Cisco DX Series Security Overview

White Paper

June 2015

Cisco DX Series Security Overview

The Cisco® DX Series (Cisco DX650, Cisco DX70, and Cisco DX80) includes many security options:

- Signed firmware images and secure boot
- Remote wipe
- Microsoft Exchange ActiveSync
- Security Enhancements for Android (SE)
- Administratively disable Google Play
- Administratively disable Wi-Fi
- Administratively disable Bluetooth
- Administratively disable installation of apps from unknown sources
- Administratively enable “simple mode”
- Administratively disable USB port
- Administratively enable encrypted video (Secure Real-Time Transport Protocol [SRTP]) and Session Initiation Protocol (SIP) signaling (Transport Layer Security [TLS])
- Cisco AnyConnect® 3.0 VPN client
- Cryptographically assured device identity

Cisco DX Series System Security

The firmware running on the DX Series endpoints includes the Android operating system, which Cisco has customized with enhanced security features.

The DX Series can load only firmware images signed by Cisco.

Secure Boot

- Hardware helps ensure that only firmware approved by Cisco can run.
- The first code that executes is nonmutable code.
- Execution of the boot sequence is authenticated by a previously trusted step.
- Secure boot chain starts from Boot ROM code and the installed firmware validates the digital signature.
- Secure boot is always on; there is no provision for bypassing.

Device Identity

- Each Cisco DX Series endpoint contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC provides a unique, factory-installed identity for the phone and allows Cisco Unified Communications Manager (UCM) to authenticate the phone.
- Each DX Series endpoint supports deployment of customer-signed identity in lieu of a MIC. Customers can install a local significant certificate (LSC) to bind the DX Series endpoint to the specific environment.

System Secure Upgrade

- The digital signature of the firmware is verified before firmware can become active.
- The firmware is signed using 2048-bit RSA.
- The firmware signature encompasses the Android operating system, framework, and default applications.

Secure Provisioning

- The configuration file is digitally signed to provide authenticity and integrity of the configuration.
- The configuration file can be signed and encrypted to further provide privacy protection of configuration data.
- The encrypted configuration file can be decrypted only by the designated DX Series endpoint.

Security-Enhanced Android

Starting with firmware Release 10.2(2), Cisco owns the policy and updates through firmware.

- SE Android is always in enforcing mode for the DX70 and DX80. The DX650, if upgraded from a load prior to release 10.2(2), requires a factory reset to go into enforcing mode.
- Privilege escalation and misuse are prevented.
- Applications that could damage other applications or the system integrity are limited or blocked.

Extension Mobility Multiuser

The Extension Mobility multiuser feature offers users the ability to log in and log out of the DX device. When the user logs in, the Cisco Unified Communications Manager server authenticates the user PIN, using the same methodology as Extension Mobility for Cisco IP Phones.

- File-system-level permission settings are changed to prevent one user from accessing other users' data.
- Extension Mobility service can be secured using HTTPS.
- This applies to all modes: public, simple, and enhanced.

Cisco Expressway (10.2.4 or later)

Administrators can choose between Cisco Expressway MRA (Mobile Remote Access) or the built-in Cisco AnyConnect® VPN for the secure connection of their remote workers. Expressway offers a simple configuration process and allows for transparent connectivity without the requirement of any special equipment such as a Cisco Virtual Office. It helps make collaboration as simple and effective at home as it is inside the office.

- Media and signaling encryption enforced between DX and Expressway-C (UCM mixed mode not required). End-to-end signaling and media encryption is supported with mixed-mode UCM.
- TLS provides encryption for privacy and integrity protection.
- Client authentication mechanism includes basic web authentication and SIP digest authentication.
- Jabber® IM&P (XMPP over TLS) is supported using Expressway MRA functions.

Third-Party Security Applications (MDM and Antivirus)

- Standard third-party MDM, antivirus, and antimalware applications can be installed.

Data Protection and Encryption

Secure VoIP Services

- Media encryption: SRTP can be enabled to help ensure that media streams between supported devices provide integrity, authenticity, and privacy protection for the intended devices.
- Signaling encryption: TLS can be enabled to help ensure that all SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
- Signaling authentication: The mutual authenticated TLS protocol can be enabled to validate that no tampering to signaling packets has occurred during transmission and help ensure the signaling is between trusted sources.

Secure Remote Access Feature

- Cisco AnyConnect Secure Mobility Client: The Cisco AnyConnect VPN software is integrated (bundled) with the operating system and requires no separate download.
  - The client has an administrator-controlled VPN policy.
  - VPN can be used over wired or wireless.
  - VPN can be configured to be “always on”.
  - VPN can encrypt existing SRTP and TLS packets.

Secure Storage

- The Cisco DX Series endpoints encrypt internal flash memory to protect data at rest.

Security Enclavement (ARM TrustZone Technology)

- The DX Series uses ARM TrustZone technology for handling cryptographic operation of platform key materials.
- DX symmetric encryption keys are protected by TrustZone, and the key material never leaves the TrustZone.
- Only cryptographic operations (encryption and decryption) using keys can be performed.

Cryptography

Hardware-Based True Random Number Generator

- The Cisco DX Series uses the hardware-based True Random Number Generator (TRNG) for providing entropy to a pseudo random number generator (PRNG), helping ensure quality of entropy (or seeding material) for all cryptographic protocols and key materials.

RSA, AES, and SHA Family

The Cisco DX Series supports approved advanced cryptographic algorithms:

- RSA signature verification and private key decryption
- Support for up to 2048-bit RSA key sizes
- Advanced Encryption Standard (AES) 128- and 256-bit Cipher Block Chaining (CBC) and Counter (CTR) block cipher modes
- SHA-1 and SHA-256 algorithms

Federal Information Processing Standard 140-2 Validated Cryptographic Module

The Cisco DX Series uses the Cisco SSL Federal Information Processing Standard (FIPS) 140-2 validated cryptographic module.

Network Security

802.1x WLAN

- 802.1x wireless provides authentication:
  - 802.1x Extensible Authentication Protocol (EAP)
  - Wi-Fi Protected Access 2 (WPA2)
- 802.1x wireless provides encryption for:
  - AES
- 802.1x wireless EAP types:
  - Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-TLS
  - Protected Extensible Authentication Protocol (PEAP) Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) and Generic Token Card (GTC) with optional server validation
- Wireless LAN (WLAN) profiles with Cisco Unified Communications Manager 10.0
  - The administrator can push up to four different profiles through a WLAN Profile Group to the DX Series endpoint. The administrator can lock down the Service Set Identifier (SSID); frequency band; and credentials, passwords, and keys so that the end user cannot change these settings.

802.1x Wired Interface

- Standard 802.1x supplicant options can be enabled for network authentication:
  - EAP-FAST
  - EAP-TLS

Client Certificates

- MIC is supported
- LSC is supported
  - LSC can be issued to support customer-specific identity instead of Cisco’s manufacturing installed certificate.
- For VPN, LSC allows for multifactor authentication (Certificate + Password).
- X.509 digital certificates in Distinguished Encoding Rules (DER) for Base-64 formats that use a 1024-, 2048-, or 4096-bit key and SHA-1 or SHA-2 signatures are supported for WLAN authentication through EAP-TLS. PKCS #12 format is used.

Application Security

Application Download Control

- The administrator can disable any and all applications from being downloaded on the Cisco DX Series endpoint. Specifically, the administrator can configure the DX endpoint to prohibit the installation of any third-party Android applications.
  - Google Play access can be administratively disabled (default). Applications from “unknown sources” can be administratively disabled (default):
    - The administrator can optionally install applications using Cisco Unified Communications Manager with the APK file.

Exchange ActiveSync

- The Cisco DX Series supports the policies from Exchange ActiveSync:
  - Remote wipe
  - Force password or personal identification number (PIN) lock

Cisco Unified Communications Manager Administration Control Policies

Device Control

- Enable/disable simple mode
- Enable/disable Wi-Fi
- Enable always-on VPN
- Lock administrator-controlled wallpaper
- Enable/disable built-in web server (for supportability and diagnostics)
- Enable/disable PC voice VLAN access

Peripheral Control

- Enable/disable Bluetooth
- Enable/disable USB port
- Enable/disable secure digital card
- Enable/disable PC port

Password and PIN Lock Enforcement

- Force PIN and password
- Remotely lock device
- Enforce screen lock during display-on-time
- Wipe after unsuccessful login attempts

Remote Wipe

- Administrators can initiate remote wipe from Cisco Unified Communications Manager.
- When a remote wipe is performed on a phone, the operation resets the phone to its factory settings. Everything previously stored on the phone is wiped out.

User Settings: Overview

IT administrator has the flexibility to select user settings depending on the user profile.

- Enhanced mode: Opens the capabilities of the device with full access to Android (e.g., apps from play store).
- Simple mode: The user interface is limited to only telephony, voicemail, contact, and basic settings.
  - Users cannot move, add shortcuts or widgets, launch applications, or long click.
  - No additional Android applications can be installed.
  - External USB storage is disabled.
- All other aspects of the Android are removed from the user interface. The user cannot modify the wallpaper (supports administrator-assigned wallpaper).

Summary

The Cisco DX Series endpoint can be secured by the administrator using the methods and techniques outlined previously. Table 1 summarizes key features.

Table 1. Security Features of Cisco DX Series

Feature	Description
Image authentication	Signed binary files prevent tampering with the firmware image before the image is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each Cisco DX Series requires a unique certificate for device authentication. Cisco DX Series devices include a MIC, but for additional security you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a LSC from the enterprise security menu on the device. Please visit: Cisco Desktop Collaboration Experience phone security for more information.
Device authentication	Authentication occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. It determines whether a secure connection between the device and a Cisco Unified Communications Manager should occur; if necessary, it creates a secure signaling path between the entities by using the TLS protocol. Cisco Unified Communications Manager does not register phones unless it can authenticate them.
File authentication	Authentication validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to flash memory on the phone. The phone rejects such files without further processing.
File encryption	Encryption prevents sensitive information from being revealed while the file is in transit to the phone. In addition, the phone validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to flash memory on the phone. The phone rejects such files without further processing.
Signaling authentication	Authentication uses the TLS protocol to validate that no tampering to signaling packets has occurred during transmission.
Manufacturing installed certificate	Each Cisco DX Series contains a unique MIC, which is used for device authentication. The MIC provides permanent unique proof of identity for the phone and allows Cisco Unified Communications Manager to authenticate the phone.
Media encryption	Encryption uses SRTP to help ensure that media streams between supported devices prove secure and that only the intended device receives and reads the data.
Security profile	This profile defines whether the phone is nonsecure, authenticated, encrypted, or protected. Other entries in this table describe security features. For more information about these features, about Cisco Unified Communications Manager, and about Cisco DX Series phone security, refer to the **Cisco Unified Communications Manager Security Guide**.
Optional web server disabling for a phone	For security purposes, you can prevent access to the webpages for a phone (which display a variety of operational statistics for the phone) and User Options webpages. For more information, please visit: Manage the User Options web pages.

Feature	Description
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration, follow: • Disable PC port • Disable Gratuitous ARP (GARP) • Disable PC voice VLAN access • Disable built-in web server (default) • Disable Bluetooth accessory port • Disable web server for a phone (optional) • Require a screen lock • Control access to Google Play • Control access to installation of applications from unknown sources
802.1X authentication	The Cisco DX Series can use 802.1X authentication to request and gain access to the network. Please visit 802.1X authentication support for more information.
Secure SIP failover for Survivable Remote Site Telephony (SRST)	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the Trivial File Transfer Protocol (TFTP) server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Signaling encryption	This encryption helps ensure that all SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.

Printed in USA C11-731685-03 05/15