White paper
Cisco public

Cisco IP Phone 7800 and 8800 Series Security Overview

Contents

System security
- Signed firmware images
- Secure boot
- Secure provisioning

Cryptography
- Identity certificates
- Cryptographic algorithms
- Ciphers
- Federal Information Processing Standard 140-2 validated cryptographic module

Data protection and encryption
- Secure VoIP services (mixed-mode Cisco Unified Communication Manager clusters only)
- Protocol encryption
- Secure Extension Mobility

Remote connectivity
- Expressway Mobile and Remote Access
- Phone VPN

Network security
- Wired 802.1x
- Wireless (WLAN) 802.1X

Cisco Unified Communications Manager administration control policies
- Device control
- Peripheral control

Summary

Cisco IP Phone 7800 and 8800 Series security overview

With security becoming increasingly important in every aspect of the enterprise, this white paper documents the state of the art security improvements that Cisco has included in its latest phone models. For example, Cisco® has updated the IP phones to use the Secure Hash Algorithm (SHA-256) hashing algorithm, since SHA-1 is being universally deprecated. The SHA-2 family provides stronger cryptographic hash properties than SHA-1 and is less susceptible to forged digital signatures. You may have read about SHA-1 collisions recently in the news, and the associated threat of applying massive compute resources to forge documents that include an identical SHA-1 digital signature. This is an emerging threat that will become more pervasive with time, and applies to any file type that is signed with SHA-1 algorithm. Consequently, it is important to understand the support for modern cryptographic hash functions and encryption ciphers for any product that provides secure communications. This white paper allows you to compare and contrast the security features and support across both older and Cisco's latest phone models.

The latest generation of Cisco IP phone models are the Cisco IP Phone 7800 and 8800 Series. The 7800 and 8800 Series include many enhanced security options. This white paper also includes the 7900, 6900, 8900, 9900 Series so you can easily compare the security features in the latest generation versus the older generation.

System security

The Cisco IP Phone 7800 and 8800 Series include system security features detailed below that guarantee only authentic Cisco firmware runs on the phone.

Signed firmware images

- The 7800 and 8800 Series can load only firmware images digitally signed by Cisco.
- The digital signature of the firmware is verified before the firmware can be active.
- Firmware is signed with a 2048-bit RSA key.

Secure boot

- Cisco IP Phone hardware ensures only authentic Cisco firmware can run.
- The first code that executes on boot is immutable.
- Execution of the boot sequence is always authenticated by a previously trusted step.
- Secure boot chain starts from the bootloader and the installed firmware validates the digital signature.
- Secure boot is always enabled, and there is no provision to bypass or disable.

Table 1 compares the image signing and secure boot features of the Cisco IP phone models.

Table 1. Image signing and secure boot

	Phone Models			
Feature	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
Imaging Signing	Yes	Yes	Yes	Yes
Secure Boot	No	Yes	No	Yes

Secure provisioning

- Configuration files are digitally signed to guarantee authenticity and integrity.
- The configuration file can also be encrypted (AES 128 bit) to provide configuration data privacy.
- Encrypted configuration files are administratively enabled via the device security profile.
- An encrypted configuration file can only be decrypted by the IP Phone that it was intended for and requires a private key that corresponds with the phone's public key stored in Cisco Unified Communications Manager.
- Secure provisioning is supported in both non-secure and mixed-mode Cisco Unified Communication Manager clusters.

Table 2 lists the configuration file signature algorithms for the Cisco IP phone models.

Table 2. Configuration file signature algorithms

	Phone Models			
Algorithm	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
SHA-1	Yes	Yes	Yes	Yes
SHA-512	No	No	Yes	Yes

Cryptography

Identity certificates

- Cisco IP Phones utilize X.509v3 certificates for device authentication in a number of security contexts.
- Each 7800 and 8800 Series phone contains a unique Manufacturing Installed Certificate (MIC).
- The MIC provides a factory-installed unique identity.
- Cisco IP Phones also support a Local Significant Certificate (LSC) that bind the phones to a customer's environment.
- An installed LSC takes precedence over the phone's MIC certificate.
- User installed certificates is a third certificate type that is only included with phones that support wireless LAN.
- User installed certificates are used specifically for wireless EAP-TLS.
- The user installed certificate is installed manually via the phone web interface or automatically using Simple Certificate Enrollment Protocol SCEP.
- Wireless EAP-TLS supports using a phone's MIC or a user installed certificate, but LSC certificates are not supported.

Table 3 lists the supported key sizes, and Table 4 lists the supported hash algorithms for the Cisco IP phone models.

Table 3. Maximum supported key sizes for identity certificates

	Phone Models			
Certificate Type	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
MIC	2048	2048	2048	2048
LSC	2048	2048	4096	4096

Table 4. Supported hash algorithms for identity certificates

	Phone Models			
Certificate Type	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
MIC	SHA-1	SHA-1	SHA-1, SHA-256*	SHA-256
LSC	SHA-1	SHA-1	SHA-1, SHA-256, SHA-384, SHA-512	SHA-1, SHA-256, SHA-384, SHA-512

* The 7800 Series MIC may vary based upon the hardware revision.

Cryptographic algorithms

The Cisco IP Phone 7800 and 8800 Series supports the following cryptographic algorithms:

- RSA signature verification, encryption and decryption.
- Support for up to 4096-bit RSA key sizes.
- Advanced Encryption Standard (AES)-128- and 256-bit Cipher Block Chaining (CBC), Counter (CTR), and Galois/Counter Mode (GCM) block cipher modes.
- SHA-1 and SHA-256 algorithms.

Ciphers

- AES 256 Encryption Support has been extended to both signaling and media encryption.
- Cisco IP Phones 7800 and 8800 Series can initiate SIP Transport Layer Security [TLS] 1.2 signaling connections with the AES-256 based TLS ciphers.
- Phones will attempt to negotiate Secure Real-Time Transport Protocol (SRTP) with AES-256 bit SRTP ciphers when establishing a session with another encrypted device.
- Requires firmware 10.3(1) firmware and Cisco Unified Communications Manager 10.5(2) or later.

Table 5 lists the ciphers supported by the Cisco IP phones.

Table 5 TLS cipher support

	Phone Models			
Ciphers	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLS)	No	No	Yes	Yes
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (TLS)	No	No	Yes	Yes
TLS_RSA_WITH_AES_128_CBC_SHA (TLS)	Yes	Yes	Yes	Yes
AES_CM_128_HMAC_SHA1_32 (SRTP)	Yes	Yes	Yes	Yes
AES_CM_128_HMAC_SHA1_80 (SRTP)	Yes	Yes	Yes	Yes
AEAD_AES_256_GCM (SRTP)	No	No	Yes	Yes
AEAD_AES_128_GCM (SRTP)	No	No	Yes	Yes

Federal Information Processing Standard 140-2 validated cryptographic module

The 7800 and 8800 Series phones use the Cisco SSL Federal Information Processing Standard (FIPS) 140-2 Level 1 validated cryptographic module.

Data protection and encryption

Secure VoIP services (mixed-mode Cisco Unified Communication Manager clusters only)

- TLS is used to authenticate and encrypt all SIP signaling messages sent between the phone and the Cisco Unified Communications Manager when a phone is provisioned with an encrypted security profile.
- TLS is also used with phones provisioned with an authenticated security profile to simply authenticate and not encrypt SIP signaling messages.
- SIP TLS communication with Cisco Unified Communications Manager is always mutually authenticated, and prevents tampering to ensure the signaling is between trusted sources.
- Media encryption is only negotiated when signaling is established over encrypted TLS sessions.
- When media encryption is negotiated between encrypted devices a padlock icon is used to notify the end user that the call is encrypted.
- Encrypted SRTP media streams provides integrity, authenticity, and confidentiality.

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

	Phone Models			
Version	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes

Protocol encryption

- SIP Signaling and IP phone services are encrypted with TLS.
- Phone VPN communication is encrypted with DTLS.
- TLS encryption can be enabled for the phone's local webserver (HTTPS).

Secure Extension Mobility

The Secure Extension Mobility HTTPS feature helps ensure that, when communications are exchanged between a Cisco IP phone service and other applications, the communications use the HTTPS protocol to ensure that they are secure. Users must log in to the Cisco Unified Communications Manager applications by providing their authentication information. Their credentials are encrypted after the communication protocol changes to HTTPS.

Table 7 lists the Cisco IP phones' support for Secure Extension Mobility.

Table 7. Secure extension mobility and Extension Mobility Cross Cluster (EMCC)

	Phone Models			
Version	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
Secure EM using TLS 1.0	Yes	Yes	Yes	Yes
Secure EM using TLS 1.2	No	No	Yes	Yes

Remote connectivity

Expressway Mobile and Remote Access

Cisco Expressway™ Mobile & Remote Access (MRA) provides VPN-less access from an external network to UC services deployed within a private network. Cisco Expressway provides firewall and NAT traversal for remote endpoints registered to Cisco Unified Communication Manager.

- Encrypted signaling and media between a remote endpoint and Expressway-C without Cisco Unified Communications Manager mixed-mode.
- Cisco Unified Communications Manager mixed-mode is required for encrypted signaling between a remote endpoint and Cisco Unified Communications Manager, and for encrypted media between a remote endpoint and on-premises endpoint, gateway, or conference bridge.
- TLS encryption provides privacy and integrity protection for SIP signaling, visual voicemail access, directory lookup and configuration file download.
- Secure SRTP.

Phone VPN

The Phone VPN feature is an alternative remote access option that is available on some Cisco IP Phones. A Cisco ASA is typically deployed as the VPN head-end for phones and other types of VPN clients. The Phone VPN feature requires phones to be staged on a network with direct access to Cisco Unified Communications Manager before they are shipped to a remote worker or remote site.

- Phone VPN feature has an administrator-controlled VPN policy.
- VPN can be configured to be "always on."
- VPN can be used over wired or wireless LAN connection.
- VPN can tunnel SRTP and SIP TLS packets, providing multiple layers of encryption up to the VPN head-end.

Table 8 lists the Cisco IP phones' remote connectivity support, and Table 9 lists the client authentication options.

Table 8. Remote connectivity support

	Phone Models			
Type of Access	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8841, 8845, 8851, 8861, 8865**
Expressway MRA	No	No	Yes	Yes
Phone VPN	Yes	Yes	No	Yes

Table 9. Client authentication options

Type of Access	PIN	Username/Password	Certificate
Expressway MRA	–	Yes	–
Phone VPN	Yes	Yes	Yes

Network security

Wired 802.1x

- Standard 802.1X supplicant options can be enabled for network authentication:
  - Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-TLS (Transport Layer Security)
- EAP-FAST (and EAP-MD5) leverage username and password for client authentication and network access.
- EAP-TLS requires a client certificate for authentication and network access.
- For wired EAP-TLS, the client certificate can be either the phone's MIC or an LSC.
- LSC is the recommended client authentication certificate for wired EAP-TLS.

Table 10 lists the network authentication protocols supported by the Cisco IP phones.

Table 10. Network authentication protocols supported

	Phone Models			
802.1X (Wired)	**7900**	**6900, 8900, 9900**	**7811, 7821, 7841, 7861**	**8811, 8821, 8841, 8845, 8851, 8861, 8865**
EAP-MD5	Yes	Yes	No (deprecated)	No (deprecated)
EAP-FAST	Yes	Yes	Yes	Yes
EAP-TLS	Yes	Yes	Yes	Yes

Wireless (WLAN) 802.1X

- 802.1X wireless provides AES encryption.
- 802.1X wireless authentication support includes:
  - 802.1x (EAP)
  - Wi-Fi Protected Access 2 (WPA2)
- 802.1X wireless supported EAP are as follows:
  - EAP-FAST
  - Protected EAP (PEAP) Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) and Generic Token Card (GTC) with optional server validation
  - EAP-TLS
- EAP-FAST and PEAP leverage username and password for client authentication and wireless network access.
- EAP-TLS requires a client certificate for authentication and network access.
- For wireless EAP-TLS the client certificate can be either the phone's MIC or a user installed certificate issued by the enterprise certificate authority (CA) or a public CA.
- The user installed certificate is installed manually via the phone web interface or automatically using Simple Client Enrollment Protocol (SCEP).
- Wireless LAN (WLAN) profiles with Cisco Unified Communications Manager 10.5.2 or higher include the ability for an administrator to provision the following wireless settings so that the end user cannot alter these settings:
  - Service Set Identifier (SSID)
  - frequency band
  - credentials
  - passwords
  - keys
- The 8821 supports up to four different profiles through a WLAN Profile Group.
- The 8861 and 8865 support one profile through a WLAN Profile Group.

Table 11 indicates the WLAN profile capabilities of the Cisco IP phones.

Table 11. Cisco Unified Communications Manager provisioning

	Phone Models	
Cisco Unified Communications Manager Provisioning	**Cisco Unified Wireless IP Phone 792x Models**	**8821, 8861, 8865**
Wireless LAN profile for provisioning security authentication: EAP-TLS,* EAP-FAST, PEAP-MS-CHAPv2, WPA, WPA2, PEAP-GTC, WEP	No	Yes
Ability to provision wireless LAN profile over the wired network	No	Yes (the 8821 requires the desktop charger for wired Ethernet provisioning)

* EAP-TLS provisioning via Cisco Unified Communications Manager WLAN profile requires Cisco Unified Communications Manager 11.0 or later.

Cisco Unified Communications Manager administration control policies

Device control

- Enable/disable Wi-Fi (8861, 8865).
- Enable always-on VPN (8811, 8841, 8845, 8851, 8861, 8865).
- Lock administrator-controlled 800x480 wallpaper (8811, 8841, 8845, 8851, 8861, 8865).
- Enable/disable built-in web server (for supportability and diagnostics); it is disabled by default.
- Enable/disable PC voice VLAN access.

Peripheral control

- Enable/disable USB port (8851, 8861, 8865):
  - The USB port is restricted to audio devices and charging of smartphones
  - USB audio devices and smartphone device charging are enabled by default
  - USB can be disabled via Cisco Unified Communications Manager on the phone device page
- Enable/disable Bluetooth (8845, 8851, 8861).
- Enable/disable PC port.

Summary

The Cisco IP Phone 7800 and 8800 Series provides modern security out of the box and can be administratively hardened and secured using the options outlined above.

C11-739097-01 07/18