Release Notes for Cisco DX Series Firmware Release 10.2(4)

First Published: June 23, 2015

Last Modified: October 26, 2015

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

AES 256 Encryption

When connected to Cisco Unified Communications Manager Release 10.5(2) and later, DX Series devices support AES 256 encryption support for TLS and SIP for signaling and media encryption. This enables the devices to initiate and support TLS 1.2 connections using AES-256 based ciphers that conform to SHA-2 (Secure Hash Algorithm) standards and are Federal Information Processing Standards (FIPS) compliant.

AnyConnect VPN

The AnyConnect VPN client has been upgraded to version 4.0.01303.

Jabber Application

The Jabber application has been updated to version 10.6.2. With this version, users can send and receive files start a call or start a WebEx meeting from a Jabber conversation. See Cisco Jabber for Android Release Notes for more information.

Related Topics

http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-release-notes-list.html

Mobile and Remote Access Through Expressway (Market Beta)

Mobile and Remote Access through Expressway requires Cisco Expressway 8.6 or later and Cisco Unified Communications Manager 10.5.2 SU2 or Cisco Unified Communications Manager 11.0 or later.

Cisco Expressway provides a way for remote workers to easily and securely connect their Cisco DX Series devices into the corporate network without using a VPN. Expressway uses Transport Layer Security (TLS) to secure network traffic. To establish a TLS session, the device must authenticate an Expressway certificate signed by a public Certificate Authority trusted by the device firmware. It is not possible to install or trust other CA certificates on DX Series devices for authenticating an Expressway certificate. See the Cisco DX Series Administration Guide for the list of trusted CA certificates embedded in the devices.

Note The marketing beta release of Mobile and Remote Access Through Expressway is made available to allow customers to test and evaluate the feature, but is NOT recommended for production use. There is no official Cisco TAC support until the feature is officially released in a future firmware load. To provide feedback, send an email to cefeedback@cisco.com.

The Maximum Session Bit Rate for Video Calls on the default region on Cisco Unified Communications Manager is 384 kbps by default. The Default call bandwidth on Expressway-C is also 384 kbps by default. These settings should be increased to deliver the expected video quality for the DX Series.

The rate of Mobile and Remote Access authorizations for a device is controlled by default on the Expressway server. The default setting is 3 authorizations in 300 seconds. Increase that rate if your Expressway server is issuing HTTP 429 “Too Many Requests” errors.

Add the Problem Report Tool server address to the Expressway HTTP server allow list to ensure that users are able to use the PRT.

For more information, see *Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide*.

Mobile and Remote Access Limitations and Restrictions

- DX Series devices connected through Expressway cannot access web browsing, or email services hosted inside the enterprise network.
- The Off Hook/KPML Dialing, Mobility, DND, Call Back, and drop conference participants features are only supported with Expressway 8.6 and later.
- Busy Line Field features require Cisco Unified Communications Manager 11.0 or later.
- A device connected through Expressway cannot download APKs from an APK server inside the enterprise network. The device can download APKs from an APK server on a public network as long as the host is accessible.
- You do not have SSH access to the device from the corporate network.
- You do not have access to the device web page from the corporate network.
- Self-provisioning is not supported through Expressway.

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

Cisco Expressway Credentials Persistence

The new Product Specific Configuration Options parameter **User Credentials Persistent for Expressway Sign In** allows you to make user credentials for Cisco Expressway persist on DX Series devices. User credentials stored on the device are encrypted.

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.

Cisco Unified Communication Manager Public Keys

To improve software integrity protection, new public keys are used to sign cop files for Cisco Unified Communications Manager Release 10.0.1 and later. These cop files have “k3” in their name. To install a k3 cop file on a pre-10.0.1 Cisco Unified Communications Manager, consult the README for the ciscocm.version3-keys.cop.sgn to determine if this additional cop file must first be installed on your specific Cisco Unified Communications Manager version. If these keys are not present and are required, you will see the error “The selected file is not valid” when you try to install the software package.

Install Firmware Release on Cisco Unified Communications Manager

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

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(4)**.

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-dx70.10-2-4-46.cop.sgn
- For Cisco DX80: cmterm-dx80.10-2-4-46.cop.sgn
- For Cisco DX650: cmterm-dx650.10-2-4-46.cop.sgn
- For all Cisco DX Series devices: cmterm-dxseries.10-2-4-46.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 filename 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.

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(4)**.

Step 5 Download the relevant zip files.

- For Cisco DX70: cmterm-dx70.10-2-4-46.zip
- For Cisco DX80: cmterm-dx80.10-2-4-46.zip
- For Cisco DX650: cmterm-dx650.10-2-4-46.zip

Step 6 Unzip the files.

Step 7 Manually copy the unzipped files to the folder 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 a 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 devices. 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 works.
- For Cisco DX70, the HDMI Out port only supports mirror mode.

  For Cisco DX80, the HDMI Out port is disabled.

  Cisco DX650 and Cisco DX70 support HDCP through the HDMI Out port in mirror mode. An HDMI monitor (or any HDMI sink device) that is connected to a Cisco DX650 or a Cisco DX70 must be HDCP-compliant. Cisco DX Series devices do not support HDCP on the HDMI in port.
- Cisco DX650 devices labeled with TAN 68-5217-xx cannot be downgraded below version 10.2(2)
- If you are deploying Cisco DX Series devices for secure calls with IPv6 and an earlier Cisco Unified Communications Manager version than Release 11, go to the CUCM **Service Parameters** page, select **Advanced Options**, and set **SIP Max Incoming Message Size** to the maximum setting (20000).

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.

Step 1 Perform one of the following actions:

- To find all caveats for this release, use this URL: https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284711383&rls=10.2(4)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV
- To find all open caveats for this release, use this URL: https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284711383&rls=10.2(3),10.2(2),10.2(1),10.2(4)&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=284711383&rls=10.2(4)&sb=fr&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

© 2015 Cisco Systems, Inc. All rights reserved.