Cisco Interactive Experience Client
User Guide
Release 2.3.3

February 16, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
The 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, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDCA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networks, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (1110R)

Cisco Interactive Experience Client User Guide
© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1  Introduction

CHAPTER 2  Setting Up the IEC

CHAPTER 3  Configuring Settings

CHAPTER 4  Off-Line Caching

CHAPTER 5  Upgrading the IEC

CHAPTER 6  Debugging Console

CHAPTER 7  Locally Configuring the IEC

APPENDIX A  Compatible Peripherals

APPENDIX B  Printers

APPENDIX C  Optical Scanners

APPENDIX D  Magnetic Card Readers and Barcode Scanners

APPENDIX E  Infrared Remote Controls

APPENDIX F  Video Conferencing Using the Session Initiation Protocol Client

APPENDIX G  Stream Live Video

APPENDIX H  Content Guidelines
Introduction

Revised: February 16, 2016

Chapter Overview

The Cisco Interactive Experience Client 4650 is a state-less computer device designed to power various-purpose kiosks, Internet terminals, and specialized workstations. The Cisco Interactive Experience Client 4650 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 4650.

The topics in this chapter are the following:

- “What’s New in This Release”
- “About This User Guide”
  - “Terminology”
  - “Audience”
  - “Scope”
- “Cisco Interactive Experience Platform”
  - “Cisco Interactive Experience Manager”
  - “Cisco Interactive Experience Client 4650”
  - “Principles of Operation”
- “Kiosk Navigation”
- “Package Contents”
- “What You Will Need”
What’s New in This Release

This release includes the following new features and enhancements:

- A new model of the IEC HW is now available. The next generation 4650 is replacing the 4632, which is being retired along with the 4610. The 4650 provides significantly higher performance than the 4632 for video, 3-D graphics, and animation. It has an i3 processor, native 4K resolution support, and a video and 3-D graphics hardware accelerator.

About This User Guide

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 - The client at the kiosk such as the Cisco Interactive Experience Client 4650.

- 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 4650 hardware and software.

Scope

This user guide explains how to use the Cisco Interactive Experience Client 4650.

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 Experience Platform

Cisco Interactive Experience Platform 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 Experience Platform 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 4650 hardware and software.

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 4650 devices. The 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 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 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 4650

The Cisco Interactive Experience Client (IEC) 4650 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 4650 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. It is highly recommended that all the Cisco IEC 4650 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 4650 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 4650 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 4650 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

Cisco IEC 4650 does 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. **Devices need to exist on the IEM in order to be managed by it.** 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 and IEM software 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 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 devices 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.

### Package Contents

The package should contain the following components:

- Cisco IEC 4650
- Power adapter
- Mounting plate
- Four mounting screws

What You Will Need

To optimize the video quality, the IEC 4650 should be connected to a 1080p or 4K LED or LCD video display using either HDMI (preferred) or Mini DisplayPort.

To install and configure the Cisco IEC 4650, you will need the following:

- Video monitor (non-touch screen or touch screen)
- HDMI or Mini DisplayPort 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 Overview

This chapter explains how to do set up the equipment and configure the Cisco IEC 4650 so that it displays the startup URL.

Topics in this chapter include:

- “Connecting the Hardware”
  - “IEC Dimensions”
  - “IEC Specifications”
  - “Environmental Tolerance Ranges”
  - “Warnings”
  - “VCCI-B Warning - Japan”
  - “EMC Warning - South Korea”
  - “RF Warning - South Korea”
  - “Federal Communication Commission Interference Statement - USA”
  - “RF Exposure”
  - “Choosing a Location”
  - “Mounting the Hardware”
  - “Connecting and Powering Up”
- “Registering the IEC”
- “Configuring the System”
- “Connecting to the Network”
  - “Configuring an Ethernet (Wired) Connection”
  - “Configuring a Wireless Connection”
- “Connecting to the Cisco IEM”
  - “Applying a Policy”
- “Calibrating the Touchscreen”
Connecting the Hardware

The Cisco IEC 4650 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 Cisco IEC 4650.

<table>
<thead>
<tr>
<th>US Customary Unit</th>
<th>Modern Metric Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width</td>
<td>Depth</td>
</tr>
<tr>
<td>7.3 inches</td>
<td>7.4 inches</td>
</tr>
</tbody>
</table>

IEC Specifications

The table below contains the Cisco IEC 4650 specifications.

<table>
<thead>
<tr>
<th>Features</th>
<th>IEC 4650</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCBA Form Factor</td>
<td></td>
</tr>
<tr>
<td>Board size</td>
<td>6.0 in. x 6.0 in. (150 mm x 150 mm)</td>
</tr>
<tr>
<td>Processor</td>
<td>Intel Broadwell Processor</td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>DDR3-1333/1600 memory (SO-DIMM Slot X2)</td>
</tr>
<tr>
<td>System memory size</td>
<td>4 GB</td>
</tr>
<tr>
<td>Storage</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>M.2 Key M</td>
</tr>
<tr>
<td>Storage Memory Size</td>
<td>32 GB</td>
</tr>
<tr>
<td>BIOS Flash Memory</td>
<td></td>
</tr>
<tr>
<td>Memory Size</td>
<td>16 MByte</td>
</tr>
<tr>
<td>Ethernet</td>
<td></td>
</tr>
<tr>
<td>Count</td>
<td>1</td>
</tr>
<tr>
<td>Speeds</td>
<td>10/100/1000 Mbps</td>
</tr>
</tbody>
</table>
## Connecting the Hardware

### Connectors
- 1 Port RJ45 with transformer

### Video
- Onboard: Intel HD5500 HDMI/Mini DisplayPort
- Connectors: 1 HDMI port, 1 Mini DisplayPort

### USB
- Type: USB 3.0 controller
- Connectors: 2 Right USB A type, 2 Back USB A type

### WiFi+Bluetooth
- Count: 1
- Speed: 802.11ac, Bluetooth 4.0

### Front I/O
- LED: 1 Green LED, 1 Orange LED
- IR receiver: 1 Built-in IR receiver

### Back I/O
- DC jack: 1 12V DC in connector
- Video: 1 Mini DisplayPort, 1 HDMI port
- Ethernet: 1 RJ45 connector with dual LEDs
- USB: 1 USB two-stack connector

### Left I/O
- COM: 1 x 3.5 mm phone jack type
- IR extension: 1 1-IR 3.5 mm phone jack
- Audio: 1 Audio port (MIC-in), 1 Audio port (line-out)
- USB: 1 USB two-stack connector

### Right I/O
- Buttons: 1 Power On/Off button (with soft/hard power option), 1 Reset button

### Power
- Adapter: Delta DPS-65VB
  - Input: 100V - 240V ~2A 50-60HZ
  - Output: 12V~5.417A
- Power consumption: 12V@60W maximum
- CPU VR: Intel VR12.5/12.6
Environmental Tolerance Ranges

Refer to the table below for the environmental tolerance ranges.

<table>
<thead>
<tr>
<th>Table 2-3</th>
<th>Cisco IEC 4650 Environmental Tolerance Ranges: Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature¹</td>
<td>US Customary Unit</td>
</tr>
<tr>
<td></td>
<td>Minimum</td>
</tr>
<tr>
<td>Operating long-term or short-term</td>
<td>32°F</td>
</tr>
<tr>
<td>Non-operating or storage</td>
<td>-4°F</td>
</tr>
</tbody>
</table>

¹. Ambient.

<table>
<thead>
<tr>
<th>Table 2-4</th>
<th>Cisco IEC 4650 Environmental Tolerance Ranges: Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative Humidity¹</td>
<td>Minimum</td>
</tr>
<tr>
<td>Operating</td>
<td>10 percent (Indoor)</td>
</tr>
<tr>
<td>Non-operating or storage</td>
<td>0 percent (Indoor and Outdoor)</td>
</tr>
</tbody>
</table>

¹. Noncondensing; ambient.

<table>
<thead>
<tr>
<th>Table 2-5</th>
<th>Cisco IEC 4650 Environmental Tolerance Ranges: Altitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>Altitude¹</td>
<td>US Customary Unit</td>
</tr>
<tr>
<td></td>
<td>Minimum</td>
</tr>
<tr>
<td>Operating and non-operating</td>
<td>0 feet</td>
</tr>
</tbody>
</table>

¹. Above sea level.

Warnings

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

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.

Warning
Ultimate disposal of this product should be handled according to all national laws and regulations.
VCCI-B Warning - Japan

This is a Class B product based on the standard of the VCCI Council. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual. VCCI-B

EMC Warning - South Korea

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A급 기기 : 업무용 방송통신기자재</td>
<td>Class A: Industrial/Official</td>
</tr>
<tr>
<td>B급 기기 : 가정용 방송통신기자재</td>
<td>Class B: Home</td>
</tr>
</tbody>
</table>

As this equipment has undergone EMC registration for business purpose (“A” class), the seller and/or the buyer is asked to beware of this point and designed to be used in the area, except for home use.

As this equipment has undergone EMC registration for household purpose (“B” class). this product can be used in any area and designed to be used mainly in a household.

RF Warning - South Korea

A minimum separation distance of 1.5 cm must be maintained between the user’s body and the device, including the antenna during body-worn operation to comply with RF exposure requirement.

Federal Communication Commission Interference Statement - USA

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.
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 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.

Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

**RF Exposure**

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

- 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.
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>
<thead>
<tr>
<th>MPE</th>
<th>Distance</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.xxx mW/cm²</td>
<td>x cm / x inches</td>
<td>x.xx mW/cm²</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MPE</th>
<th>Distance</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.xxx mW/cm²</td>
<td>x cm / x inches</td>
<td>x.xx mW/cm²</td>
</tr>
</tbody>
</table>

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 then recommended.

Additional information on the subject can be found at the following links:
- FDA Website http://www.fda.gov
- World Health Organization Internal Commission on Non-Ionizing Radiation Protection at www.who.int/emf
- Mobile Manufacturers Forum at www.mmfai.org
Choosing a Location

The Cisco IEC 4650 is intended for indoor use only. The Cisco IEC 4650 must be located within eight feet of an electrical outlet for the power adapter to reach the outlet.

Mounting the Hardware

The Cisco IEC 4650 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 4650 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 Cisco IEC 4650 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).

Step 3
Carefully slide the Cisco IEC 4650 onto the tabs. The display and network connections will be facing the floor.

Connecting and Powering Up

The back of the Cisco IEC 4650 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.

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.

Step 1
Connect an USB keyboard to one of the USB ports on the Cisco IEC 4650.

Step 2
Connect an USB cable or wireless USB adapter for a mouse to an USB port on the Cisco IEC 4650.

Step 3
(Optional) Connect an USB cable for a webcam to an USB port on the Cisco IEC 4650.

Step 4
(Optional) Connect other peripherals such as speakers, microphone, magnetic card reader, barcode scanner, printer, etc.
Chapter 2  Setting Up the IEC

Registering the IEC

The Cisco IEC 4650 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.

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 HDMI port or Mini DisplayPort on the Cisco IEC 4650. Then connect the other end of the cable to the video display.

Tip
To optimize the video quality, the Cisco IEC 4650 should be connected to a 1080p or 4K LED or LCD video display using the HDMI or Mini DisplayPort cable.

Step 6
If the display is a touch screen, connect an USB cable to it and an USB interface on the Cisco IEC 4650.
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 4650. 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 4650.
Step 11
Plug the power adapter into an electrical outlet.

The Cisco IEC 4650 will initialize now. When it finishes initializing, the COBRA screen appears.

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 4650 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”.

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.
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. 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.

| **Tip** | You can use either the mouse or arrow keys on a keyboard to navigate the icons within the System Settings window. |

**Step 3** Now you will configure the system to connect the Cisco IEC 4650 to the Cisco IEM. By default, the Server tab is displayed. If the Server tab is not displayed, click the **Server** tab.

**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.

**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”.

**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**. The COBRA screen appears.

Next you will connect the Cisco IEC 4650 to the Cisco IEM.
Connecting to the Network

The Cisco IEC 4650 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 Cisco IEC 4650 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.

**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.
- To use a static IP address:
  - Uncheck the Use DHCP check box.
  - Enter the IP address in the IP Address field.
  - Enter the subnet mask in the Subnet Mask field.
  - Enter the gateway address in the Gateway field.
  - Enter the primary DNS server’s IP address in the Primary DNS server IP Address field.
  - If there is a second DNS server, enter the secondary DNS server’s IP address in the Secondary DNS server IP Address field.

**Step 5** Click Apply.

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

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

If the network connection is changed, the Cisco IEC 4650 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.

**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.
Connecting to the Network

Chapter 2  Setting Up the IEC

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**.

If you change the network connection, the Cisco IEC 4650 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.

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

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

All the wireless networks detected are displayed.

**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.

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

- 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.
Step 7  Click the **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**.

---

If you change the network connection, the Cisco IEC 4650 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 Manager Installation Guide* and *Cisco Interactive Experience Manager Administrator Guide* to install and configure the 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.

**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**.
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.

**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 Experience Platform 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.
Using a VNC Viewer

The IEC can be accessed by a VNC viewer. VNC is enabled or disabled in the IEM. The instructions below explain how to create a custom action for VNC, set the remoteview.enabled property in the IEM to 'true', and then launch the VNC viewer.

You will need the following:

1. The IEC’s Maintenance Code, which can be found in the General Tab of the device (see figure below)
2. A VNC viewer

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

Step 1  Log into the IEM.
Step 2  Click Policies in the left pane.
Step 3  In the Edit menu, click New Policy.
Step 4  Enter a policy name in the Policy Name field that indicates the purpose of this policy such as “VNC_Start” or “VNC_Viewer”.
Step 5  Check the Is action check box to make this policy runtime.
Step 6  Check the Add to custom actions checkbox to create a custom action.
Step 7  Click Create.
Step 8  After the policy is created, open the policy and click the Policy tab.
Step 9  Find the remoteview > enabled property.
Step 10  Change the value to true.
Step 11  Click Apply.
Step 12  When you are ready to use a VNC viewer to access an IEC, go to the IEM and find the device that you want to access using a VNC viewer.
Step 13  From the Custom actions menu, click the custom action that you created for VNC such as “VNC_Start”.
Step 14  Launch a VNC viewer.
Step 15  In the VNC Server field, enter the IEC’s IP address followed by a colon and the port number. For example, 188.32.16.55:5980.

Step 16  Click Connect.

Step 17  When prompted for a password, enter the IEC’s Maintenance Code.

Note  When entering the Maintenance Code as the password, enter the letters of the Maintenance Code as upper case. If for example the Maintenance Code is 6A54F3, enter “6A54F3”. The password will not work if you enter “6a54f3”.

The screen will then show the application that is currently running on the IEC.
Configuring Settings

Revised: February 16, 2016

Chapter Overview

Note

The Cisco IEC 4650 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 Cisco IEC 4650 settings for the network, proxy, and system. It also explains how to sort logs and reboot the Cisco IEC.

The topics in this chapter include the following:

- “Network Settings”
  - “Configuring an Ethernet Connection using DHCP”
  - “Configuring an Ethernet Connection using a Static IP Address”
  - “Configuring a Wireless Connection using DHCP”
  - “Configuring a Wireless Connection using a Static IP Address”
- “Proxy Server Settings”
  - “Static Option”
  - “Autoconfiguration Script Option”
  - “Autoconfiguration URL Option”
- “System Settings”
  - “Setting Management Mode”
  - “Setting Standalone Mode”
  - “Changing the IEM’s URL”
- “System Logs”
  - “Sorting Logs”
  - “Enabling the Debug Mode”
- “Reboot”
Network Settings

The Cisco IEC 4650 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.
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.
Step 5 Click Apply.
Step 6 To exit the Network window, click Close.
Step 7 In the System Settings window, click Reboot.

If you change the network connection, the Cisco IEC 4650 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.
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.
Step 5 Enter the IP address in the IP Address field.
Step 6 Enter the subnet mask in the Subnet Mask field.
Step 7 Enter the gateway address in the Gateway field.
Step 8 Enter the primary DNS server’s IP address in the Primary DNS server IP Address field.
Step 9 If there is a second DNS server, enter the secondary DNS server’s IP address in the Secondary DNS server IP Address field.
Step 10 When you complete the selections in this window, click Apply.
Step 11 To exit the Network window, click Close.
Step 12 In the System Settings window, click **Reboot**.

If you change the network connection, the Cisco IEC 4650 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.

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

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

**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.

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

- 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.

**Step 7** Click on the **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.

If you change the network connection, the Cisco IEC 4650 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.
Step 3  Click the Wireless radio button.
Step 4  Click Scan.
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.
    • If the security type is WPA Personal or WPA2 Personal:
      – Enter the passphrase in the 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.
    • 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.

Step 7 Click on the IP address tab.
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.

If you change the network connection, the Cisco IEC 4650 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.
Step 4 In the Proxy Server dialog box, choose the Static radio button as proxy type.
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.

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

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.
Step 4  In the Proxy Server dialog box, choose the Autoconfiguration URL radio button as proxy type.
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.
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 Cisco IEC 4650 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.

Now you will configure the system to connect the Cisco IEC 4650 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.

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 Manager host field.
Step 7 Click the Switch to managed 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.
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”.
Step 13 Click Reboot now.

Setting Standalone Mode

If you will not use the Cisco IEM to manage the kiosk, configure the Cisco IEC 4650 using the standalone mode.

Warning If you have already registered a Cisco IEM account, choosing standalone will unregister that account.

Step 1 Press Ctrl-Alt-S to display the System Settings window.
Step 2 Click the System icon.
Step 3 Enter the device name in the **Device name** field.

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 **Switch to standalone** button.

Step 7 In the Account Details dialog box, 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 Once the account is unregistered, you will see the word “Success”.

Step 12 Click the **Reboot now** button.

---

**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.

Step 3 In the System dialog box, enter the device name in the **Device name** field.

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 **Switch to standalone** button.

Step 7 In the Account Details dialog box, 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 the **Unregister** button.

Step 11 Once the account is unregistered, you will see the word “Success”.

Step 12 Click the **Reboot now** button. The IEC will reboot.

Step 13 After the IEC reboots, press **Ctrl-Alt-S** to display the System Settings window.

Step 14 Click the **System** icon.

Step 15 In the System dialog box, enter the device name in the **Device name** field.

Step 16 Enter the device description in the **Device Description** field.

Step 17 Enter the device location in the **Device Location** field.

Step 18 Enter the new IEM address in the **Manager host** field.
Step 19  Click the **Switch to managed** button.

Step 20  Enter the account name for the new IEM in the **Account** field.

Step 21  Enter the user name in the **User name** field.

Step 22  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 23  Click the **Register** button.

Step 24  Once the account is registered, you will see the word “Success”.

Step 25  Click the **Reboot now** button.

---

**Resetting the Device**

The Cisco IEC 4650 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.

Step 3  Click the **Device** tab.

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

Step 5  Click **Yes**.

---

**System Logs**

The System Logs window displays all the data collected since the device was last powered on. The Cisco IEC 4650 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.

### 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.

### 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.

- **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
  - bluetoothhd
  - co
  - dhclient
  - dmmd
  - kernel
  - management-daemon-system
ntpd
ntpd_intres
ntpdate
replicator
rsyslogd
sconsole
scron
sshd
udev-configure-printer
wpa_supplicant

**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.

**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 4650 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.

**Step 3**
Check the 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 4650 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**.
Chapter 4

Off-Line Caching

Chapter Overview

This chapter identifies how to enable aggressive caching on an IEC.
Topics in this chapter include:
- “Off-Line Caching”
  - “Configuring Property Settings in the IEM to Enable Aggressive Caching”

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.
Off-Line Caching

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.

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

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

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.

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

Step 11 (Optional) Set the web cache size.

Step 12 Click Apply.

Step 13 If you created a new policy for aggressive caching, apply it to the devices.
Upgrading the IEC

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”
  - “Saving XML Files”
- “IEC Firmware Upgrade Using the Terminal Utility”

Warning

Before upgrading an IEC to the latest version, ensure that the software version of the IEM is the latest too.

IEC Firmware Upgrade Using the IEM

You will need the following files that can be downloaded from 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.

Step 2
Click Supported Products

Step 3
Click IEC.

Step 4
Click 4600.
Step 5  Go to the Edit menu in the right pane and click **Versions**.
A list of versions is displayed in the center pane.
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.

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 +.
The Upload Image dialog box opens.

Step 11  Click +add.

Step 12  Find the file on your desktop and click **Open**.
The file appears in the Upload Image dialog box.

Step 13  Click **upload**.
The file will appear in the System Image list.

Step 14  In the Application column, click +.
The Upload Image dialog box opens.

Step 15  Click +add.

Step 16  Find the file on your desktop and click **Open**.
The file appears in the Upload Image dialog box.

Step 17  Click **upload**.
The file will appear in the Applications Image list.

Step 18  In the Specification column, click +.
The Upload Image dialog box opens.

Step 19  Click +add.

Step 20  Find the file on your desktop and click **Open**.
The file appears in the 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.
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.
Step 3  Click page to expand the drop-down list.
Step 4  Click View source.
The file opens in a 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.
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 uploaders 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:

- System file
- Application 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.
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.
Step 4  To view a list of commands, type help and press the Enter key.
Step 5  Locate the upgrade commands in the list.
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 uoloaders command.
Debugging Console

Chapter Overview

This chapter explains how to use the debugging console of the Cisco IEC 4650.
Topics in this chapter include:
- “Debugging Console”
  - “General Commands”
  - “Upgrade Commands”
  - “Debugging Commands”
  - “Management Commands”
  - “Properties Commands”

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.
To access the debugging console, follow these steps:

Step 1 Press Ctrl-Alt-S to open the 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.
Step 4 To view a list of commands, type help and press the Enter key.
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>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Show the help screen containing the list of commands</td>
</tr>
<tr>
<td>exit</td>
<td>Quit the shell</td>
</tr>
<tr>
<td>quit</td>
<td></td>
</tr>
<tr>
<td>sn</td>
<td>Show device’s serial number</td>
</tr>
<tr>
<td>dmc</td>
<td>Show the Device Maintenance Code (DMS)</td>
</tr>
<tr>
<td>reboot</td>
<td>Reboot the device (note that no confirmation to reboot will be asked)</td>
</tr>
<tr>
<td>reset</td>
<td>Reset the device to factory default settings and reboot (note that no confirmation will be asked)</td>
</tr>
</tbody>
</table>

### Upgrade Commands

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Show firmware version</td>
</tr>
<tr>
<td>usys &lt;url&gt;</td>
<td>Upgrade system firmware from URL</td>
</tr>
<tr>
<td>uapps &lt;url&gt;</td>
<td>Upgrade applications firmware from URL</td>
</tr>
<tr>
<td>uploaders</td>
<td>Upgrade loaders</td>
</tr>
</tbody>
</table>

*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 **uploaders** 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>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>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.</td>
</tr>
<tr>
<td>release</td>
<td>Switch the device to release mode to stop debug level logging. The device must be rebooted to start all the applications in release mode.</td>
</tr>
<tr>
<td>memstat</td>
<td>Print memory statistics</td>
</tr>
<tr>
<td>cpustat</td>
<td>Print CPU statistics</td>
</tr>
<tr>
<td>iostat</td>
<td>Print I/O statistics</td>
</tr>
<tr>
<td>dstat</td>
<td>Print local storage statistics</td>
</tr>
<tr>
<td>lsusb</td>
<td>List connected USB devices</td>
</tr>
<tr>
<td>lssinput</td>
<td>List connected input devices</td>
</tr>
<tr>
<td>httphead</td>
<td>Send HEAD request to URL url. Response header will be printed.</td>
</tr>
<tr>
<td>ifconfig</td>
<td>Show network interfaces configuration.</td>
</tr>
<tr>
<td>traceroute</td>
<td>Track the route packets taken from an IP network on their way to a given host.</td>
</tr>
<tr>
<td>nslookup</td>
<td>Query Internet domain name servers to find out host's IP addresses.</td>
</tr>
</tbody>
</table>

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

Management Commands

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

<table>
<thead>
<tr>
<th>Table 6-4</th>
<th>Management Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>mng</td>
<td>Show IEM’s URL</td>
</tr>
<tr>
<td>setmng &lt;url&gt;</td>
<td>Set IEM’s URL (note that the prefix will be ignored; it always should be ‘https’)</td>
</tr>
<tr>
<td>compression &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>dload</td>
<td>Load device’s profile from the IEM</td>
</tr>
<tr>
<td>diload</td>
<td>Load device’s information (name and description) from the IEM</td>
</tr>
<tr>
<td>dsave</td>
<td>Save device’s entire profile on the IEM</td>
</tr>
<tr>
<td>disave</td>
<td>Save device’s information (name and description) on the IEM</td>
</tr>
<tr>
<td>esave</td>
<td>Save events on the IEM (note that the saved events will be removed from the local event database)</td>
</tr>
<tr>
<td>dsync</td>
<td>Save unsaved properties from the device’s profile on the IEM</td>
</tr>
<tr>
<td>pingmng</td>
<td>Update device’s status on the IEM</td>
</tr>
<tr>
<td>ping &lt;host&gt;</td>
<td>Ping the specified host</td>
</tr>
<tr>
<td>ismanaged</td>
<td>Check if the device is in managed mode</td>
</tr>
<tr>
<td>isreg</td>
<td>Check if the device is registered in the IEM</td>
</tr>
<tr>
<td>reg &lt;account&gt; &lt;user&gt; [password]</td>
<td>Register device in the IEM</td>
</tr>
<tr>
<td>ureg &lt;user&gt; [password]</td>
<td>Unregister device in the IEM</td>
</tr>
</tbody>
</table>

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.

### Properties Commands

The properties commands display and set values and parameters.

<table>
<thead>
<tr>
<th>Table 6-5</th>
<th>Properties Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>rm [wildcard]</td>
<td>Remove persistent properties’ values (note that if no wildcard (‘*’) is provided, the entire storage will be cleared</td>
</tr>
<tr>
<td>ls [wildcard]</td>
<td>List properties’ values</td>
</tr>
<tr>
<td>lsp &lt;name&gt;</td>
<td>List persistent property’s value</td>
</tr>
</tbody>
</table>
### Command and Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set &lt;name&gt; &lt;value&gt;</code></td>
<td>Set properties’ values</td>
</tr>
<tr>
<td><code>lsc &lt;wildcard&gt;</code></td>
<td>List configuration parameters</td>
</tr>
<tr>
<td><code>setc &lt;name&gt; &lt;value&gt;</code></td>
<td>Set configuration parameters. Although the device description field in the IEM accepts spaces between words (e.g. “located in lobby of San Jose branch”), the <code>setc</code> command within the IEC’s terminal shell does not accept spaces for part of its value and returns the error: “ERROR: Invalid command or parameters. Type 'help' to print usage information”. Setc SJ located_in_lobby_of_San_Jose_branch</td>
</tr>
</tbody>
</table>

**Note**
The angle brackets (<>') indicates a required value. The square brackets ([ ]) indicate an optional value.
CHAPTER 7

Locally Configuring the IEC

Revised: February 16, 2016

Chapter Overview

Note
The Cisco IEC 4650 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 Cisco IEC 4650 settings for demos or special deployment situations.

The topics in this chapter include the following:

- “Setting Stand-Alone Mode”
- “Audio Settings”
  - “Specifying the Audio Input Device”
  - “Specifying the Audio Output Device”
- “Date and Time Settings”
  - “Setting the Date and Time”
  - “Selecting the Time Zone”
- “Display Settings”
  - “Adjusting the Rotation”
  - “Selecting the Master Video Display”
- “Keyboard Settings”
  - “Adjusting the Keyboard Parameters”
  - “Specifying the Keyboard Layout”
- “Kiosk Settings”
  - “Displaying the Navigational Panel and Content Title”
  - “Displaying a Website using the Kiosk URL feature”
  - “Specifying the Scrolling Mode”
“Mouse Settings”
  – “Changing the Mouse Button Order”
  – “Changing the Mouse Acceleration and Threshold”
  – “Displaying the Mouse Cursor”

### Setting Stand-Alone Mode

If you will not use the Cisco IEM to manage the kiosk, configure the Cisco IEC 4650 using the stand-alone mode.

**Warning**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Press Ctrl-Alt-S to display the System Settings window.</td>
</tr>
<tr>
<td>2</td>
<td>Click the System icon.</td>
</tr>
<tr>
<td>3</td>
<td>If the Server tab is not displayed, click the Server tab.</td>
</tr>
<tr>
<td>4</td>
<td>Enter the device name in the Device name field.</td>
</tr>
<tr>
<td>5</td>
<td>Enter the device description in the Device Description field.</td>
</tr>
<tr>
<td>6</td>
<td>Enter the device location in the Device Location field.</td>
</tr>
<tr>
<td>7</td>
<td>Click the Switch to standalone button.</td>
</tr>
<tr>
<td>8</td>
<td>Enter the account name in the Account field.</td>
</tr>
<tr>
<td>9</td>
<td>Enter the user name in the User name field.</td>
</tr>
<tr>
<td>10</td>
<td>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.</td>
</tr>
<tr>
<td>11</td>
<td>Click Unregister.</td>
</tr>
<tr>
<td>12</td>
<td>To exit the System window, click Close.</td>
</tr>
<tr>
<td>13</td>
<td>In the System Settings window, click Reboot.</td>
</tr>
</tbody>
</table>

### 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.
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 4650. 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 4650.
Step 4  From the Input drop-down list, choose USB camera microphone or USB headset.
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.
Step 3  Connect the cable from the output device to a port (HDMI, USB, TRS headphone, or IR) on the Cisco IEC 4650.
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.
Step 3  Click the 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.

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.

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

Step 4 From the **Closest city** drop-down list, choose a city.

Step 5 Click **Apply** to set the time zone.

Step 6 To exit the Date and Time window, click **Close**.

---

**Display Settings**

There are two 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 4650 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.

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.

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 Cisco IEC 4650 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.
Step 3 Click the General tab.
Step 4 From the Master drop-down list, choose the type of connection used for the video display.
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.
Step 3 Check the Enable keyboard repeat check box.
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 Cisco IEC 4650 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:
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 Cisco IEC 4650 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.
Step 3  Check the Title check box to display a title.
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.

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

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

**Displaying a Website using the Kiosk URL feature**

If the Cisco IEC 4650 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.
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.
Step 5  Click Apply.
Step 6  To exit the Kiosk window, click Close.
Step 7  In the System Settings window, click Reboot.
Specifying the Scrolling Mode

If scrolling is enabled, customers can scroll through the content on a page. When “Scroll bars” or “Kinetic scrolling” 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 “Scroll panes” 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.
Step 3 Enter the website address in the URL field.
Step 4 From the Scrolling mode drop-down list, choose a scrolling mode.
Step 5 Click Apply.
Step 6 To exit the Kiosk window, click Close.
Step 7 In the System Settings window, click Reboot.

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: Hide

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.
Step 3 To change the button order from right handed to left handed, click the Left handed radio button.
Step 4 Click Apply.
Step 5 To exit the Mouse window, click Close.
Step 6 In the System Settings window, click Reboot.
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.
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.
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.

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 to change the mouse cursor setting.
Step 4  To exit the Mouse window, click Close.
Step 5  In the System Settings window, click Reboot.
Compatible Peripherals

Appendix Overview

This appendix identifies which peripherals are compatible with the Cisco IEC 4650. Topics in this appendix include:

- “Compatible Peripherals”
  - “Touchscreens and Touchscreen Overlays”
  - “Monitors”
  - “Remote Controls”
  - “Wireless Keyboard and Mouse Combination”
  - “Wired Mouse”
  - “Wired Keyboards”
  - “Analog Speakers”
  - “Digital Speakers”
  - “Analog Headsets”
  - “Analog Microphones”
  - “Digital Microphones”
  - “Webcams”
  - “Document Cameras”
  - “Video Encoder Dongles”
  - “Printers”
  - “Optical Scanners”
  - “Barcode Scanners”
  - “Magnetic Card Readers”
  - “HDMI Switches”
  - “Wi-Fi: 3G USB Mobile Broadband”
- “Vendor Certification Guidelines”
Compatible Peripherals

This section contains a list of peripherals that have been tested or deployed with the Cisco IEC 4650 devices without incidence.

Other manufacturers and models may also be compatible. The following matrix indicates which of the following properties that peripherals should possess:

1. Interface: Indicates how the peripheral connects to the IEC
2. Emulates: Indicates what device that the peripheral emulates when it communicates with the IEC
3. Compatibility: Indicates any industry standards that the peripheral must meet
4. Widget: Indicates the IEC’s widget code that controls the peripheral

<table>
<thead>
<tr>
<th>Peripheral</th>
<th>Interface</th>
<th>Emulates</th>
<th>Compatibility Criteria</th>
<th>Widget</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Touch Screen</td>
<td>USB</td>
<td>HID (Human Interface Device)</td>
<td>Should not require special drivers.</td>
<td>N/A</td>
<td>Manufacturer should claim Linux support.</td>
</tr>
<tr>
<td>Printer</td>
<td>USB</td>
<td>CUPS</td>
<td>Global.printer</td>
<td></td>
<td>Due to the way the drivers are written and integrated into the distributions, it's recommended that you pick the model that’s 1+ years old, and is not a low-end model. HP has most developed drivers for Linux.</td>
</tr>
<tr>
<td>Scanner</td>
<td>USB</td>
<td>SANE Project Compatible <a href="http://www.sane-project.org/sane-supported-devices.html">http://www.sane-project.org/sane-supported-devices.html</a></td>
<td>Global.scanner</td>
<td></td>
<td>Most scanners that are supported are flatbeds. Very few multi-function printers are supported.</td>
</tr>
<tr>
<td>Mag-stripe and Barcode Reader</td>
<td>Keyboard</td>
<td></td>
<td>Global.magstripe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact-less ID Reader</td>
<td>USB</td>
<td>Keyboard</td>
<td>USB</td>
<td>Global.magstripe</td>
<td>Should not implement proprietary encryption protocols.</td>
</tr>
</tbody>
</table>
If you try a peripheral that is not on the list and is incompatible, the following are possible reasons for incompatibility:

- There is no Linux support for the device.
- The device is brand new. It is best to choose devices that are older than one year to ensure that Linux drivers have been developed and bugs with drivers have been fixed.
- The vendor of the device has not contributed to the OpenSource Ubuntu development tree.
- There are bugs in the driver.
- The IEC’s current Ubuntu distribution does not contain the particular driver.

**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.

**Touchscreens and Touchscreen Overlays**

Touchscreens and touchscreen overlays must support Linux and be HID (Human Interface Device) compliant. The following have been tested with version 2.3.3 and are supported:

- Elo Touchscreen ET1928L
- Elo Touchscreen ET2243L
- NEC MultiSync V552 (see next section for instructions on how to configure this touchscreen to work on a Linux platform)
- ViewSonic ePoster EP5502T
- Panasonic - See Table A-1 for a complete list of compatible Panasonic displays and touchscreens
- ELO - See Table A-2 for a complete list of compatible ELO touchscreens
### Table 8-2  Compatible Panasonic Touchscreens

<table>
<thead>
<tr>
<th>Application Family</th>
<th>Device Model Numbers</th>
<th>Device Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kiosk and Interactive Signage</td>
<td>TH-42LF60</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-47LF60</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-55LF60</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-42LF6</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-47LF6</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-55LF6</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>PPMT-IR42-EL</td>
<td>Overlay</td>
</tr>
<tr>
<td></td>
<td>PPMT-IR47-EL</td>
<td>Overlay</td>
</tr>
<tr>
<td></td>
<td>PPMT-IR55-EL</td>
<td>Overlay</td>
</tr>
<tr>
<td>Passive Signage</td>
<td>TH-42LFE7</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-65LFE7</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-47LFV5</td>
<td>Video Wall Display</td>
</tr>
<tr>
<td></td>
<td>TH-55LFV5</td>
<td>Video Wall Display</td>
</tr>
<tr>
<td></td>
<td>TH-55LFV50</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-47LFV70</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>TH-55LFV70</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>PT-DZ870</td>
<td>Projector</td>
</tr>
<tr>
<td></td>
<td>PT-DZ770</td>
<td>Projector</td>
</tr>
<tr>
<td></td>
<td>PT-DZ680</td>
<td>Projector</td>
</tr>
<tr>
<td></td>
<td>PT-DZ6700</td>
<td>Projector</td>
</tr>
<tr>
<td>Outdoor Passive Signage</td>
<td>TH-47LFX6</td>
<td>Display</td>
</tr>
</tbody>
</table>

### Table 8-3  Compatible ELO Touchscreens

<table>
<thead>
<tr>
<th>Family Name</th>
<th>Type of Enclosure</th>
<th>Size (Inches)</th>
<th>Aspect Ratio</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1215L</td>
<td>Desktop</td>
<td>12</td>
<td>4:3</td>
<td>E432532</td>
</tr>
<tr>
<td>1215L</td>
<td>Desktop</td>
<td>12</td>
<td>4:3</td>
<td>E991639</td>
</tr>
<tr>
<td>1247L</td>
<td>Open Frame</td>
<td>12</td>
<td>4:3</td>
<td>E655204</td>
</tr>
<tr>
<td>1509L</td>
<td>Desktop</td>
<td>15</td>
<td>16:9</td>
<td>E534869</td>
</tr>
<tr>
<td>1515L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E344320</td>
</tr>
<tr>
<td>1515L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E399324</td>
</tr>
<tr>
<td>1517L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E144246</td>
</tr>
<tr>
<td>1517L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E590483</td>
</tr>
<tr>
<td>1519L</td>
<td>Desktop</td>
<td>15.6</td>
<td>16:9</td>
<td>E175716</td>
</tr>
<tr>
<td>1519L</td>
<td>Desktop</td>
<td>15.6</td>
<td>16:9</td>
<td>E114849</td>
</tr>
<tr>
<td>Family Name</td>
<td>Type of Enclosure</td>
<td>Size (Inches)</td>
<td>Aspect Ratio</td>
<td>Part Number</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1519L</td>
<td>Desktop</td>
<td>15.6</td>
<td>16:9</td>
<td>E264492</td>
</tr>
<tr>
<td>1522L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E889598</td>
</tr>
<tr>
<td>1528L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E338457</td>
</tr>
<tr>
<td>1528L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E606958</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E619005</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E582772</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E659634</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E229149</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E641269</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E926109</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E101984</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E273617</td>
</tr>
<tr>
<td>1529L</td>
<td>Desktop</td>
<td>15</td>
<td>4:3</td>
<td>E733714</td>
</tr>
<tr>
<td>1537L</td>
<td>Open Frame</td>
<td>15</td>
<td>4:3</td>
<td>E731919</td>
</tr>
<tr>
<td>1537L</td>
<td>Open Frame</td>
<td>15</td>
<td>4:3</td>
<td>E701210</td>
</tr>
<tr>
<td>1537L</td>
<td>Open Frame</td>
<td>15</td>
<td>4:3</td>
<td>E512043</td>
</tr>
<tr>
<td>1541L</td>
<td>Open Frame</td>
<td>15.6</td>
<td>16:9</td>
<td>E805638</td>
</tr>
<tr>
<td>1541L</td>
<td>Open Frame</td>
<td>15.6</td>
<td>16:9</td>
<td>E606625</td>
</tr>
<tr>
<td>1715L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E603162</td>
</tr>
<tr>
<td>1715L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E719160</td>
</tr>
<tr>
<td>1717L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E649473</td>
</tr>
<tr>
<td>1717L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E679434</td>
</tr>
<tr>
<td>1717L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E179069</td>
</tr>
<tr>
<td>1717L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E227652</td>
</tr>
<tr>
<td>1729L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E763885</td>
</tr>
<tr>
<td>1729L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E274975</td>
</tr>
<tr>
<td>1729L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E461870</td>
</tr>
<tr>
<td>1729L</td>
<td>Desktop</td>
<td>17</td>
<td>5:4</td>
<td>E629992</td>
</tr>
<tr>
<td>1739L</td>
<td>Open Frame</td>
<td>17</td>
<td>5:4</td>
<td>E734455</td>
</tr>
<tr>
<td>1739L</td>
<td>Open Frame</td>
<td>17</td>
<td>5:4</td>
<td>E607940</td>
</tr>
<tr>
<td>1739L</td>
<td>Open Frame</td>
<td>17</td>
<td>5:4</td>
<td>E012584</td>
</tr>
<tr>
<td>1900L</td>
<td>Desktop</td>
<td>19</td>
<td>16:10</td>
<td>E500662</td>
</tr>
<tr>
<td>1915L</td>
<td>Desktop</td>
<td>19</td>
<td>5:4</td>
<td>E607608</td>
</tr>
<tr>
<td>1915L</td>
<td>Desktop</td>
<td>19</td>
<td>5:4</td>
<td>E266835</td>
</tr>
<tr>
<td>1919L</td>
<td>Desktop</td>
<td>18.5</td>
<td>16:9</td>
<td>E706956</td>
</tr>
<tr>
<td>1919L</td>
<td>Desktop</td>
<td>18.5</td>
<td>16:9</td>
<td>E876321</td>
</tr>
<tr>
<td>1919L</td>
<td>Desktop</td>
<td>18.5</td>
<td>16:9</td>
<td>E015447</td>
</tr>
<tr>
<td>Family Name</td>
<td>Type of Enclosure</td>
<td>Size (Inches)</td>
<td>Aspect Ratio</td>
<td>Part Number</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1919L</td>
<td>Desktop</td>
<td>18.5</td>
<td>16:9</td>
<td>E120415</td>
</tr>
<tr>
<td>1919L</td>
<td>Desktop</td>
<td>18.5</td>
<td>16:9</td>
<td>E803857</td>
</tr>
<tr>
<td>1928L</td>
<td>Desktop</td>
<td>19</td>
<td>5:4</td>
<td>E522556</td>
</tr>
<tr>
<td>1928L</td>
<td>Desktop</td>
<td>19</td>
<td>5:4</td>
<td>E935808</td>
</tr>
<tr>
<td>1928L</td>
<td>Desktop</td>
<td>19</td>
<td>5:4</td>
<td>E188117</td>
</tr>
<tr>
<td>1937L</td>
<td>Open Frame</td>
<td>19</td>
<td>5:4</td>
<td>E897317</td>
</tr>
<tr>
<td>1937L</td>
<td>Open Frame</td>
<td>19</td>
<td>5:4</td>
<td>E679610</td>
</tr>
<tr>
<td>1938L</td>
<td>Open Frame</td>
<td>19</td>
<td>16:10</td>
<td>E965017</td>
</tr>
<tr>
<td>1939L</td>
<td>Open Frame</td>
<td>19</td>
<td>5:4</td>
<td>E779866</td>
</tr>
<tr>
<td>1939L</td>
<td>Open Frame</td>
<td>19</td>
<td>5:4</td>
<td>E945445</td>
</tr>
<tr>
<td>1940L</td>
<td>Open Frame</td>
<td>19</td>
<td>16:9</td>
<td>E855244</td>
</tr>
<tr>
<td>2200L</td>
<td>Desktop</td>
<td>22</td>
<td>16:10</td>
<td>E808372</td>
</tr>
<tr>
<td>2201L</td>
<td>Desktop</td>
<td>22</td>
<td>16:9</td>
<td>E107766</td>
</tr>
<tr>
<td>2201L</td>
<td>Desktop</td>
<td>22</td>
<td>16:9</td>
<td>E382790</td>
</tr>
<tr>
<td>2239L</td>
<td>Open Frame</td>
<td>22</td>
<td>16:10</td>
<td>E846997</td>
</tr>
<tr>
<td>2240L</td>
<td>Open Frame</td>
<td>22</td>
<td>16:10</td>
<td>E186354</td>
</tr>
<tr>
<td>2242L</td>
<td>Open Frame</td>
<td>22</td>
<td>16:10</td>
<td>E667969</td>
</tr>
<tr>
<td>2243L</td>
<td>Open Frame</td>
<td>22</td>
<td>16:9</td>
<td>E059181</td>
</tr>
<tr>
<td>2244L</td>
<td>Open Frame</td>
<td>22</td>
<td>16:9</td>
<td>E469590</td>
</tr>
<tr>
<td>2400L</td>
<td>Desktop</td>
<td>24</td>
<td>16:10</td>
<td>E100905</td>
</tr>
<tr>
<td>2400L</td>
<td>Desktop</td>
<td>24</td>
<td>16:10</td>
<td>E964424</td>
</tr>
<tr>
<td>2639L</td>
<td>Open Frame</td>
<td>26</td>
<td>16:9</td>
<td>E864190</td>
</tr>
<tr>
<td>3200L</td>
<td>IDS</td>
<td>32</td>
<td>16:9</td>
<td>E994558</td>
</tr>
<tr>
<td>3239L</td>
<td>Open Frame</td>
<td>32</td>
<td>16:9</td>
<td>E162387</td>
</tr>
<tr>
<td>4200L</td>
<td>IDS</td>
<td>42</td>
<td>16:9</td>
<td>E841203</td>
</tr>
<tr>
<td>4200L</td>
<td>IDS</td>
<td>42</td>
<td>16:9</td>
<td>E505459</td>
</tr>
<tr>
<td>4600L</td>
<td>IDS</td>
<td>46</td>
<td>16:9</td>
<td>E960985</td>
</tr>
<tr>
<td>4600L</td>
<td>IDS</td>
<td>46</td>
<td>16:9</td>
<td>E536712</td>
</tr>
<tr>
<td>5500L</td>
<td>IDS</td>
<td>55</td>
<td>16:9</td>
<td>E053414</td>
</tr>
<tr>
<td>5500L</td>
<td>IDS</td>
<td>55</td>
<td>16:9</td>
<td>E891542</td>
</tr>
</tbody>
</table>

**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 MultiSynch 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.

**Monitors**

Any monitor with a Mini DisplayPort or HDMI connector will work with 2.3.3. It is recommended that you use a 1920 x 1080 resolution.

**Remote Controls**

The Cisco remote control that is supported for 2.3.3 is Cisco Remote Control IEP-IR-K9.

Other remote controls can also be used. See the “Non-Cisco Remote Controls” section in Appendix E for instructions on how to configure remote controls.

**Wireless Keyboard and Mouse Combination**

*A wireless keyboard cannot be used during the installation of the IEC.*

A wireless keyboard and mouse combination must be USB.

The following wireless keyboard and mouse combinations have been tested with 2.3.3 and are supported:

- Logitech USB wireless MK320
- Logitech USB wireless combo MK52
Wired Mouse

A wired mouse must be USB.

The following have been tested with 2.3.3 and are supported:

- Inland Optical USB Mouse
- Logitech Optical USB Mouse
- Targus AMU81USZ

Wired Keyboards

Note
A wired keyboard is required during the installation of the IEC.

A wired keyboard must be USB.

The following wired keyboards have been tested with 2.3.3 and are supported:

- Logitech USB Keyboard K120
- Logitech USB Keyboard K200
- Lenovo USB Keyboard LXN-EKB-10YA
- Microsoft Keyboard 600 1366

Analog Speakers

Any analog speaker will work with the IEC.

Digital Speakers

Digital speakers must be USB.

The following digital speakers have been tested with 2.3.3 and are supported:

- Altec Lansing Orbit USB speaker
- Logitech USB speaker S-0155A
- Logitech USB speaker S-150 (Volume control on the device does not take effect. The volume needs to be controlled from the IEC.)

Analog Headsets

All analog headsets except those with integrated microphones such as an iPhone headset will work with the IEC.
### Analog Microphones

Any analog microphone will work with the IEC.

### Digital Microphones

Digital microphones must be USB.

The following digital microphones have been tested with 2.3.3 and are supported:

- Logitech USB Desktop Microphone AK5370

### Webcams

Webcams must be HID compliant, USB, and V4L compatible.

The following webcams have been tested with 2.3.3 and are supported:

- Cisco PrecisionHD USB Firmware 1
- Logitech HD Portable 1080p Webcam C615
- Logitech C525
- Logitech C310
- Logitech C920

### Document Cameras

Document cameras must be USB and V4L compatible.

The following document cameras have been tested with 2.3.3 and are supported:

- Vaddio CeilingVIEW HD-18 DocCAM with DVI/HDMI Quick-Connect

### Video Encoder Dongles

The following video encoder dongles have been tested with 2.3.3 and are supported:

- System Dimensions AVS 2610 Portable Adaptive Video Streamer for Live Events

### Printers

Printers must be CUPS (abstraction library) compliant.

Cisco recommends the use of models that are 1+ years old.

Cisco recommends the use of more mature commercial-grade printers with longer lifespans. Consumer-grade printers where the models change frequently are less likely to be supported. 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.

The following printers have been tested with 2.3.3 and are supported:
• Microcom 814M 8.5" HID-compliant thermal kiosk printer
• HP LaserJet P3015
• HP LaserJet P2035
• HP P1606dn (The network feature is not supported. It can only print via a direct USB connection.)

HP printers should have HP Linux Imaging and Printing (HPLIP) 3.1 drivers (see http://hplipopensource.com/hplip-web/supported_devices/index.html)

Note: HP provides best Ubuntu compatibility.

### Optical Scanners

Optical scanners should be compatible with SANE (abstraction library).

Very few multifunctional scanners are supported. The following optical scanners have been tested with 2.3.3 and are supported:

• Epson Perfection V37
• HP ScanJet G4050
• HP 5590 Workgroup Scanner

### Barcode Scanners

Barcode scanners must have keyboard emulation and be USB.

The following barcode scanners have been tested with 2.3.3 and are supported:

• Honeywell Vuquest 3310g
• Cypress Semiconductor Corp. Barcode Reader

### Magnetic Card Readers

Magnetic card readers must have keyboard emulation and be USB.

The following magnetic card readers have been tested with 2.3.3 and are supported:

• MagTek 21040147
• MagTek 21040108

### HDMI Switches

The following HDMI switches have been tested with 2.3.3 and are supported:

• Extron HDMI Switcher
Wi-Fi: 3G USB Mobile Broadband

The following Wi-Fi devices have been tested with 2.3.3 and are supported:

- Sierra Wireless Aircard 597E
- Cisco 881G Ethernet Sec Router w/3G B/U

Vendor Certification Guidelines

Vendors of peripherals can perform self-certification based on the plug-and-play tests with the IEC. The following table provides a comparison of the use of standard Linux drivers and custom Linux drivers with some of the peripherals.

<table>
<thead>
<tr>
<th>Peripheral</th>
<th>Standard Linux Driver</th>
<th>Custom Linux Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Touchscreen</td>
<td>HID-based, emulates mouse</td>
<td>Requires custom drivers, closed</td>
</tr>
<tr>
<td>Magnetic card reader</td>
<td>HID-based, emulates keyboard</td>
<td>Closed, requires custom drivers, not visible to the browser application</td>
</tr>
<tr>
<td>Printer</td>
<td>CUPS compliant, drivers are included in distribution</td>
<td>Non-CUPS compliant, drivers must be installed, cannot be handled by the configuration and printer widget in Cobra</td>
</tr>
<tr>
<td>Keypad</td>
<td>Emulates keyboard, SR232</td>
<td>Closed to the system, cannot read from it from the application</td>
</tr>
</tbody>
</table>

Touchscreens

Vendors who want to certify touchscreens should ensure the following:

- Vendors should confirm that the touchscreen is supported WITHOUT inserting special drivers.
- Vendors should claim LINUX support.
- Vendors should claim support of HID.

Webcams and Document Cameras

Vendors who want to certify webcams or document cameras should ensure the following:

- The cameras should be USB-based.
- The cameras should be V4L compatible.

Printers

Vendors who want to certify printers should ensure the following:

- Printers’ drivers should be CUPS (abstraction library) compliant.
- Models should be 1+ years old.
- Printers should be Ubuntu compatible.
Appendix A
Compatible Peripherals

Scanners

Vendors who want to certify scanners should ensure the following:

- Scanners should be compatible with SANE (abstraction library).

**Note** Few multifunctional scanners are compatible.

Magnetic Card Readers

Vendors who want to certify magnetic card readers should ensure the following:

- Magnetic card readers should be USB-based or implement Serial-on-USB.
- Magnetic card readers should emulate keyboard events.
- Magnetic card readers should not implement proprietary encryption protocols.

Barcode Scanners

Vendors who want to certify barcode scanners should ensure the following:

- Barcode scanners should be USB-based or implement Serial-on-USB.
- Barcode scanners should emulate keyboard events.
- Barcode scanners should not implement proprietary encryption protocols.

ID Readers

Vendors who want to certify ID readers should ensure the following:

- ID readers should be USB-based or implement Serial-on-USB.
- ID readers should emulate keyboard events.
- ID readers should not implement proprietary encryption protocols.

Touchpads

Vendors who want to certify touchpads should ensure the following:

- Touchpads should be USB-based or implement Serial-on-USB.
- Touchpads should emulate keyboard events.
- Touchpads should not implement proprietary encryption protocols.
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”
- “Printer Implementation”
  - “global.printer Object”
  - “PrintJob”
  - “Example Usage of the global.printer Object”
  - “Best Practices and Tips”
  - “Testing the Printer Widget”

Printer Compatibility

Refer to Appendix A for a list of printers that have been tested with the IEC 4650.

\[\text{Note}\]
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 4650 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:

```plaintext
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;
    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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collateCopies</td>
<td>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 numCopies amount before the next page is started. With collating turned on, all pages are printed before the next copy of those pages is started.</td>
</tr>
<tr>
<td>colorCount</td>
<td>Contains the number of different colors available for the printer.</td>
</tr>
<tr>
<td>colorMode</td>
<td>Contains the current color mode.</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copyCount</td>
<td>Contains the number of copies that will be printed. The default value is 1.</td>
</tr>
<tr>
<td>doubleSidedPrinting</td>
<td>Contains true if double side printing is enabled.</td>
</tr>
<tr>
<td>duplex</td>
<td>Contains the current duplex mode.</td>
</tr>
<tr>
<td>fontEmbeddingEnabled</td>
<td>Contains true if font embedding is enabled.</td>
</tr>
<tr>
<td>fromPage</td>
<td>Contains the number of the first page in a range of pages to be printed (the &quot;from page&quot; 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 &quot;from page&quot; setting is unset.</td>
</tr>
<tr>
<td>fullPage</td>
<td>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.</td>
</tr>
<tr>
<td>widthMM</td>
<td>Contains the width of printing area in millimeters.</td>
</tr>
<tr>
<td>heightMM</td>
<td>Contains the height of printing area in millimeters.</td>
</tr>
<tr>
<td>isValid</td>
<td>Contains true if the printer currently selected is a valid printer in the system.</td>
</tr>
<tr>
<td>name</td>
<td>Contains the printer name.</td>
</tr>
<tr>
<td>orientation</td>
<td>Contains the orientation setting.</td>
</tr>
<tr>
<td>pageOrder</td>
<td>Contains the current page order.</td>
</tr>
<tr>
<td>paperSize</td>
<td>Contains the printer paper size.</td>
</tr>
<tr>
<td>paperSource</td>
<td>Contains the printer's paper source.</td>
</tr>
<tr>
<td>printerState</td>
<td>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).</td>
</tr>
<tr>
<td>resolution</td>
<td>Contains the current assumed resolution of the printer.</td>
</tr>
<tr>
<td>supportedResolutions</td>
<td>Contains a list of the resolutions (a list of dots-per-inch integers) that the printer says it supports.</td>
</tr>
<tr>
<td>supportsMultipleCopies</td>
<td>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.</td>
</tr>
<tr>
<td>abort()</td>
<td>Aborts the current print run. Returns true if the print run was successfully aborted and printerState 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.</td>
</tr>
<tr>
<td>newPage()</td>
<td>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.</td>
</tr>
<tr>
<td>getPageMargins()</td>
<td>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.</td>
</tr>
<tr>
<td>setPageMargins()</td>
<td>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.</td>
</tr>
<tr>
<td>paperSize()</td>
<td>Returns the paper size unit.</td>
</tr>
</tbody>
</table>
PrintJob

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

```java
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

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

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.
Example Usage of the global.printer Object

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

```html
<!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: #1048576; color: #000000; color: #eeeee;
  font: #1048576; weight: bold;
  font-family: Arial;
  font-size: 20px;
  color: #eeeee;
}
</style>
<script type="text/javascript">
var pageNumber;

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

function onPagePrinted(number)
{
  pageNumber.innerHTML = number;
}
</script>
</head>
<body>
</body>
</html>
```
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_1600x1200.jpg");
}
</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 Ctrl + 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 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”
- “Optical Scanner Implementation”
  - “global.scanner Object”
  - “Best Practices and Tips”
  - “Testing the Scanner Widget”

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:

```javascript
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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dpiX</td>
<td>DPI X of the selected scanner</td>
</tr>
<tr>
<td>dpiY</td>
<td>DPI Y of the selected scanner</td>
</tr>
<tr>
<td>color</td>
<td>Is selected scanner in color mode</td>
</tr>
<tr>
<td>source</td>
<td>Document source</td>
</tr>
<tr>
<td>devices</td>
<td>List of available scanners</td>
</tr>
<tr>
<td>sources</td>
<td>List of available document sources</td>
</tr>
<tr>
<td>lastError</td>
<td>Last error occurred</td>
</tr>
<tr>
<td>base64Data</td>
<td>Scanned image as base64 JPEG data</td>
</tr>
<tr>
<td>busy</td>
<td>Check if the scanner is busy</td>
</tr>
<tr>
<td>setCurrentScanner(in string deviceName)</td>
<td>Set the current scanner to use. You need to call this method before scanning.</td>
</tr>
<tr>
<td>finished()</td>
<td>The scanner has finished scanning</td>
</tr>
<tr>
<td>error(out string error)</td>
<td>An error has occurred</td>
</tr>
<tr>
<td>start()</td>
<td>Start scanning from the selected scanner and document source</td>
</tr>
<tr>
<td>stop()</td>
<td>Stop scanning</td>
</tr>
<tr>
<td>shutdown()</td>
<td>Shutdown scanning subsystem and reset all internal caches</td>
</tr>
</tbody>
</table>
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: February 16, 2016

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”
- “Magnetic Card Reader and Barcode Scanner Implementation”
  - “Magnetic Card Reader or Barcode Scanner Name”
  - “global.magstripe Object”
  - “Implement the global.magstripe Object”

Magnetic Card Reader and Barcode Scanner Compatibility

HID or keyboard emulation-type magnetic card readers and barcode scanners are supported by IEC 4650 devices. Refer to Appendix A for a list of magnetic card readers and barcode scanners that have been tested with the IEC 4650.

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 Touch id=14[slave pointer (2)]
  MCE IR Keyboard/Mouse (ite-cir) id=15[slave pointer (2)]
  Elo TouchSystems, Inc. Elo TouchSystems 2700 IntelliTouch(r) USB Touch monitor Interface id=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.

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:

```java
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>
<thead>
<tr>
<th><strong>Table D-1</strong></th>
<th><strong>global.magstripe Object Variables</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>open(in string deviceName)</td>
<td>Open the device for reading data. If <code>deviceName</code> is not empty, use this device name, and <code>browser.magstripe.scanner</code> property otherwise.</td>
</tr>
<tr>
<td>close()</td>
<td>Close the device.</td>
</tr>
<tr>
<td>opened()</td>
<td>The device has been open successfully.</td>
</tr>
<tr>
<td>scanning()</td>
<td>The device has started data scanning.</td>
</tr>
<tr>
<td>scanned(out string data)</td>
<td>The device has finished scanning, read the scanned data from <code>deviceName</code>.</td>
</tr>
<tr>
<td>error(out string error)</td>
<td>Error has occurred.</td>
</tr>
</tbody>
</table>

**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.
Infrared Remote Controls

Appendix Overview

An Infrared (IR) Cisco Remote Control can be connected to the Cisco IIEC 4650 device so that the end user can control applications and remote playback without touching the screen or using a mouse. This appendix explains how to configure applications to allow use of either a Cisco and non-Cisco remote control.

Topics in this appendix include:

- “Cisco Remote Control IEP-IR-K9”
  - “Battery”
  - “Infrared Sensor”
  - “Remote Control Buttons”
  - “Remote Control Implementation”
  - “global.ir Object”
  - “Usage of global.ir Object”
- “Non-Cisco Remote Controls”
  - “Using the IEM’s IR Configuration Property”
  - “Using the API”

Cisco Remote Control IEP-IR-K9

The Cisco Remote Control IEP-IR-K9 is the remote control model that is supported with the IEC.

Battery

⚠️ Lithium Batteries are used in this module. Do not try to charge, discharge, or replace these batteries.
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:

1. Place the remote control on a flat surface, button-side down.
2. To unlock the battery clip and remove it, pinch the locking mechanism and slide the clip out of the remote control.
3. To remove the old battery from the clip, pivot the battery so that it touches only the opening of the clip.
4. Insert a new battery so that positive charge (+) symbols are visible simultaneously on the battery and the clip.
5. Slide the clip back into 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.

Note: Please ensure that you are using a suitable IR cable that was suggested by your Cisco distributor or importer source.

Remote Control Buttons

All the buttons can be programmed. The functions listed in the tables below are standard functions for the keys.
### Table E-1  System Control Buttons

<table>
<thead>
<tr>
<th>Function</th>
<th>IR Signal Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>0xff 00 0090</td>
</tr>
<tr>
<td>Input</td>
<td>0xef 10 0090</td>
</tr>
<tr>
<td>Information</td>
<td>0xe0 1f 0090</td>
</tr>
<tr>
<td>Help</td>
<td>0xf6 09 0090</td>
</tr>
</tbody>
</table>

### Table E-2  Playback Control Buttons

<table>
<thead>
<tr>
<th>Function</th>
<th>IR Signal Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play</td>
<td>0xf9 06 0090</td>
</tr>
<tr>
<td>Pause</td>
<td>0xfd 02 0090</td>
</tr>
<tr>
<td>Stop</td>
<td>0xfc 03 0090</td>
</tr>
<tr>
<td>Rewind</td>
<td>0xfb 04 0090</td>
</tr>
<tr>
<td>Fast forward</td>
<td>0xfa 05 0090</td>
</tr>
<tr>
<td>Live</td>
<td>0xf7 08 0090</td>
</tr>
</tbody>
</table>

*Note* The Live button is usually used to jump to the next channel or track.

### Table E-3  Audio Control Buttons

<table>
<thead>
<tr>
<th>Function</th>
<th>IR Signal Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume increase</td>
<td>0xbf 40 0090</td>
</tr>
<tr>
<td>Volume decrease</td>
<td>0xbe 41 0090</td>
</tr>
<tr>
<td>Mute</td>
<td>0xFE 01 0090</td>
</tr>
</tbody>
</table>

### Table E-4  Channel Control Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>IR Signal Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel down (-)</td>
<td>0xbc 43 0090</td>
</tr>
<tr>
<td>Channel up (+)</td>
<td>0xbd 42 0090</td>
</tr>
<tr>
<td>Last</td>
<td>0xe3 1c 0090</td>
</tr>
<tr>
<td>1</td>
<td>0xf2 0d 0090</td>
</tr>
<tr>
<td>2</td>
<td>0xf1 0e 0090</td>
</tr>
<tr>
<td>3</td>
<td>0xf0 0f 0090</td>
</tr>
<tr>
<td>4</td>
<td>0xe1 1e 0090</td>
</tr>
<tr>
<td>5</td>
<td>0xe8 17 0090</td>
</tr>
</tbody>
</table>
The following is an example of programming for the remote control in an application:

```javascript
if(!filterIR){
    filterIR = true;
    document.getElementById("trace").innerHTML = 'IR pressed key code: "key"
    ("skey")';
    switch(skey){
    case "play":
    // additional code here
    }
}
```

### Table E-5 Menu Control Buttons

<table>
<thead>
<tr>
<th>Function</th>
<th>IR Signal Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu</td>
<td>0xb8 47 0090</td>
</tr>
<tr>
<td>Up</td>
<td>0xea 15 0090</td>
</tr>
<tr>
<td>Left</td>
<td>0xec 13 0090</td>
</tr>
<tr>
<td>OK</td>
<td>0xed 12 0090</td>
</tr>
<tr>
<td>Right</td>
<td>0xeb 14 0090</td>
</tr>
<tr>
<td>Down</td>
<td>0xe9 16 0090</td>
</tr>
</tbody>
</table>

### Table E-6 Guide Control Buttons

<table>
<thead>
<tr>
<th>Function</th>
<th>IR Signal Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guide</td>
<td>0xf5 0a 0090</td>
</tr>
<tr>
<td>Page up</td>
<td>0xea 15 0090</td>
</tr>
<tr>
<td>Page down</td>
<td>0xf3 0c 0090</td>
</tr>
<tr>
<td>Exit</td>
<td>0xee 11 0090</td>
</tr>
</tbody>
</table>

### Table E-7 Soft Keys

<table>
<thead>
<tr>
<th>Button</th>
<th>IR Signal Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0xa9 56 0090</td>
</tr>
<tr>
<td>B</td>
<td>0xaf 50 0090</td>
</tr>
<tr>
<td>C</td>
<td>0xad 52 0090</td>
</tr>
<tr>
<td>D</td>
<td>0xab 54 0090</td>
</tr>
</tbody>
</table>
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:

```javascript
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-8  global.ir Object Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lastError</td>
<td>Last error occurred</td>
</tr>
<tr>
<td>availableControls()</td>
<td>Returns the list of the supported remote controls</td>
</tr>
<tr>
<td>setCurrentControl(in string device)</td>
<td>Sets the current remote control to use.</td>
</tr>
<tr>
<td></td>
<td>The device name must be obtained from availableControls() list.</td>
</tr>
<tr>
<td></td>
<td>Leave the device name empty to use browser.ir.configuration. In this case you should set browser.ir.configuration.enabled to true and browser.ir.configuration to the valid LIRC configuration.</td>
</tr>
<tr>
<td>event(in uint key, in string skey, in string configName)</td>
<td>Remote control event</td>
</tr>
<tr>
<td></td>
<td>• The event control code is set to key.</td>
</tr>
<tr>
<td></td>
<td>• The control name (such as &quot;poweroff&quot;, &quot;ch1&quot;, &quot;up&quot;, etc.) is set to skey.</td>
</tr>
<tr>
<td></td>
<td>• The configuration name, which is rarely needed, is set to configName.</td>
</tr>
</tbody>
</table>

Usage of global.ir Object

The following HTML code contains an example of global.ir usage.

```html
<!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;
    }
  
```
<script type="text/javascript">
var errorId;
var eventId;
var controlId;
var timer;
var remoteInfo;

function init()
{
  errorId = document.getElementById("error");
  eventId = document.getElementById("event");
  controlId = document.getElementById("control");
  remoteInfo = document.getElementById("remoteInfo");

  global.ir.error.connect(onError); writeLog("onError() connected to signal global.ir.error");
  global.ir.event.connect(onEvent); writeLog("onEvent() connected to signal global.ir.event");

  try{
    var irconf = global.registry.value("browser.ir.configuration");
    if(irconf!='<binary mimeType="text/plain"><! [CDATA[]]> </binary>') {
      // set default remote as current.
      //global.ir.setCurrentControl(defaultRemote);
      remoteInfo.innerHTML = "Default (Cisco remote control)");
      writeLog("Default remote control configuration applied.");
    } else{
      global.ir.setCurrentControl();
      remoteInfo.innerHTML = "* user defined remote control *";
      writeLog("User defined remote control configuration applied.");
    }
  } catch(ex){
    writeLog("Exception: "+ex);
  }
}

function deinit()
{
  global.ir.error.disconnect(onError);
  global.ir.event.disconnect(onEvent);
}

function onError(err)
{
  eventId.innerHTML = err;
  writeLog("onError(): "+err);
}

function onEvent(key, skey, config)
{
  eventId.innerHTML = "* key + ' ' + skey + ' ' + config;";
  writeLog("onEvent(): "+key + " " + skey + " " + config);

  clearTimeout(timer);
  timer = setTimeout(function() { eventId.innerHTML = ""; }, 750);"};
</script>
Non-Cisco Remote Controls

This section explains how to customize remote control programming so that non-Cisco remote controls can be used. You can use either the IEM’s IR Configuration property or the global.ir.setCurrentControl() API.

Using the IEM’s IR Configuration Property

To customize remote control programming, you will need to perform the following tasks:

1. Create a new group if the devices that will use the customized programming are not already in a group
2. Add devices to the new group
3. Create an IR configuration policy and upload the remote’s Linux Infrared Remote Control (LIRC) config file from the manufacturer
4. Apply policy to the device group

Create a New Group

If the devices that will use the customized programming are not already in a group, create a new group by following these steps:
Appendix E  Infrared Remote Controls

Non-Cisco Remote Controls

Step 1  Click Devices in the left pane.

Step 2  In the Edit menu, click New Group.

Step 3  In the Create New Group dialog box, enter a group name in the Group Name field such as “IRConfig_IECs”.

Step 4  Click Create.

A folder labeled with the group’s name appears in the left and center panes.

Add Devices to the New Group

Add all the devices that will use the customized programming to this new group:

Step 1  Click Devices in the left pane.

Step 2  In the center pane, double-click the new group’s icon.

Step 3  In the Edit menu, click Properties.

Step 4  Click the Member Of tab in the center pane to view a list of devices in the group.

Step 5  Click +.

Step 6  In the Add to Group dialog box, check the devices’ check boxes.

Step 7  Scroll to the bottom of the Add to Group dialog box and click Add.

Step 8  Click Apply.

Step 9  In the Predefined actions menu, click Reboot.

Step 10  Click OK.

Create an IRConfig Policy

You will need a remote configuration file for this task. Contact the manufacturer of your remote control to obtain it.

Follow these steps to create a policy for the IR configuration:

Step 1  Click Policies in the left pane.

Step 2  In the Edit menu, click New Policy.

Step 3  Enter a policy name (for example, “IRConfig”) in the Policy Name field of the Create New Policy dialog box.

Step 4  Click Create. A new policy is created and its icon appears in the center pane.

Step 5  Click the Policy tab within the new policy.

Step 6  Click the browser > ir > configuration property.

Step 7  Go to the IR configuration button under the Value column.

Step 8  Click Load file in the IR configuration editor and upload the LIRC config file for your remote control.
Step 10 Click **Apply**.

### Apply the IRConfig Policy to the Device Group

Now apply the policy to the device group:

**Step 1** Click **Devices** in the left pane.

**Step 2** In the center pane, click on the new groups icon.

**Step 3** In the Edit menu, click **Properties**.

**Step 4** Click the **Policies** tab.

**Step 5** In the Available policies list, choose the IRConfig policy.

**Step 6** Click the green arrow.

The policy now appears in the Applied policies list.

**Step 7** Click **Apply**.

**Step 8** In the Predefined actions menu, click **Reboot**.

**Step 9** Click **OK**.

### Using the API

The IR can also be configured using the `global.ir.setCurrentControl()` API.

**Step 1** Create and upload the LIRC config file for the remote.

**Step 2** To enable and use the uploaded config file, call `global.ir.setCurrentControl()` API from your application. See the “global.ir Object” section above for information on how to call the API.

The user-defined remote controller should now work.
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”
- “SipPhone Widget”
  - “Sample Test Code”
- “IEC Preparation”
- “SIP Client”
- “Cisco IP Phone Set Up on the CUCM”
  - “Finding The IP Phone’s MAC Address”
- “Cisco IEC Set Up on the CUCM”
- “Configuring Call Manager Information”
  - “Using a Policy on the IEM”
  - “Using the SipPhone Widget”
- “SIP DTMF”
  - “Sample usage of sendDtmf() API”

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:

```javascript
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 set idleImage (in string imgurl, in bool stretchFlag);
        bool changeidleImage (in string imgurl, in bool stretchFlag);
        string cameraDevice() const;
        int setCameraDevice (in string deviceId);
        int capture() const;
        string getImage() const; // Returns the Jpeg imgage if captured
        void answer();
        void reject();
        void setAutoAnswer (in bool autoAnswerFlag);

    signals:
        void ready();
        void registered();
        void placingCall();
        void incomingCall();
        void established();
        void ring();
        void disconnected();
        void video();
        void novideo();
        void hold();
        void resume();
        void captured();
        void error (in int code, in string explanation);
};
```
## Table F-1 sipphone Variables

<table>
<thead>
<tr>
<th>Method Call</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>start(username, password, domain, transport)</code></td>
<td>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).</td>
</tr>
<tr>
<td><code>call(sipUri)</code></td>
<td>This method should be used only after the <code>start(...)</code> method is called. This method initiates the call to the sipUri (called party).</td>
</tr>
<tr>
<td><code>hangup()</code></td>
<td>This method, when called, disconnects the existing call.</td>
</tr>
<tr>
<td><code>sendDtmf(dtmfkey)</code></td>
<td>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 #.</td>
</tr>
<tr>
<td><code>setIdleImage(imgUrl, stretchFlag)</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>changeIdleImage(imgUrl, sipUri)</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>cameraDevice()</code></td>
<td>This method returns the currently configured webcam that is being used by the SipPhone widget. The value returned would be in the UNIX format similar to “/dev/video0”.</td>
</tr>
<tr>
<td><code>setCameraDevice()</code></td>
<td>Use this method to let the SipPhone widget know which webcam to use to place the call. You need to call this API with UNIX format identifier for camera, such as “/dev/video0” or “/dev/video1”.</td>
</tr>
<tr>
<td><code>capture()</code></td>
<td>Use this method to initiate taking a still image when the video call is in progress. This is useful if you would like to take a snapshot of the participant and save it for future reference.</td>
</tr>
</tbody>
</table>

**Note** Call this API before the `start()` method in the Javascript.

**Caution** Call this routine only when there is an active video call.
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getImage()</td>
<td>Call this method after you have received a captured() signal. When called, this routine returns base64 content of the JPEG image captured.</td>
</tr>
<tr>
<td>answer()</td>
<td>Accepts incoming call.</td>
</tr>
<tr>
<td>reject()</td>
<td>Rejects incoming call.</td>
</tr>
<tr>
<td>setAutoAnswer(bool autoAnswerFlag)</td>
<td>Enables auto answer mode if the autoAnswerFlag is “true”.</td>
</tr>
<tr>
<td>ready()</td>
<td>This signal is indicative that values given for initializing the SIP phone are accepted.</td>
</tr>
<tr>
<td>registered()</td>
<td>This signal means that the SIP phone is now registered with the SIP Registrar (or Call Manager) and you can make and receive calls from the widget.</td>
</tr>
<tr>
<td>placingCall()</td>
<td>This signal means the widget is trying to place the call to the called party of interest.</td>
</tr>
<tr>
<td>incomingCall()</td>
<td>This signal means the widget is receiving an incoming call request from another SIP peer.</td>
</tr>
<tr>
<td>established()</td>
<td>This signal is indicative that the call is in progress.</td>
</tr>
<tr>
<td>ring()</td>
<td>This signal means that the called party has been notified about the incoming call.</td>
</tr>
<tr>
<td>disconnected()</td>
<td>This signal means that the call has been terminated.</td>
</tr>
<tr>
<td>video()</td>
<td>This signal means that the call was negotiated as a video call and the remote site video is available to display.</td>
</tr>
<tr>
<td>novideo()</td>
<td>This signal means that the call that was negotiated does not have video being sent by the remote end. The application can use the novideo signal to improve the user experience such as displaying a “Please wait” message.</td>
</tr>
<tr>
<td>hold()</td>
<td>This signal means that the remote party has put the call on hold. An image can be displayed on the screen when a SIP call is placed on hold. The image that is included in this signal will be shown on the screen.</td>
</tr>
<tr>
<td>resume()</td>
<td>This signal means that the remote party has resumed the call. Upon receiving this signal, the application will revert to the original screen and the on-hold image will be hidden.</td>
</tr>
</tbody>
</table>
Sample Test Code

```html
<!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;
}
.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;
}
</style>
</head>
```

This signal is fired when an user action of taking a still snapshot of an video call is successfully finished. Once this signal is fired, the application can call getImage() to get the captured image (as a JPEG image).

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.

**Error Codes:**

- 404: No answer
- 401: Registration failed
- 485: User busy
- 494: User not found
- 486: Call manager not able to route call
- 503: Service unavailable
SipPhone Widget

-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;
}
.status {color:#848d9d; text-shadow:0 -1px 1px #000; font:normal 14px Arial, Helvetica, sans-serif; height:41px;}
.bottomPanel {background:#0e1014 url('img/bottom_panel_bg.png') top left repeat-x;
}
.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: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;}
{-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}
.dislpad_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";
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+\")
    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";
    sipStatus.innerHTML = "Call";
    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);
  sipbutton.disabled = false;
  sipbutton.className="callButton";
  sipbutton.innerHTML=" ";
  sipStatus.innerHTML = "Connecting to server...";
  sipTimer.className = "timerOff";
  sipRegistered.className = "LED_off";
  writeLog('Waiting for server...');
  checkRegistrationStatusTimeout = setTimeout("onDisconnected()", 15000);
}
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 = 0;
    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("?", 0)+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%">
                                    <tr>
                                        <td width="49%" style="min-width:160px" align="left"><span class="status" id="SIPstatus"></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"></div></td>
                                                        <td width="74" align="center" style="width:74px"><img id="camera" src="img/eye.png" width="30" height="30"></td>
                                                        <td width="44"><img id="registeredLED" class="LED_off" src="img/spacer.png" width="44" height="24"></td>
                                                </tr>
                                            </div>
                                        </td>
                                        <td width="49%" style="min-width:160px" align="right"></td>
                                    </tr>
                                </table>
                            </td>
                        </tr>
                    </table>
                </td>
            </tr>
        </table>
    </div>
</div>
</body>
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)

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.

SIP Client

In order for the SIP to work, the Cisco IEC 4650 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 version 9.x or 10.x
- Cisco IEC4650
- 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.
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).
Step 5  Enter admin in the Username field of the 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.
Step 9  Click the Find button.
All the devices registered on the CUCM will be listed.
Step 10  To add a new phone, click Add New.
Step 11  From the Phone Type drop-down menu, choose Cisco 9951.
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.

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.
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.
Step 20  From the Cisco Camera drop-down menu within the Product Specific Configuration Layout, choose Enabled.
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.
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.

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.

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.

Step 34 Choose the Administrator Settings icon, which is button #4 on the 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.

**Second Method**

Step 1 Press the System Settings button.

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.

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 4650 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 4650 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.
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).
Step 5 Enter admin in the Username field of the 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.
Step 9 Click the Find button.
All the devices registered on the CUCM will be listed.
Step 10 To add a new phone, click Add New.
Step 11 From the Phone Type drop-down menu, choose Third Party SIP Device (Advanced).
Step 12 Click Next.
Step 13 Enter the Cisco IEC 4650 device’s MAC address in the MAC Address field within the Device Information area.

Note The Cisco IEC 4650 device’s MAC address is located on the label on the back of the device.

Step 14 Enter a description of the Cisco IEC 4650 device. This field automatically enters “SEP” plus the MAC Address but the field 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 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 4650 device to be activated, it must be associated with a User Profile.
Step 21 From the User Management drop-down menu, choose End User.
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.

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’.

The user profile and the Cisco IEC 4650 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.
Step 29 Click the Find button.

All the devices registered on the CUCM will be listed.

Step 30 Choose the Cisco IEC 4650 device, which starts with the letters “SEP” followed by the MAC address.

Step 31 On the Phone Configuration screen, choose Line [1] – Add a new DN within the Association Information area.

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.

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.

Step 37 Click Add Selected.

Step 38 Click Close.

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.

Step 43 Click Save.

Step 44 Click Apply Config.

This Cisco IEC 4650 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.

**Step 6** In the Application data editor, click +.

**Step 7** Click key:value.

**Step 8** Enter `sip.target` in the key field.

**Step 9** Enter the directory number in the value field.

**Step 10** Click Ok.

   If you click on data property’s Value field, you will see the data in the form sip.target:[directoryNumber].

   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 +.
Configuring Call Manager Information

**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.

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.

```html
....
{
    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.
  ```java
  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 have the **Media Termination Point Required** checkbox unchecked.
  3. The **Unattended Port** checkbox should be unchecked.
  4. The **Require DTMF Reception** checkbox should be unchecked.
  5. The **Allow Presentation Sharing using BFCP** checkbox should be unchecked.
  6. The **Allow iX Applicable Media** checkbox should be unchecked.

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:

```javascript
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:

```html
<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>
```
Stream Live Video

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 setup 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”
- “Vaddio HD Document Camera”
- “Stream Live Video”
  - “Connect Hardware”
  - “global.videoEncoder Object”

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.

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.

**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>
<thead>
<tr>
<th>Rotary Switch Setting</th>
<th>HD Camera Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>720p/59.94</td>
</tr>
<tr>
<td>1</td>
<td>1080i/59.94</td>
</tr>
<tr>
<td>2</td>
<td>1080p/59.94</td>
</tr>
<tr>
<td>3</td>
<td>1080p/60</td>
</tr>
<tr>
<td>4</td>
<td>720p/50</td>
</tr>
<tr>
<td>5</td>
<td>1080i/50</td>
</tr>
<tr>
<td>6</td>
<td>1080p/50</td>
</tr>
<tr>
<td>7</td>
<td>1080p/30</td>
</tr>
<tr>
<td>8</td>
<td>1080p/25</td>
</tr>
<tr>
<td>9</td>
<td>1024 x 768/60 RGBHV</td>
</tr>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>1280 x 800/60 RGBHV</td>
</tr>
<tr>
<td>F</td>
<td>1680 x 1050/60 RGBHV</td>
</tr>
</tbody>
</table>
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**

**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.

<table>
<thead>
<tr>
<th>Number</th>
<th>Connection</th>
<th>Purpose</th>
<th>Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EZCamera Power &amp; HD Video Port</td>
<td>Supplies power to camera and returns HD video from the camera</td>
<td>CAT-5e Ethernet cable</td>
</tr>
<tr>
<td>2</td>
<td>SR Interface to Camera</td>
<td>RS-232 control to and from camera and IR signals returned from the camera</td>
<td>CAT-5e Ethernet cable</td>
</tr>
</tbody>
</table>
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.

```javascript
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();

}
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>videoInputCount</td>
<td>Returns the available video sources including the HDMI input from the USB dongle and all available webcams.</td>
</tr>
<tr>
<td>videoInputDescription</td>
<td>Returns the description of all video input devices present in the box.</td>
</tr>
<tr>
<td>targetHost</td>
<td>Returns the target host to which the encoded stream is being sent.</td>
</tr>
<tr>
<td>targetPort</td>
<td>Returns the port number on which the encoded stream is being sent.</td>
</tr>
<tr>
<td>protocol</td>
<td>Returns integer value for the Transport Protocol: ‘0’ for UDP or ‘1’ for TCP.</td>
</tr>
<tr>
<td>videoMode</td>
<td>Returns video mode on which the video encoder is operating. Values are: ‘0’ - SD, ‘1’ - HD, and ‘2’ for Custom.</td>
</tr>
<tr>
<td>videoSource</td>
<td>Returns the video source being selected for encoding either as ‘0’ for HDMI or ‘1’ for videoInputCount for webcam.</td>
</tr>
<tr>
<td>h264Profile</td>
<td>Returns the encoding H.264 profile being used by the encoder: ‘0’ for Baseline, ‘1’ for Main, and ‘2’ for Extended Profile.</td>
</tr>
<tr>
<td>inputResolution</td>
<td>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.</td>
</tr>
<tr>
<td>isProgressive</td>
<td>Returns ‘true’ if the scan format is set to Progressive.</td>
</tr>
<tr>
<td>streamType</td>
<td>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.</td>
</tr>
<tr>
<td>inputFrameRate</td>
<td>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.</td>
</tr>
<tr>
<td>outputFrameRate</td>
<td>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.</td>
</tr>
<tr>
<td>averageOutputBitRate</td>
<td>Returns the Video-Out Average Bit Rate in kbps.</td>
</tr>
<tr>
<td>minimumOutputBitRate</td>
<td>Returns the Video-Out Minimum Bit Rate in kbps.</td>
</tr>
<tr>
<td>maximumOutputBitRate</td>
<td>Returns the Video-Out Maximum Bit Rate in kbps.</td>
</tr>
<tr>
<td>outputResolution</td>
<td>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.</td>
</tr>
<tr>
<td>Method</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>audioBitRate</td>
<td>Returns the Audio-Out Bit Rate being sent from the encoder in bps.</td>
</tr>
<tr>
<td>setTargetHost(in string targetHost)</td>
<td>Allows you to set the Target Host (IP Address either as Unicast or Multicast ipv4 Address).</td>
</tr>
<tr>
<td>setTargetPort(in string targetPort)</td>
<td>Allows you to set the Target Host’s (Layer4) port Number (TCP or UDP port number).</td>
</tr>
<tr>
<td>setProtocol(in int transportProtocol)</td>
<td>Allows the Transport (Layer 4) Protocol to be used when sending the encoded stream. Choices are ‘0’ for UDP or ‘1’ for TCP.</td>
</tr>
<tr>
<td>setVideoMode(in int videoMode)</td>
<td>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.</td>
</tr>
<tr>
<td>setVideoSource(in int videoSource)</td>
<td>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.</td>
</tr>
<tr>
<td>setH264Profile(in int h264Profile)</td>
<td>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.</td>
</tr>
<tr>
<td>setInputResolution(in int inputResolution)</td>
<td>Allows you to set the input resolution for the video source. Choices are ‘0’ for 1920x1080, ‘1’ for 1280x720, and ‘2’ for 1024x600.</td>
</tr>
<tr>
<td>setProgressive(in int flag)</td>
<td>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’.</td>
</tr>
<tr>
<td>setStreamType(in int streamType)</td>
<td>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.</td>
</tr>
<tr>
<td>setInputFrameRate(in int frameRate)</td>
<td>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.</td>
</tr>
<tr>
<td>setOutputFrameRate(in int frameRate)</td>
<td>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.</td>
</tr>
<tr>
<td>setAverageOutputFrameRate(in int avgRate)</td>
<td>Allows you to set the Average Output Rate (Video-Out) in kbps.</td>
</tr>
<tr>
<td>setMinimumOutputBitRate(in int minRate)</td>
<td>Allows you to set the Minimum Output Rate (Video-Out) in kbps.</td>
</tr>
<tr>
<td>setMaximumOutputBitRate(in int maxRate)</td>
<td>Allows you to set the Maximum Output Rate (Video-Out) in kbps.</td>
</tr>
</tbody>
</table>
Stream Live Video

global.videoEncoder object Enumeration

{
    enum ErrorCodes
    {
        videoEncoderNotPresent = -1,
        UnableToStopStreaming = -2,
        UnableToStartStreaming = -3,
        RemoteSideNotListening = -4,
        MemoryExhaustionError = -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
{
    StreamProgram = 0,
    StreamTransport = 1,
    StreamMp4 = 2,
    StreamElementary = 3,
    StreamRav = 4,
};
enum InputFrameRate
{
    Input15fps = 0,
    Input24fps = 1,
    Input30fps = 2,
    Input60fps = 3,
};
enum OutputFrameRate
{
    Output15fps = 0,
    Output24fps = 1,
    Output30fps = 2,
    Output60fps = 3,
};
# Content Guidelines

Revised: February 16, 2016

## Content Guidelines

The following table lists the content guidelines for the Cisco IEC 4650.

<table>
<thead>
<tr>
<th>Table H-1</th>
<th>Content Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Video formats</strong></td>
<td>Multiple video formats are supported on the native player including MPEG-1, MPEG-2, MPEG-4, and H.264. 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). Formats not recommended: On2 VP 6 (used by old FLV)</td>
</tr>
</tbody>
</table>

| Note | Native video is strongly preferred over Flash video. |
| Note | The IEC 4650 supports WebM (VP8/Vorbis) and Ogg (Theora/Vorbis) for HTML5 video. |
| Note | Use of the native player strongly preferred over HTML5 video. |
| Note | The native player’s video compatibility can be validated by using VLC 2.0.8. |
| **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

When using a native player, the IEC 4610 can support H.264 video up to 720p @ 6Mbps.

**Note** 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.

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.

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.

**Note** 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.

**Note** 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.

### Screen Resolutions

Up to 1920x1080 (1080p); IEC4650 defaults to monitor’s native resolution

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.

### Screen Rotations

Both horizontal (landscape) and vertical (portrait) modes are supported with 90, 180, 270 degree turns. The content should be laid out naturally.

### General Content Guidelines

HTML/JavaScript is a preferred mechanism for building kiosk applications.

Use of Flash should be limited to small size and non-video rendering functionality.

Ticker tapes should be using CSS3 for scrolling.

“Screensaver” video playback should be postponed when the kiosk is being interacted with to avoid audio conflicts and preserve responsiveness.

Regularly-playing videos should be cached locally.