-down menu and choose the User ID.

**Figure F-43 Digest User Drop-Down Menu**

**Step 43** Click **Save**.

**Step 44** Click **Apply Config**.

This Cisco IEC 4600 Series device is now registered on the CUCM.

## Configuring Call Manager Information

Once the end points (the video IP phone and an IEC) have been registered on the CUCM, you have several options for configuring the call manager information so that the IEC can call or receive calls from the video IP phone:

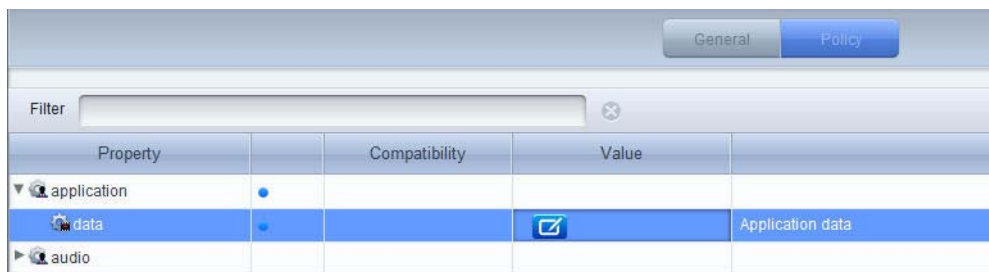
- You can enter the call manager information in a policy on the IEM.
- You can hard code the call manager information in the sipphone widget.

### Using a Policy on the IEM

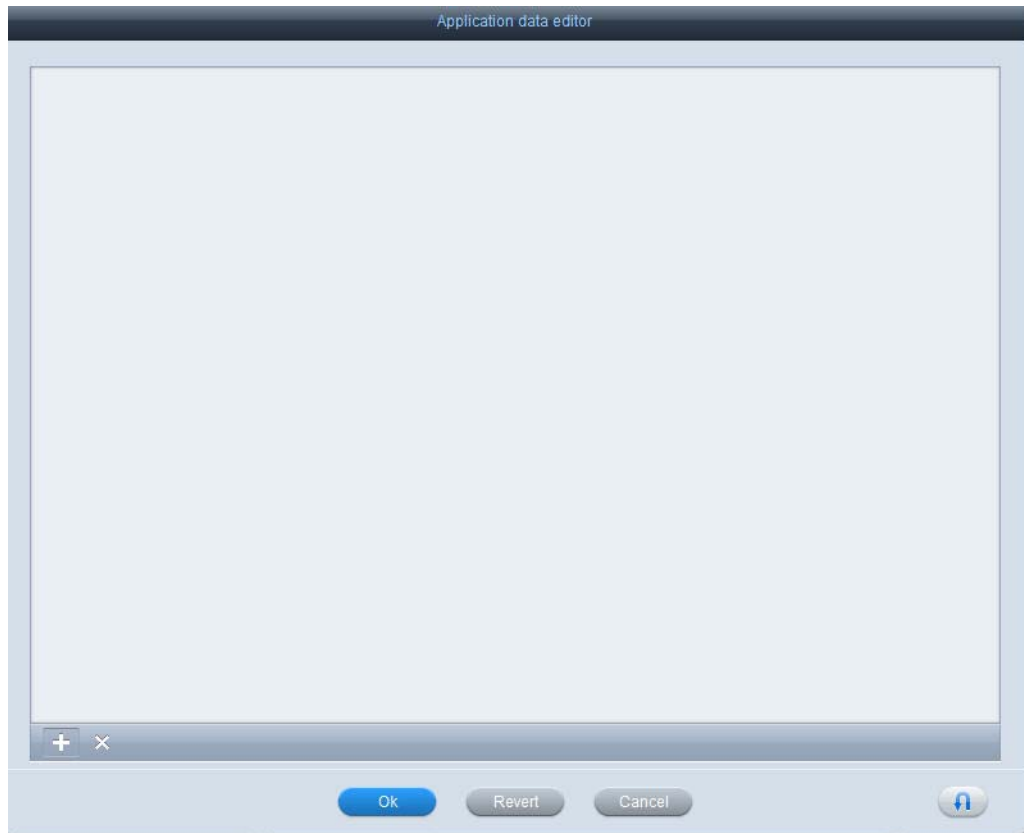
The following steps explain how to enter the call manager information into the IEC's policy on the IEM.

- 
- Step 1** Log in to the Cisco IEM which has the SIP policy enabled on it.
- Step 2** Go to the policy that is applied to the Cisco IEC4610 or 4632 device.
- Step 3** Click the Policy tab.
- Step 4** Expand the application property.
- Step 5** In the data property, click the value field.

**Figure F-44** Value Field of the Data Property

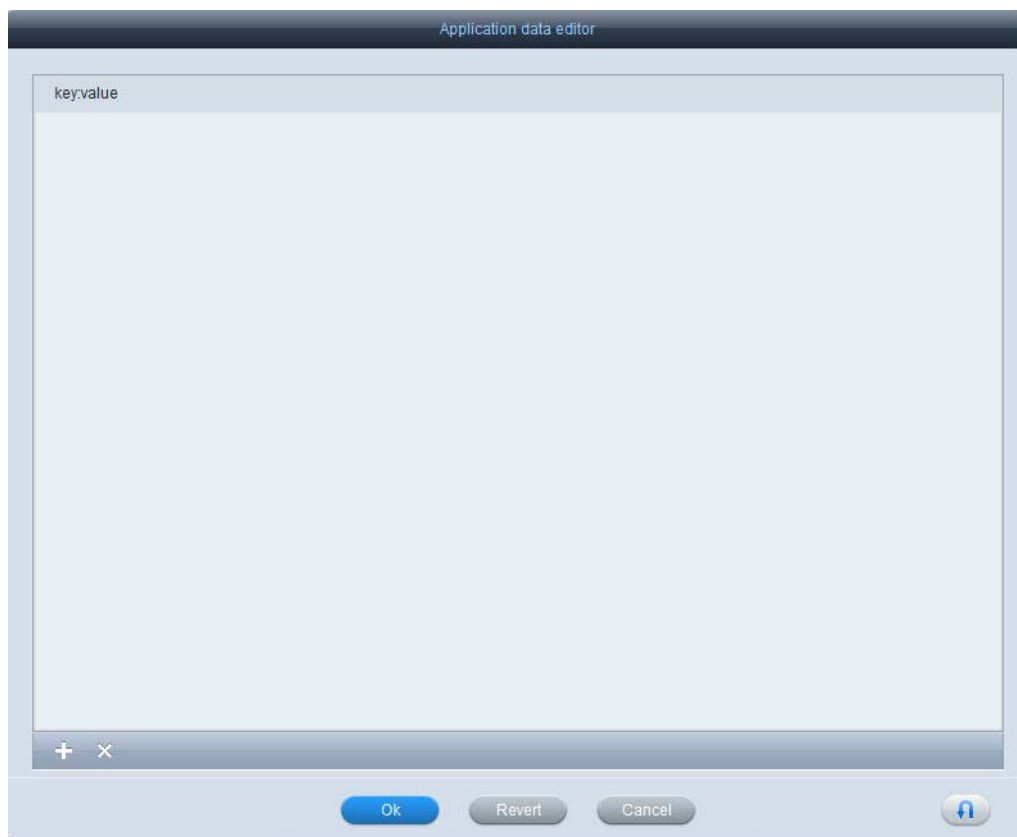


- Step 6** In the Application data editor, click +.

**Figure F-45**     *Application Data Editor*

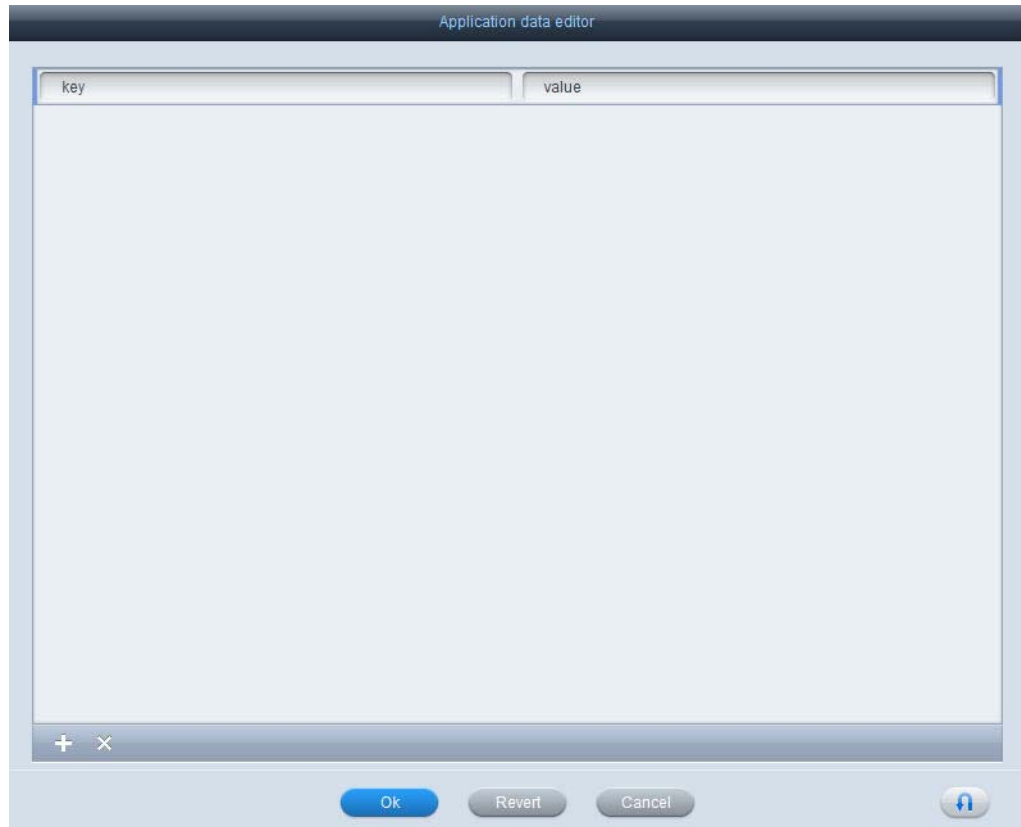
**Step 7**     Click key:value.

**Figure F-46** Key:Value in the Application Data Editor



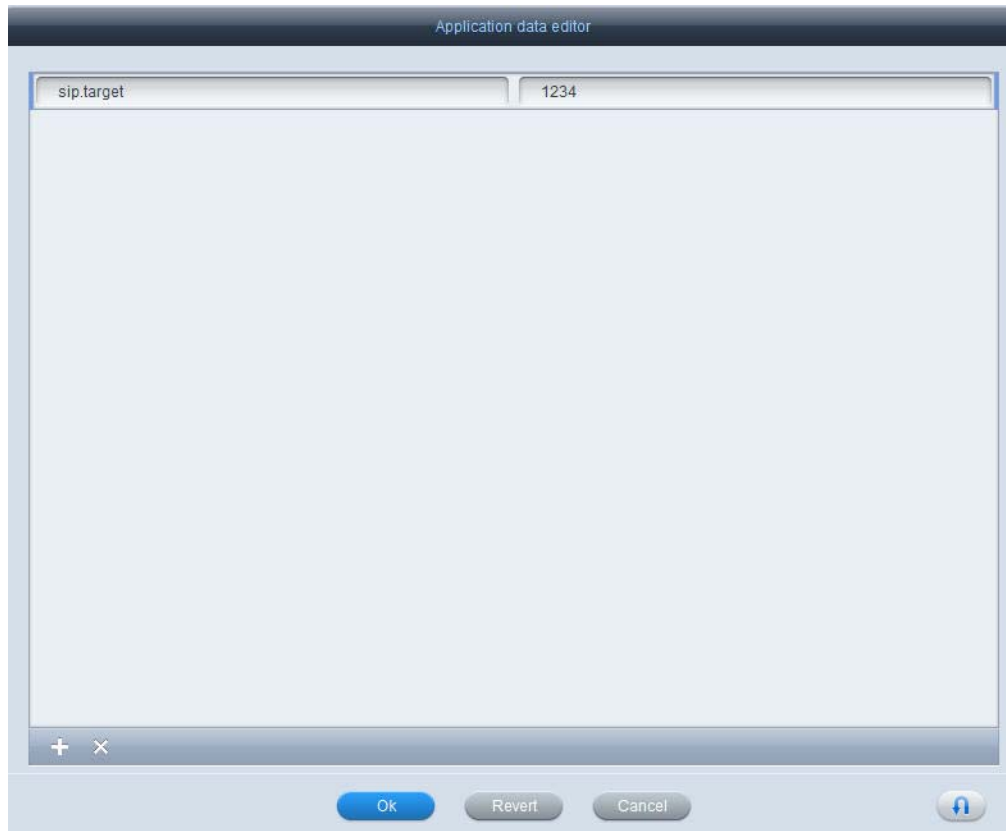
**Step 8** Enter **sip.target** in the key field.

**Figure F-47** Key and Value Fields in the Application Data Editor



**Step 9** Enter the directory number in the value field.

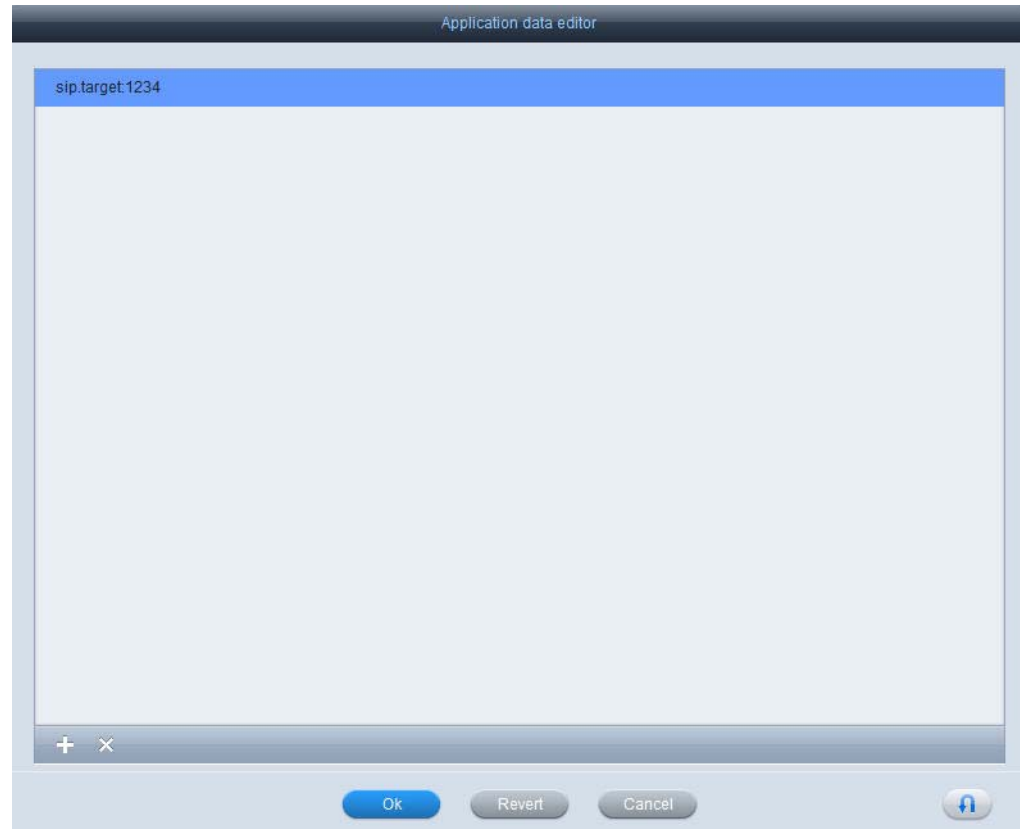
**Figure F-48** Key and Value Fields Filled in the Application Data Editor



**Step 10** Click **Ok**.

If you click on data property's Value field, you will see the data in the form sip.target:[directoryNumber] as shown in the figure below where the directory number is 1234.



**Figure F-49**      *Directory Number in the Application Data Editor*

Next you will add the username, password, domain, and transport protocol for the Cisco Unified Communications Manager (CUCM).

- Step 11** In the Application data editor, click +.
- Step 12** Enter **sip.username** in the key field.
- Step 13** In the value field, enter the username that the IEM will use to log into the CUCM. This is the unique User ID that was entered in the CUCM.



**Note** It is imperative that the value entered in the User ID field is a number. The SIP device will not work if you enter alphabetic characters, punctuation, or spaces.

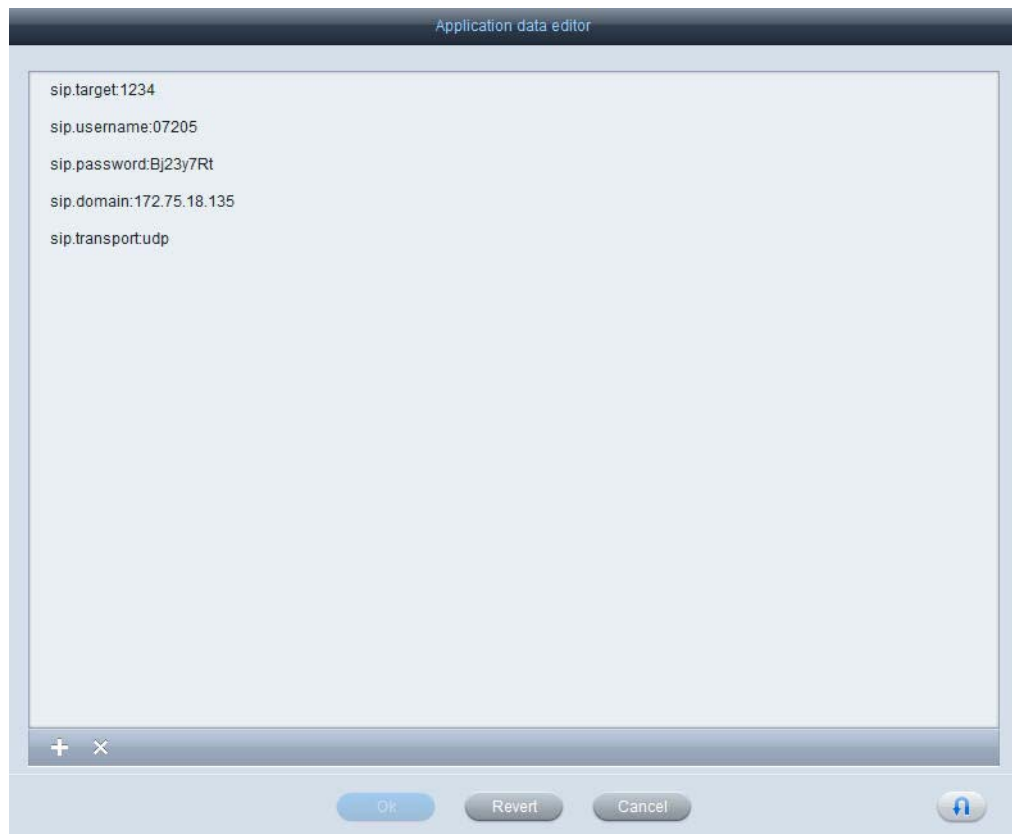
- Step 14** In the Application data editor, click +.
- Step 15** Enter **sip.password** in the key field.
- Step 16** In the value field, enter the password that the IEM will use to log into the CUCM.
- Step 17** In the Application data editor, click +.
- Step 18** Enter **sip.domain** in the key field.
- Step 19** In the value field, enter the IP address of the CUCM.
- Step 20** In the Application data editor, click +.
- Step 21** Enter **sip.transport** in the key field.
- Step 22** Enter **udp** in the value field.

**Note**

It is important to enter all values in lowercase characters. If you enter “UDP” instead of “udp”, the call will not work.

**Step 23** Click **Ok**.

**Figure F-50** Entries in the Application Data Editor



If you click on the data property's Value field, you will see the data.

**Step 24** Click **Apply**.

## Using the SipPhone Widget

You can hard code the call manager information in the sipphone widget. If you want to hard code the SIP client information in this widget, follow these steps.

**Step 1** Open the sipphone widget code using a text editor.

**Step 2** Find the `sipphone.start(username, password, domain, transport)` line in the HTML as shown below.

```
....  
{
```

```

sipphone = document.getElementById("sipphone");

// Now Call Start Routine with the SIP Credentials
// that we got from the applicationData
sipphone.start(username, password, domain, transport);

sipphone.placingCall.connect(onPlacingCall);
sipphone.incomingCall.connect(onIncomingCall);
sipphone.ready.connect(onReady);
sipphone.registered.connect(onRegistered);
sipphone.established.connect(onEstablished);
sipphone.ring.connect(onRing);
sipphone.disconnected.connect(onDisconnected);
sipphone.error.connect(onError);
}
....

```

- Step 3** Replace “username” with the call manager ID, which is a number.
  - Step 4** Replace “password” with call manager’s password.
  - Step 5** Replace “domain” with the IP address for the call manager.
  - Step 6** Replace “transport” with “udp”.
  - Step 7** Save your changes.
- 

## SIP DTMF

Dual-Tone Multifrequency (DTMF) for SIP is a feature that is available starting with version 2.1.1. The purpose of DTMF setup for SIP is to provide the audio prompts heard over the phone such as “Press 1 to reach \_\_\_\_.”

You will need the following to set up DTMF for SIP calls:

- Latest SipPhone widget with the sendDtmf line of code.  

```
void sendDtmf(in string dtmfkey);
```
- Cisco Unified Contact Center Express (UCCX) 9.x: UCCX provides DTMF capability.
- CUCM 9.x: Although CUCM does not have the DTMF feature, when configuring the IEC as a SIP device in the CUCM, the following options must be configured in order for DTMF to work correctly:
  1. Follow the steps in the following link to enable the Media Termination Point system wide for the CUCM: [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/admin/3\\_0\\_9/p4mtp.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/3_0_9/p4mtp.html)
  2. The IEC should be created as a **Third-party SIP Device (Advanced)**.

**Figure F-51** *Third-party SIP Device (Advanced) Phone Type*

**Add a New Phone**

Next

**Status**

Status: Ready

**Select the type of phone you would like to create**

Phone Type\* Third-party SIP Device (Advanced) ▼

Next

3. The **Media Termination Point Required** checkbox should be unchecked.
4. The **Unattended Port** checkbox should be unchecked.
5. The **Require DTMF Reception** checkbox should be unchecked.
6. The **Allow Presentation Sharing using BFCP** checkbox should be unchecked.
7. The **Allow iX Applicable Media** checkbox should be unchecked.

**Figure F-52** *CUCM Checkboxes*

Digest User

☐ Media Termination Point Required

☐ Unattended Port

☐ Require DTMF Reception

☐ Allow Presentation Sharing using BFCP

## Sample usage of sendDtmf() API

This section provides an example on how to use the sendDtmf() API.

The following is the Javascript Function to send the DTMF keys:

```
function sendDtmf(key){
  var k = String(key);
  var validValues = "0123456789*#";
  if(validValues.indexOf(k)>=0){
    writeLog("sendDtmf('"+key+"' )");
    sipphone.sendDtmf(k);
    writeLog("ok");
  } else {
    writeLog("Invalid DTMF argument.")
  }
}
```

The HTML code to bind the keys to the function is:

```
<tr>
<td><button onClick="sendDtmf('1')" class="siphone_key">1</button></td>
<td><button onClick="sendDtmf('2')" class="siphone_key">2</button></td>
<td><button onClick="sendDtmf('3')" class="siphone_key">3</button></td>
<!-- More such lines for each of the DTMF keys -->
</tr>
```

The figure below is a screenshot of the application using DTMF key.

**Figure F-53**      *Application Using the DTMF Key*







## APPENDIX **G**

# Stream Live Video

---

Revised: January 29, 2014, OL-26457-05

## Appendix Overview

To stream live video from the IEC to other endpoints, you will need a video encoder dongle and an input source such as a camera, camcorder, or IEC. This appendix describes a set up using the dongle and a document camera that can be used to stream a document, a training session, a meeting, or a demo.

Topics in this appendix include:

- [System Dimensions Video Encoder Dongle, page G-1](#)
- [Vaddio HD Document Camera, page G-2](#)
- [Stream Live Video, page G-3](#)
  - [Connect Hardware, page G-3](#)
  - [global.videoEncoder Object, page G-6](#)

## System Dimensions Video Encoder Dongle

The System Dimensions AVS 2610 is a video encoder dongle that is HDMI compatible. When connected to the IEC and a camera, live video is captured by a HD video camera and then streamed by the dongle to other IECs or remote computers.

The video stream is sent as part of the MPEG2 Transport Protocol (MPEG-TS). The stream can be sent as either unicast or multicast.

- **Unicast:** The dongle can be used for a point-to-point video stream, for example, when a customer wants to share their document with a virtual agent at a remote site. The stream is sent from an IEC to a single endpoint such as another IEC or a remote computer.
- **Multicast:** The dongle can be used to allow multiple endpoints to view the same video stream such as for a meeting or a training session. To accomplish this, the stream is sent to a multicast address, which is a virtual address, and then anyone within the multicast group can access the stream at the multicast address.

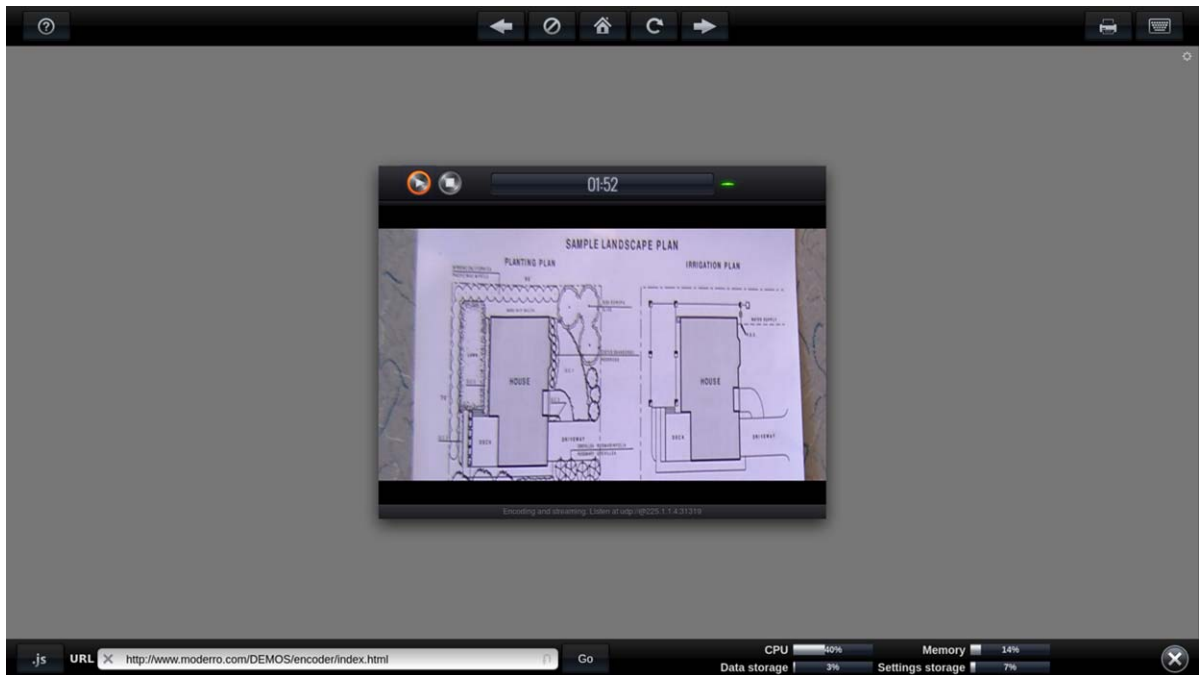


### Note

A media server is not necessary for streaming to a multicast address if your network is multicast-enabled. If you cannot do multicasting on your network, then you need a streaming media server.

If the destination of the stream is another IEC, the native video player of the IEC will receive the video stream and display it. If the destination is a computer, you will need a player on that computer that is capable of receiving H.264 video codec and MPEG-TS as well as decoding UDP multicast streams; a VLC player will meet these requirements. If a robust streaming solution is needed, a media server that receives both UDP multicast and TCP unicast streams could be placed on the network between the streaming endpoint and the receiving endpoints.

**Figure G-1** IEC Receiving the Video Stream of a Document from Another IEC



## Vaddio HD Document Camera

The Vaddio CeilingVIEW™ HD-18 DocCAM is a high-definition ceiling-mounted document camera connected to the IEC via a video encoder dongle. The Vaddio camera can capture documents that the customer is holding or places on the desk or table below the camera. This camera can also be used to capture live events such as demos or lectures.

The Vaddio document camera has the following features:

- Supports 16:9 resolutions at 1080p, 1080i and 720p and 4:3 resolutions at 480i and 576i
- Component HD (1080p, 1080i or 720p) or RGBHV outputs
- 18X optical zoom lens
- 1.3 megapixel 1/3-type CCD image sensor for precise HD video image acquisition even in low light applications
- 16-position rotary switch to select HD camera resolutions



**Table G-1 Vaddio HD Camera Resolutions**

Rotary Switch Setting	HD Camera Resolution
0	720p/59.94
1	1080i/59.94
2	1080p/59.94
3	1080p/60
4	720p/50
5	1080i/50
6	1080p/50
7	1080p/30
8	1080p/25
9	1024 x 768/60 RGBHV
A	
B	
C	
D	
E	1280 x 800/60 RGBHV
F	1680 x 1050/60 RGBHV

The Document Camera is composed of two units: the camera itself mounted to the ceiling and the Vaddio Quick-Connect HD-18 DVI/HDMI, which delivers simultaneous analog component video (YPbPr) and digital video (DVI-D or HDMI) outputs on separate connectors, up to 100 feet over a single Cat. 5 cable.

There is no API for the Vaddio document camera. Instead a hex string is sent via RS232 to the camera using the serialPorts API. For example:

Camera ON: \x81\x01\x04\x00\x02\xff

Camera OFF: \x81\x01\x04\x00\x03\xff

## Stream Live Video

To stream live video, the following components are required:

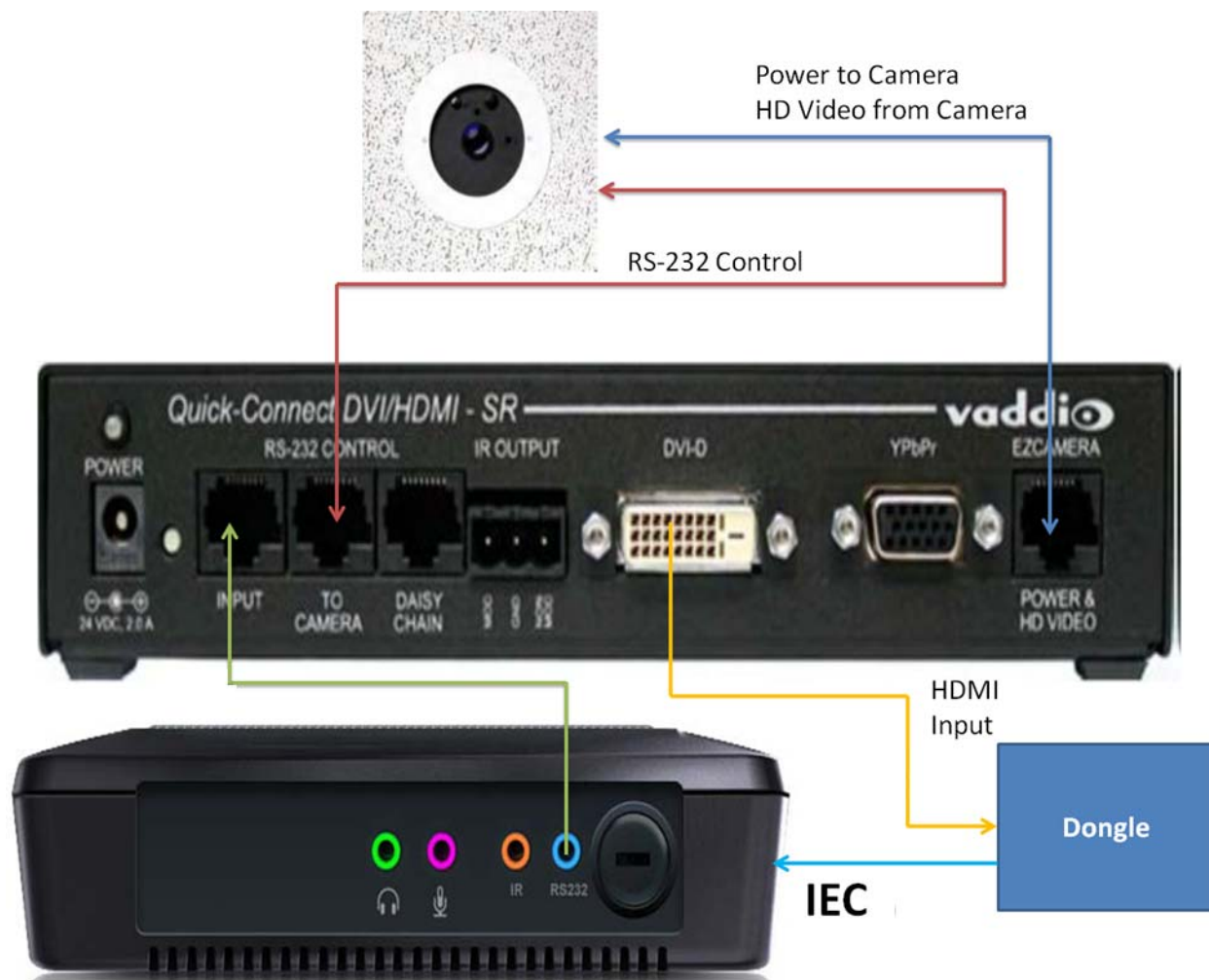
1. Vaddio CeilingVIEW HD-18 DocCAM
2. Vaddio Quick-Connect HD-18 DVI/HDMI
3. System Dimensions AVS 2610 encoder dongle
4. USB extension cable

## Connect Hardware

Follow these steps to connect the camera, Quick-Connect, and encoder dongle to the IEC:

- Step 1** Mount the Vaddio camera to the ceiling above the kiosk or desk/table in a position that allows it to capture a document below it. Follow the mounting instructions found in Vaddio's manual for the camera: <http://www.vaddio.com/images/document-library/342-0195-RevB-CeilingVIEW-HD-18-DocCAM-Manual.pdf>
- Step 2** Use the EZCamera power and HD Video Port cord to connect the Quick-Connect to the camera.
- Step 3** Use a RS-232 Control cord to connect the To Camera port on the Quick-Connect and the camera.
- Step 4** Connect another RS-232 cord into the Input port on the Quick-Connect and plug the other end into the RS232 port on the IEC.
- Step 5** Connect the HDMI input of the encoder dongle to the DVI-D output of the Quick-Connect.
- Step 6** Insert one end of the USB extension cable to the encoder dongle and the other end into the USB port on the IEC.
- Step 7** Reboot the IEC so that it recognizes the video encoder dongle.

**Figure G-2 Vaddio Camera Setup**



**Table G-2 Cable Connection Details for the Above Diagram**

Number	Connection	Purpose	Cable
1	EZCamera Power & HD Video Port	Supplies power to camera and returns HD video from the camera	CAT-5e Ethernet cable
2	SR Interface to Camera	RS-232 control to and from camera and IR signals returned from the camera	CAT-5e Ethernet cable
3	RS-232 Control Input (A photo of this connection is shown in the figure below)	Input to SR interface from IEC RS-232 port	Shown in figure below: a) 9 pin male to 2.5mm jack adapter b) 9 pin female to Ethernet port adapter (comes with Vaddio camera - no need to purchase) c) CAT-5e Ethernet cable
4	DVI-D Output	From SR interface DVI-D to HDMI port of dongle	DVI to HDMI cable: HDMI (v 1.3 with deep color) and DVI v 1.0 compliant
5	HDMI Output	From dongle USB to USB port of IEC	Male to female USB cable

**Figure G-3** Cables for RS-232 Control Input



## global.videoEncoder Object

The `global.videoEncoder` object allows the web application to take a video feed from a HDMI Source and encode it to MPEG-TS and stream it out to an endpoint either via UDP or via TCP. This object can be coupled with the video player and can serve as a local view of the encoded frame that is being sent out on the wire.

**Note**

While using TCP as the connection type, ensure that the TCP endpoint on the host to which you are interested to stream to is listening on the port of interest.

**Tip**

While using the camera, make sure the input resolution that you select is supported by the camera. It is recommended that you use either a 720p or a 1080i. A lower resolution camera may not give the desired output.

```
interface videoEncoder
{
    readonly attribute bool isAvailable; // Checks if Encoder is Available
    readonly attribute int status;
    readonly attribute int errorCode;
    readonly attribute string errorMessage;

    readonly attribute int videoInputCount;
    readonly attribute stringlist videoInputDescription;
    readonly attribute string snapshot;

    attribute string targetHost; // Target Host where MPEG2-TS has to be sent
    attribute int targetPort; // Target Port on Target Host to Receive it
    attribute int protocol; // Udp=0, Tcp=1

    attribute int videoMode; // SD=0, HD=1, CUSTOM=2
    attribute int videoSource; // Must be in [0, videoInputCount] range. 0 is for
    HDMI, 1-videoInputCount is for webcams

    attribute int h264Profile;
    attribute int inputResolution;
    attribute bool isProgressive;
    attribute int streamType;

    attribute int inputFrameRate; // 15, 24, 30, 60
    attribute int outputFrameRate; // 15, 24, 30, 60
    attribute int averageOutputBitRate;
    attribute int minimumOutputBitRate;
    attribute int maximumOutputBitRate;

    attribute int outputResolution;

    attribute int audioBitRate;

    signals:
        notready();
        ready();
        started();
        stopped();
        error(in int code, in string message);

    slots:
        start();
        stop();
        takeSnapShot();
}
```

## global.videoEncoder object Variables

**Table G-3** *global.videoEncoder Object Variables*

Variable	Description
isAvailable	Use this routine to check if the box has videoEncoder Module in it. A 'true' value indicates presence of the module.
status	Represents status of video encoder. The status are listed in the section below as enumeration for your reference.
errorCode	This attribute will be set when an error occurs. Use this attribute for error handling in your application.
errorMessage	This routine returns the error string corresponding to the errorCode that was set. Use this function to display an error message to the user in your application.
videoInputCount	Returns the available video sources including the HDMI input from the USB dongle and all available webcams.
videoInputDescription	Returns the description of all video input devices present in the box.
targetHost	Returns the target host to which the encoded stream is being sent.
targetPort	Returns the port number on which the encoded stream is being sent.
protocol	Returns integer value for the Transport Protocol: '0' for UDP or '1' for TCP.
videoMode	Returns video mode on which the video encoder is operating. Values are: '0' - SD, '1' - HD, and '2' for Custom.
videoSource	Returns the video source being selected for encoding either as '0' for HDMI or '1' for videoInputCount for webcam.
h264Profile	Returns the encoding H.264 profile being used by the encoder: '0' for Baseline, '1' for Main, and '2' for Extended Profile.
inputResolution	Returns the input resolution that is being used for the source. Possible values are '0' for 1920x1080 resolution, '1' for 1280x720, and '2' for 1024x600.
isProgressive	Returns 'true' if the scan format is set to Progressive.

<code>streamType</code>	Returns the input stream type that is configured on the encoder. Possible values are '0' = Program Stream, '1' = Transport Stream, '2' = MPEG4 Stream (default), '3' = Elementary Stream, and '4' = Raw Stream.
<code>inputFrameRate</code>	Returns the Video-In Frame Rate as integer value in fps. Possible values are '0' for 15fps, '1' for 24fps, '2' for 30fps, and '3' for 60 fps.
<code>outputFrameRate</code>	Returns the Video-Out Frame Rate as integer value in fps. Possible values are '0' for 15fps, '1' for 24fps, '2' for 30fps, and '3' for 60 fps.
<code>averageOutputBitRate</code>	Returns the Video-Out Average Bit Rate in kbps
<code>minimumOutputBitRate</code>	Returns the Video-Out Minimum Bit Rate in kbps
<code>maximumOutputBitRate</code>	Returns the Video-Out Maximum Bit Rate in kbps
<code>outputResolution</code>	Returns the Video-Out Resolution from the encoding stream. Possible values are '0' for 1920x1080, '1' for 1280x720, '2' for 1200x672, '3' for 1168x656, '4' for 1024x576, and '5' for 768x432.
<code>audioBitRate</code>	Returns the Audio-Out Bit Rate being sent from the encoder in bps.
<code>setTargetHost(in string targetHost)</code>	Allows you to set the Target Host (IP Address either as Unicast or Multicast ipv4 Address).
<code>setTargetPort(in string targetPort)</code>	Allows you to set the Target Host's (Layer4) port Number (TCP or UDP port number).
<code>setProtocol(in int transportProtocol)</code>	Allows the Transport (Layer4) Protocol to be used when sending the encoded stream. Choices are '0' for UDP or '1' for TCP.
<code>setVideoMode(in int videoMode)</code>	Allows you to set video Encode mode either as SD (Standard Definition) or HD (High Definition). If you would like to still fine tune the encoding properties, you can select the custom option. Choices are '0' for SD, '1' for HD, and '2' for Custom.
<code>setVideoSource(in int videoSource)</code>	Allows you to set the video source for the encoder. Choices are '0' for HDMI Input from USB Dongle, and '1' for all available (v4l compliant) webcams.
<code>setH264Profile(in int h264Profile)</code>	Allows you to set the H.264 profile to be used for encoding. Choices are '0' for baseline profile, '1' for main profile, and '2' (default) for extended profile.
<code>setInputResolution(in int inputResolution)</code>	Allows you to set the input resolution for the video source. Choices are '0' for 1920x1080, '1' for 1280x720, and '2' for 1024x600.

<code>setProgressive(in int flag)</code>	Allows you to set the input scan format to Progressive. Call this API with parameter of '1' to set to Progressive. Choices are '0' or '1'.
<code>setStreamType(in int streamType)</code>	Allows you to set the stream type for the Video-In stream. Choices are '0' for PS, '1' for TS (default), '2' for Mp4, '3' for ES, and '4' for Raw.
<code>setInputFrameRate(in int frameRate)</code>	Allows you to set the Incoming (Video-In) Frame rate in fps. Choices are '0' for 15fps, '1' for 24fps, '2' for 30fps, and '3' for 60fps.
<code>setOutputFrameRate(in int frameRate)</code>	Allows you to set the Output (Video-Out) Frame rate in fps. Choices are '0' for 15fps, '1' for 24fps, '2' for 30fps, and '3' for 60fps.
<code>setAverageOutputFrameRate(in int avgRate)</code>	Allows you to set the Average Output Rate (Video-Out) in kbps.
<code>setMinimumOutputBitRate(in int minRate)</code>	Allows you to set the Minimum Output Rate (Video-Out) in kbps.
<code>setMaximumOutputBitRate(in int maxRate)</code>	Allows you to set the Maximum Output Rate (Video-Out) in kbps.
<code>setOutputResolution(in int outputResolution)</code>	Allows you to set the Output Resolution for Video-Out. Choices are '0' for 1920x1280, '1' for 1280x720, '2' for 1200x672, '3' for 1168x656, '4' for 1024x576, and '5' for 768x432.
<code>setAudioBitRate(in int bitRate)</code>	Allows you to set the Audio-In bit rate in kbps.

## global.videoEncoder object Enumeration

```

{
    enum ErrorCodes
    {
        videoEncoderNotPresent = -1,
        UnabletoStopStreaming = -2,
        UnabletoStartStartStreaming = -3,
        RemoteSideNotListening = -4,
        MemoryExuastionError = -5,
        NoHdmiVideoSignal = -6,
        BothUsbAndPcieTogetherNotSupported = -7,
        HdmiVideoFormatNotUnderstood = -8,
    };
    enum Protocol
    {
        ProtocolUdp = 0,
        ProtocolTcp = 1,
    };
    enum VideoMode
    {
        VideoModeSD = 0,
        VideoModeHD = 1,
        VideoModeCustom = 2,
    };
}

```



```
enum VideoSource
{
    HdmiVideo = 0,
    WebcamVideo = 1,
};
enum H264Profile
{
    H264ProfileBaseLine = 0,
    H264ProfileMain = 1,
    H264ProfileExtended = 2,
};
enum InputResolution
{
    InputResolution1920x1080 = 0,
    InputResolution1280x720 = 1,
    InputResolution1024x600 = 2,
};
enum OutputResolution
{
    OutputResolution1920x1080 = 0,
    OutputResolution1280x720 = 1,
    OutputResolution1200x672 = 2,
    OutputResolution1168x656 = 3,
    OutputResolution1024x576 = 4,
    OutputResolution768x432 = 5,
};
enum StreamType
{
    StreamPgoram = 0,
    StreamTransport = 1,
    StreamMp4 = 2,
    StreamElementary = 3,
    StreamRaw = 4,
};
enum InputFrameRate
{
    Input15fps = 0,
    Input24fps = 1,
    Input30fps = 2,
    Input60fps = 3,
};
enum OutputFrameRate
{
    Output15fps = 0,
    Output24fps = 1,
    Output30fps = 2,
    Output60fps = 3,
};
};
}
```





# APPENDIX H





## Content Guidelines




Revised: January 29, 2014, OL-26457-05

## Content Guidelines

The following table lists the content guidelines for IEC Series.

**Table H-1**      **Content Guidelines**

Video formats	<p>Multiple video formats are supported on the native player including MPEG-1, MPEG-2, MPEG-4, and H.264.</p> <p>Multiple containers/muxers are supported on the native player including AVI, MOV, MP4, MPEG2, and MPEG-2/TS (extensions: .wmv, .avi, .mov, .mp4, .mpg, .ts).</p> <p>Formats not recommended: On2 VP 6 (used by old FLV)</p> <div> <b>Note</b> Native video is strongly preferred over Flash video.</div> <div> <b>Note</b> The IEC 4600 series supports WebM (VP8/Vorbis) and Ogg (Theora/Vorbis) for HTML5 video.</div> <div> <b>Note</b> Use of the native player strongly preferred over HTML5 video.</div> <div> <b>Note</b> The native player's video compatibility can be validated by using VLC 2.0.8.</div>
Audio formats	Multiple audio formats are supported on the native player including mp2, mp3, aac, mp4a, wma1, wma2, flac, and mpga.
HTML	HTML4 / CSS3 (early support for HTML5)
Flash	Up to Flash 11

Video Performance Limitations	<p>When using a native player, the IEC 4610 can support H.264 video up to 720p @ 6Mbps.</p> <p> <b>Note</b> The amount of CPU power required to decode a video clip depends on multiple factors such as codec, bitrate, and resolution of the video source.</p> <p>Different video codecs have different compression algorithms. H.264 offers much better compression efficiency than MPEG-2 or MPEG-4 but uses much more a complex algorithm and requires more CPU power to decode. For example, to achieve the same level of quality, it may require 5 Mbps using MPEG2 but less than 2 Mbps using H.264.</p> <p>The IEC 4610 can decode 1080p 14Mbps MPEG2 video with less than 90% of CPU usage, but cannot decode 720p 8Mbps H.264 video without obvious frame drops.</p> <p> <b>Note</b> When the video source is interlaced (1080i, 480i, etc.), you may see interlacing artifacts due to the lack of de-interlacing capability on the native player.</p> <p> <b>Note</b> The size of the native player object does not affect the CPU usage. If the video source is the same, the CPU usage is the same regardless of the player's height and width. That is, if the video source is 1280x720, the CPU usage will not change by setting the native player's size to 320x180 or 1920x1080.</p>
Screen Resolutions	<p>Up to 1920x1080 (1080p); IEC4600 Series defaults to monitor's native resolution</p> <p>To ensure the content scales well, build for the lowest resolution expected, then use stretchers to make sure it can stretch to the highest resolution expected.</p>
Screen Rotations	<p>Both horizontal (landscape) and vertical (portrait) modes are supported with 90, 180, 270 degree turns. The content should be laid out naturally.</p>
General Content Guidelines	<p>HTML/JavaScript is a preferred mechanism for building kiosk applications.</p> <p>Use of Flash should be limited to small size and non-video rendering functionality.</p> <p>Ticker tapes should be using CSS3 for scrolling.</p> <p>“Screensaver” video playback should be postponed when the kiosk is being interacted with to avoid audio conflicts and preserve responsiveness.</p> <p>Regularly-playing videos should be cached locally.</p>



# HD Video Conferencing Between Two IECs Using the Video Encoder Card

---

Revised: January 29, 2014, OL-26457-05

## Appendix Overview

An embedded video encoder card is built into IEC devices starting with release 2.1. Those who have IEC software release 2.1.1 or later can use the video encoder cards to make high-definition (HD) video calls between two IECs.

Topics in this appendix include:

- [Video Encoder Card \(VEC\), page I-1](#)
- [Set Up Video Calls Between Two IECs with VECs, page I-2](#)
  - [Connect the Hardware, page I-2](#)
  - [Configure Call Information, page I-3](#)

## Video Encoder Card (VEC)

The VEC is a Peripheral Component Interconnect Express (PCIe)-based encoder that allows IEC 4600 Series devices to record and transcode video using the H.264 video codec. As a result, HD video calls can be made between two IECs with VECs as an alternative to making a SIP call between an IEC and a Cisco Unified IP Phone 9951.



### Note

SIP calls between an IEC and an IP phone are not high-definition video calls. The only supported HD video calls are between IECs with embedded VECs.

HD video calling relies on the presence of internal VEC encoders in both end points. There are several ways to verify that an IEC has an internal VEC:

1. Go to the Status tab of the device in the IEM. Expand Connected USB and PCIe devices. Find Video Encoder. If the VEC is present, the value will be “Available”.

**Figure I-1 Video Encoder in Status Tab**

Name	Value
▶ Hardware	
▶ Network	
▶ Displays	
▶ Locale	
▼ Connected USB and PCIe devices	
Bus 004 Device 002	ID 0d3d:0040 Tangtop Technology Co., Ltd
Bus 004 Device 003	ID 04e7:0020 Elo TouchSystems Touchscreen Interface (2700)
Bus 006 Device 002	ID 13d3:3314 IMC Networks
Video Encoder	Available

2. The IEC splash screen indicates if a VEC is built-in.
3. IECs with VECs have a sticker on the bottom of the device indicating that an encoder card is built-in.

## Set Up Video Calls Between Two IECs with VECs

To set up calls between two IECs with VECs, you will need the following:

- IEC4610 or IEC4632 with embedded VECs (found in Release 2.1 and later)



**Note** Calls between two IECs cannot be accomplished with older versions of the IEC hardware such as 2.0 or 1.0.3.

- IEC Firmware 2.1.1
- High-definition video cameras such as the Cisco PrecisionHD or the Logitech C110 with USB cables
- Microphones
- CUCM 9.1.1.10000-5

## Connect the Hardware

Follow the steps below to connect the hardware.

- Step 1** Make sure that both IECs are installed, registered, configured, and up and running. Confirm that the startup URL is displaying.
- Step 2** For each IEC, connect a HD video camera using a USB cable to a USB port on the IEC.
- Step 3** For each IEC, connect a microphone to either a USB port or the MIC-in port (shown on the figure below as the pink port with the microphone icon).

**Figure I-2**      **MIC-in Port on the IEC**



## Configure Call Information

To configure HD video conferencing, you will need CUCM version 9.1.1.10000-5 and the SipPhone widget.



**Note**

This set up is not compatible with Cisco Contact Center Express.

To configure call information:

- Step 1**      Configure both IECs on the CUCM. See the “Cisco IEC Set Up on the CUCM” section of Appendix F for instructions.
- Step 2**      Configure the call information either using a policy or the SipPhone widget. See either the “Using a Policy on the IEM” or the “Using the SipPhone Widget” section of Appendix F.

