Release Notes for Cisco DX Series Firmware Release 10.2(2)

Revised: April 29, 2015,

Cisco DX Series Devices

Cisco DX Series devices provide these capabilities:

- High-definition (HD) voice and video communications
- Conferencing with Cisco WebEx meeting applications
- Presence and instant message with the Cisco Jabber messaging integration platform
- On-demand access to cloud services
- Native support for HD 1080p at 30 frames per second (fps)
- Video calling interoperability to other H.264 video endpoints, such as these:
    - Cisco Unified IP Phone 8900 and 9900 Series models
    - Cisco Jabber platform on personal mobile devices
    - CTS-compliant Cisco TelePresence endpoints and room systems

Because they are Compatibility Test Suite (CTS) compliant with the open Android™ platform, Cisco DX Series devices offer you access to the ecosystem of Cisco and commercial third-party applications that are developed for Android. You can also develop custom applications for Android and deploy them to both Cisco DX Series devices and mobile users. The Cisco DX Series devices also take advantage of the touch-directed ease of use of Android, and its ability to personalize experiences with customizable home screens, communications widgets, ringtones, and more.

New and Changed Features

Note Some features may require the installation of a Cisco Unified Communications Manager Device Package. Failure to install the Device Package before the phone firmware upgrade may render the phones unusable.

Features Available with Firmware Release

AAC-LD Codec

Cisco DX70 and Cisco DX80 support the AAC-LD wideband audio compression codec.

Acoustic Echo Canceller and Laptop Shadowing

Cisco DX80 includes an Acoustic Echo Canceller (AEC) and laptop shadowing. Users at the far end of a call experience clear audio quality even if the user puts an obstacle, such as a laptop, in front of one of the microphones. If the current microphone is blocked by an object, the device automatically switches to the other microphone array in the other foot.

Binary Floor Control Protocol

Binary Floor Control Protocol (BFCP) allows users to share a presentation within an ongoing video conversation. BFCP is automatically enabled.

Content Viewing and Sharing via HDMI In Port

With Cisco DX70 and Cisco DX80, you can share your PC (MAC) desktop, or any other source that uses HDMI, by connecting to the HDMI In port.

Presentation starts only when you tap **Start sharing**. Before you do so, you see a preview that is not shared with anyone.

You can use this feature to see your own PC desktop in a call without sharing it. The video call is then displayed as a picture-in-picture (PiP).

Document Camera

With Cisco DX70 and Cisco DX80, your system camera can work as a document camera. Just tilt your camera to present a physical document or any other physical object that is lying on your table in front of the system. The camera senses what you do to it and automatically flips the image vertically. Thus, the image appears as expected to the far end.

IPv6

The device supports Internet Protocol Version 6 (IPv6) addresses.

Configure IPv6 in the Settings application under Ethernet options.

PC Display

With Cisco DX70 and Cisco DX80, you can use the PC Display feature to see your own PC desktop in a call without sharing it. The video call is then displayed as a picture-in-picture (PiP). If you use PiP but want to return to a full-screen video call without sharing your PC desktop, double-tap the PiP (without tapping any of its buttons).

SE Android

The Security Enhancements for Android™ (SE Android) feature enhances device security. SE Android protects against malicious applications through prevention of attempts to execute unauthorized or dangerous code on the device. SE Android does the following:

- Can prevent privilege escalation by processes
- Can prevent misuse and limit damage if privileged process, such as root, is compromised
- Provides centralized, enforced, analyzable policy
- Protects from undiscovered vulnerabilities

The device contains a policy that specifies the data that an application, process, or user can access. SE Android supports two modes:

- Permissive
- Enforcing

Anything that violates the policy is logged. If the mode is enforcing, the action is denied. No user nor administrator control exists over the policy or the mode.

When you upgrade a Cisco DX650to Release 10.2(2), it remains in permissive mode because it must work with existing field units. After a Cisco DX650 has been factory reset, the mode switches automatically to enforcing mode.

Enforcing mode remains in effect for the Cisco DX650 unless the device is downgraded to a firmware release below 10.2(2). Upon upgrade to Release 10.2(2) or later, the device returns to permissive mode until factory reset is performed.

Cisco DX70 and Cisco DX80 devices are always in enforcing mode from the factory. Cisco DX70 and Cisco DX80 devices cannot be placed in permissive mode.

Self Care Portal

From the Cisco Unified Communications Self Care Portal, users can customize and control phone features and settings. For information about the Self Care Portal, see the *Cisco Unified Communications Self Care Portal User Guide* located at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html.

As the administrator, you control access to the Self Care Portal. You must also provide information to your users so that they can access the Self Care Portal.

Before a user can access the Cisco Unified Communications Self Care Portal, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager End User group.

You must provide end users with the following information about the Self Care Portal:

- The URL to access the application. This URL is:

  http://<server_name:portnumber>/ucmuser/, where server_name is the host on which the web server is installed and portnumber is the port number on that host.

- A user ID and default password to access the application.
- An overview of the tasks that users can accomplish with the portal.

These settings correspond to the values that you entered when you added the user to Cisco Unified Communications Manager.

SHA-256 Manufacturing Installed Certificate

Cisco DX70 and Cisco DX80 use a manufacturing installed certificate (MIC) with the signature algorithm of SHA-256 with an RSA 2048 key. The signature algorithm requires Cisco Unified Communications Manager, Cisco Secure Access Control Server (ACS), and Secure SRST support.

The SHA-256 MIC feature has the following support requirements:

- Cisco Unified Communications Manager Release 9.1(2) and later
- ACS Release 5.2 and later.

Note ACS 5.2 and later do not support EAP-FAST with EAP-TLS inner method. Use EAP-TLS or migrate to ISE for EAP-FAST with EAP-TLS inner method.

- IOS 12.4(15)T1 and later
- Cisco Identity Service Engine release is 1.1 and later. The EAP-FAST with EAP-TLS inner method is supported starting from ISE release 1.2 and later.

The Cisco certificate authority issuing the MIC for this series of phones can be obtained from the following links if separate applications are used and these applications need to authenticate MIC from the phone:

- http://www.cisco.com/security/pki/certs/cmca2.cer
- http://www.cisco.com/security/pki/certs/crcam2.cer

These Cisco certificate authorities must be imported into applications in order for the applications to authenticate MIC for Cisco DX Series devices.

Two-Microphone Array Beam Forming

Cisco DX80 includes two-microphone array beam forming. If the user moves out of the beam (that is, out of the camera view), the sound sent to the far end weakens. All sound sources that are not located within the pickup beam (in front of the unit) attenuate.

TIP/MUX

Telepresence Interoperability Protocol (TIP)/Multiplex (MUX), or TIP/MUX, is an IP protocol that is used to negotiate audio and video media options between endpoints prior to reception or transmission of media.

TIP/MUX is invoked for multiparticipant conferences and enables content sharing.

Uniform Resource Identifier Dialing

The Uniform Resource Identifier (URI) Dialing feature allows the user to place calls by using an alphanumeric URI address as a directory number, for example, bob@cisco.com. The user must enter the URI address to select the contact.

The screen displays the call information for the URI call. The call logs record the URI call information in the Call History and the Details page.

For more information, see *Features and Services Guide for Cisco Unified Communications Manager*.

Uniform Resource Identifier Dialing Enhancement
Allows you to specify the device display preference for calls that have both Directory Number (DN) and URI available.

If the URI Dialing Display Preference is set to DN, DN is displayed when available. If the URI Dialing Display Preference is set to URI, URI is displayed when available.

To specify the preference, set the URI Dialing Display Preference service parameter in the Clusterwide Parameters (Device - Phone) pane for the Cisco CallManager service in Cisco Unified Communications Manager Administration.

Cisco DX650 User Interface Updates

This release includes updates to the user interface for all core applications and the Setup Assistant. The Desktop Widget was added to provide shortcuts to configured applications on the Home screen.

Camera Application
The native Android Camera application has been removed as of this release.

Features Available with Latest Device Packs

It is required that the latest device packs be installed before configuring your Cisco DX Series devices.

For information about Cisco DX Series devices and the required Cisco Unified Communications Manager device packs, see the following URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html

Operating Modes

The values for the Device UI Profile field in the Cisco Unified Communications Manager Administration product-specific configuration parameters have been updated to the following:

- Simple Mode (default)
- Enhanced Mode
- Public Mode

For more information on the operating modes available for Cisco DX Series devices, see the "Customizations" chapter of the *Cisco DX Series Administration Guide*.

Deploy Simple Mode on Existing Devices

Procedure

Step 1 Install the latest device packs on your Cisco Unified Communications Manager servers.

Step 2 Choose one of the following options:

- For bulk deployment: In the **Enterprise Phone Configuration** window or the **Common Phone Profile** window, verify that **Device UI Profile** is set to Simple Mode.
- For individual deployment: In the **Phone Configuration** window, verify that **Device UI Profile** is set to Simple Mode.

Step 3 Check **Override Common Settings**.
The device reboots into Simple Mode after a minute. The user may experience error messages before the device reboots.

Deploy Simple Mode on a New Device

Procedure

Step 1 Install the latest device packs on your Cisco Unified Communications Manager servers.

Step 2 In the **Enterprise Phone Configuration** window or the **Common Phone Profile** window, verify that **Device UI Profile** is set to Simple Mode.

Step 3 Check **Override Common Settings**.

Step 4 Register the device to Cisco Unified Communications Manager.

Installation Notes

System Requirements

Cisco DX Series devices are supported by Cisco Unified Communications Manager Release 8.5(1), 8.6(1), 8.6(2), 9.1(2), 10.5(1) and later.

The initial release of Cisco DX Series devices requires the latest device pack installed on each Cisco Unified Communications Manager release.

Install Firmware Release on Cisco Unified Communications Manager

Before using the Cisco DX Series firmware release on the Cisco Unified Communications Manager, you must install the latest Cisco Unified Communications Manager firmware on all Cisco Unified Communications Manager servers in the cluster.

Procedure

Step 1 Go to the following URL: http://software.cisco.com/download/navigator.html.

Step 2 Choose **Collaboration Endpoints** > **Collaboration Desk Endpoints** > **Cisco DX Series**.

Step 3 Choose your device type.

Step 4 In the Latest Releases folder, choose **10.2(2)**.

Step 5 Select one of the following firmware files, click the **Download** or **Add to cart** button, and follow the prompts:

- For Cisco DX70: cmterm-dx70.10-2-2-23.cop.sgn
- For Cisco DX80: cmterm-dx80.10-2-2-23.cop.sgn
- For Cisco DX650: cmterm-dx650.10-2-2-23.cop.sgn
- For all Cisco DX Series devices: cmterm-dxseries.10-2-2-23.cop.sgn

Note If you added the firmware file to the cart, click the **Download Cart** link when you are ready to download the file.

Step 6 Click the arrow next to the firmware file name in the Download Cart section to access additional information about this file. The link for the readme file is in the Additional Information section. The readme file contains installation instructions for the corresponding firmware.

Step 7 Follow the instructions in the readme file to install the firmware.

Install Firmware ZIP Files

If a Cisco Unified Communications Manager is not available to load the installer program, the following .zip files are available to load the firmware.

Firmware upgrades over the WLAN interface may take longer than upgrades that use a wired connection. Upgrade times over the WLAN interface may take more than an hour, depending on the quality and bandwidth of the wireless connection.

Procedure

Step 1 Go to the following URL: http://software.cisco.com/download/navigator.html.

Step 2 Choose **Collaboration Endpoints** > **Collaboration Desk Endpoints** > **Cisco DX Series**.

Step 3 Choose your device type.

Step 4 In the Latest Releases folder, choose **10.2(2)**.

Step 5 Download the relevant zip files.
Zip files are available for each model: one each for Cisco DX650, Cisco DX70, and Cisco DX80.

A fourth zip file, cmterm-dxseries.10-2-2-23.cop.sgn, allows you to download the firmware for all Cisco DX Series devices in a single step.

Step 6 Unzip the files.

Step 7 Manually copy the unzipped files to the directory on the TFTP server. See *Cisco Unified Communications Operating System Administration Guide* for information about how to manually copy the firmware files to the server.

Important Note

Cisco Virtual Office Setup

In a Cisco Virtual Office setup, Cisco recommends the use of a Cisco 881 Integrated Services Router instead of the Cisco 871 router.

Limitations and Restrictions

- When a user is sharing their computer desktop in a Cisco DX70 or Cisco DX80 presentation call, any audio from the desktop is not shared.
- Users should only pair their mobile phone with one Cisco DX Series device at a time.
- The only supported external cameras for Cisco DX650 are the Logitech C920-C Webcam and Logitech C930e.
- Cisco DX Series devices do not support Android apps that require portrait mode, GPS, or Accelerometer. However, apps that support both portrait and landscape are supported in landscape mode.
- Use the Google Play™ Store to find and add applications to your phone. Depending on your security settings, the Google Play Store may not be available. Cisco does not guarantee that an application that you download from a third-party site will work.
- For Cisco DX70, the HDMI Out port is enabled. However, the HDMI Out port only supports mirror mode.
- For Cisco DX80, the HDMI Out port is disabled.
- To prevent unauthorized copying of Digital Rights Management (DRM) protected HD video through the HDMI port, an HDMI monitor (or any HDMI sink device) that is connected to a Cisco DX650 or a Cisco DX70 must be HDCP compliant.
- Cisco DX650 devices labeled with TAN 68-5217-xx cannot be downgraded below version 10.2(2)

Problem Report Tool in Simple Mode

In Simple Mode, the Problem Report Tool generates logs and debug data locally, and does not email these to the device administrator. Instead, the user is given a file name, which the administrator can access through the device serviceability web page.

Device Redistribution

When an administrator redistributes a device (that is, gives the device to a different user), the administrator should execute a factory reset of the device to remove any user data that was previously stored on the device.

If an administrator changes the user ID of a device from user A to user B, none of the data that is associated with user A will be available to user B. The new user must download apps and other data. This scenario may apply to a single user that changes from an old user ID to a new user ID.

Behavior During Times of Network Congestion

Anything that degrades network performance can affect voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

To reduce or eliminate any adverse effects, schedule administrative network tasks during a time when the devices are not being used or exclude the devices from testing.

Supported Languages

Arabic, Egypt (ar_EG)	French, France (fr_FR)	Portuguese, Brazil (pt_BR)
Bulgarian, Bulgaria (bg_BG)	German, Germany (de_DE)	Portuguese, Portugal (pt_PT)
Catalan, Spain (ca_ES)	Greek, Greece (el_GR)	Romanian, Romania (ro_RO)
Chinese, PRC (zh_CN)	Hebrew, Israel (he_IL)	Russian (ru_RU)
Chinese, Taiwan (zh_TW)	Hungarian, Hungary (hu_HU)	Serbian, Republic of Serbia (sr_RS)
Croatian, Croatia (hr_HR)	Italian, Italy (it_IT)	Slovak, Slovakia (sk_SK)
Czech, Czech Republic (cs_CZ)	Japanese (ja_JP)	Slovenian, Slovenia (sl_SI)
Danish, Denmark (da_DK)	Korean (ko_KR)	Spanish, Spain (es_ES)
Dutch, Netherlands (nl_NL)	Latvian, Latvia (lv_LV)	Swedish, Sweden (sv_SE)
English, Britain (en_GB)	Lithuanian, Lithuania (lt_LT)	Thai, Thailand (th_TH)
English, US (en_US)	Norwegian bokmål , Norway (nb_NO)	Turkish, Turkey (tr_TR)
Finnish, Finland (fi_FI)	Polish (pl_PL)	

View Caveats

You can search for problems by using the Cisco Bug Search. To access Cisco Bug Search, you need a Cisco.com user ID and password.

Known caveats (bugs) are graded according to severity level, and can either be open or resolved.

Procedure

Step 1 Perform one of the following actions:

- To find all open Cisco DX650 caveats for this release, use this URL: https://tools.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=284721679&st=Session%20Initiation%20Protocol%20(SIP)%20Software&sb=anfr&rls=10.2(2)&sts=open&svr=3nH&srtBy=byRel&bt=custV
- To find all open Cisco DX70 caveats for this release, use this URL: https://tools.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286267306&rls=10.2(2)&sb=anfr&sts=open&svr=3nH&srtBy=byRel&bt=custV
- To find all open Cisco DX80 caveats for this release, use this URL: https://tools.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286267308&rls=10.2(2)&sb=anfr&sts=open&svr=3nH&srtBy=byRel&bt=custV
- To find all resolved caveats for this release, use this URL: https://tools.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=284721679&st=Session%20Initiation%20Protocol%20(SIP)%20Software&sb=anfr&rls=10.2(2)&sts=fd&svr=3nH&srtBy=byRel&bt=custV

Step 2 Log in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the Search for field, then press **Enter**.

Documentation, Service Requests, and Additional Information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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

Related Documentation

Cisco DX Series

All Cisco DX Series documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

User-oriented documents are available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-user-guide-list.html

Administrator-oriented documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

The *Cisco DX Series Wireless LAN Deployment Guide* is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-implementation-design-guides-list.html

Translated publications are available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-translated-end-user-guides-list.html

Open Source license information is available as the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-licensing-information-listing.html

Regulatory Compliance and Safety Information is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-installation-guides-list.html

Cisco Unified Communications Manager

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Business Edition 6000

Refer to the *Cisco Business Edition 6000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 6000 release. Navigate from the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

Cisco and the Environment

Related publications are available at the following URL:

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

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

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

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

The following information is for FCC compliance of Class B devices: 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 the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

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

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

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

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


The Bluetooth word mark and logo are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Cisco Systems, Inc., is under license.

Google, Google Play, Android and certain other marks are trademarks of Google Inc.

The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing LLC in the United States and other countries.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands