Cisco Desk Phone 9800 Series Security

Security Technical Paper

June 2024

webex by CISCO

Contents

Cisco Desk Phone 9800 Series running PhoneOS provides state-of-the-art security features. This technical paper covers important security features of the Desk Phone 9800 Series.

This technical paper documents the security improvements that Cisco has included in the Desk Phone 9800 Series. The Desk Phone 9800 Series and the Cisco Video Phone 8875 run PhoneOS. This operating system can register to either Unified Communications Manager (Unified CM) or designated cloud calling platforms, such as Webex Calling, after just a simple factory reset. Unlike the 7800 and 8800 series running Enterprise Firmware, with PhoneOS it is no longer required to migrate firmware when moving between environments. Moreover, the additional hardware security improvement of a Trusted Platform Module (TPM) has been added to the Desk Phone 9800 Series making the 9800 Series the first desk phone in the industry to include a TPM 2.0 hardware module.

1. Best End to End Security

The security framework of the Cisco Desk Phone 9800 Series provides state-of-the-art security features. As shown in Figure 1, the following security pillars cover important security features in PhoneOS firmware and Desk Phone 9800 Series hardware:

- Hardware-enabled security
  - Trusted Platform Module (TPM)
  - Hardware-Enforced Audio Path Control (Hardware Mute)
  - Hardware authenticity check
  - Chip protection (Chip Guard)
  - Image Signing
  - Secure boot
- Runtime protection
  - Runtime defenses
  - Security Enhanced Linux
- Application Security
  - Secure Infrastructure: PKI certificate management.
  - TLS 1.3
  - Secure user data at Rest and in Use

  - End to End Encryption of User Data
  - Secure on-boarding
  - Secure Call
  - Anti-Spam support to protect the end user
  - Privacy for Personally Identifiable Information (PII) with Webex Calling.
- Industry Compliance
  - Security Compliance: FedRAMP* and FIPS.
- Cisco CSDL, PSIRT & Product Security Baseline.

* Coming soon.

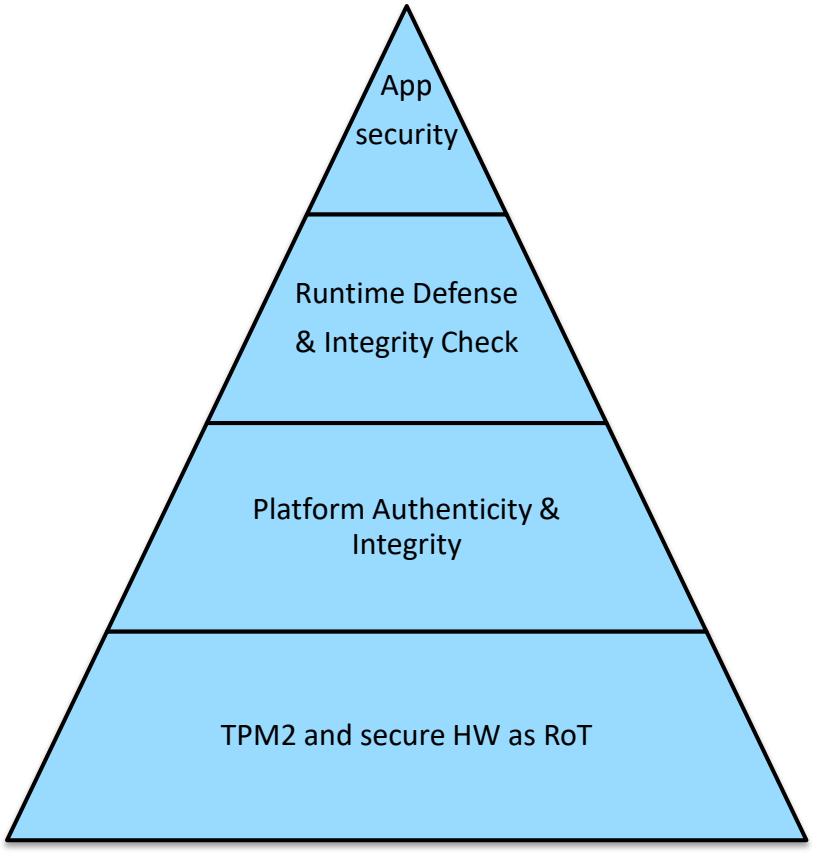

Figure 1. PhoneOS Security Architecture with Desk Phone 9800 Series

2. Hardware-Enabled Security

As you can see in Figure 1 above, Cisco has designed a layered approach to security. Each of these layers work together, both in hardware and in software, to maintain the integrity of the system.

TPM2 and Secure SoC provides hardware Root-of-Trust to build a solid security foundation for PhoneOS with the Desk Phone 9800 Series to circumvent security threats throughout device lifecycle.

3. Trusted Platform Module 2.0

- The TPM 2.0 module included in 9800 hardware is a discrete hardware module designed to provide security-related functions such as cryptography. The module is compliant with Industry Standard (TCG-TPM2.0).
- The TPM mitigates threats such as:
    - Hardware tampering. The act of replacing a hardware chip to by-pass PhoneOS secure boot.
    - Hardware spoofing (Hardware cloning). The act of spoofing the identity of the phone to gain access to the corporate network or cloud calling service.
    - Counterfeit hardware. The act of creating fake hardware to create a backdoor for data theft.
    - Compromising of data. The theft of sensitive user data or credentials.
    - Unsecure communication. Data compromise due to weak ciphers that can be exploited to decrypt traffic.
- Hardware authenticity check
    - A process using the X.509 Secure Unique Device Identifier (SUDI) certificate installed in the TPM to verify that the Cisco hardware is authentic. The hardware authenticity check runs only after the secure boot process is complete and the software verified to be trusted.
    - PhoneOS retrieves the SUDI certificate from the TPM as cryptographic proof the certificate belongs to the platform.
- Chip protection (Chip Guard)
    - Mitigates the supply chain threat of CPU replacement containing malware or similar types of attacks. The Chip Guard mitigates this threat using the TPM 2.0 hardware module.
- Secure Communication
    - PhoneOS supports TLS 1.3, SUDI certificates, and User Installed certifies (LSC) protected by the TPM hardware, and SIP OAuth.

Note: The 8875 runs PhoneOS and does not contain a TPM 2.0 hardware module. The 8875 will support TLS 1.3.

4. Hardware-Enforced Audio Path Control

Hardware-enforced audio path control is also known as Hardware mute. Cisco phone hardware is designed so that the hardware itself physically controls the state of the microphone. This means that the microphone's electrical circuit is directly tied to a hardware switch (hook-switch) or indicator (LED) that cannot be overridden by software. Detailed behavior is as follows.

Handset microphone Cut-Off Mechanism: When the handset hook-switch is in the depressed state (indicating the handset is on the hook), the hardware disconnects or disables the microphone circuit at the hardware level. There is no software interaction that can close the circuit to activate the microphone, ensuring that the microphone cannot be turned on remotely by software means when the handset is not in use.

Speaker LED Status Indicator: The LED on speaker key functions as a reliable indicator of the microphone status. When the LED is illuminated, it signals that the handsfree microphone circuit is active and can capture audio. Conversely, when the LED is off, the hardware ensures that the microphone is inactive. Software cannot activate the microphone without simultaneously triggering the LED to turn on, providing a visual cue to the user.

With these hardware controls, the device guarantees that any activation of the internal microphone, while the handset is on the hook, will be accompanied by the illumination of the speaker LED. This design prevents covert activation of the microphone by compromised software, as the user will have a clear, unmistakable hardware indication (the lit LED) whenever the microphone is live.

These measures leverage physical design elements to create a "hardware root of trust," ensuring that certain critical functions are strictly controlled by the hardware and are beyond the reach of potentially compromised software. This approach provides a strong security assurance to users about the privacy of their conversations and the integrity of the device's audio input mechanisms.

5. Secure Unique Device Identification (SUDI)

During manufacturing, device identification is programmed into Cisco Trust Anchor Module (backed by TPM2 module) using a Secure Unique Device Identification (SUDI), an X.509 certificate that is globally unique per device. SUDI is an extension of device identity as defined by the IEEE 802.1 working group. The 802.1 AR standard defines a secure device identifier as a cryptographic identity that is bound to a device and used to assert device identity. SUDI is permanently programmed into the Trust Anchor module and logged by Cisco manufacturing and is used for device authentication purposes. Cisco has a secure business-to-business network with its silicon, software, and manufacturing partners to exchange critical system information such as SUDI between suppliers and the Cisco back-end process.

With the SUDI, each Cisco desk phone device has a unique and secure identifier that is used to authenticate the device throughout its lifecycle, from manufacturing to end-of-life. The SUDI protected by TPM module, provides a robust defense against counterfeit devices and unauthorized access, enhancing overall device security in the supply chain and operational environments.

6. Secure Boot and Hardware Authenticity Check

Secure Boot is deeply integrated with the System on Chip (SoC) hardware, ensuring that only verified, untainted code is permitted to execute on the Cisco Desk phone during startup. With the establishment of root of trust, secure boot monitors all stages of the boot process. At boot time the secure boot process authenticates a micro-loader, bootloader, and the bootloader authenticates the operating system. This process creates a chain of trust from the micro-loader to the operating system, which establishes the software authenticity and integrity. All of these signatures are cryptographically verified using RSA signature. If any of the digital signature checks fail, the Cisco device will not allow the software to boot.

Once the Secure Boot sequence is completed, with the software deemed trustworthy, PhoneOS software retrieve the Secure UDI (SUDI) certificate from the TPM and challenge the chip to provide cryptographic proof that the SUDI certificate belongs to the underlying platform. This challenge process is referred to as the hardware authenticity check or anti-counterfeit check. With this capability, PhoneOS software can determine whether it is running on genuine Cisco 9800 phone hardware.

Through this comprehensive verification, the authenticity of both the hardware and software is assured at the time of booting, safeguarding against the risks of hardware and software counterfeiting.

7. Chip Protection

Supply chain attacks can involve substituting original System on Chip (SoC) components with compromised versions that contain trojans or malicious code. Cisco Chip Protection helps mitigate this threat with the use of unique identifiers stored inside the Trust Anchor module (backed by TPM2 module) as a way to identify and track components through the product lifecycle.

The Trust Anchor module houses an imprint database—a definitive catalog that records the unique identifiers of SoC chips and other device types specific to a circuit board. These identifiers are typically the device serial numbers or similar unique values. The imprint database, which contains 'known good' values, is exclusive to the board in which it resides and serves as a reference for the authentication process to confirm component authenticity. These identifiers are embedded into the Trust Anchor module during manufacturing, in a process akin to that used for SUDI and secure boot procedures.

Every time Desk phone hardware powers up, the firmware collects and compares the current component identifiers to those stored in the imprint database within the Trust Anchor module. A discrepancy between the observed identifiers and the imprint database signifies a potential security breach and triggers a report to the host system for further investigation and response.

8. Runtime Defenses

Runtime defenses are designed to safeguard the PhoneOS software from the insertion of harmful code while it is operational, thereby significantly challenging attackers' efforts to leverage known weaknesses in software and hardware setups. Cisco's suite of runtime protections encompasses techniques such as Address Space Layout Randomization (ASLR), which randomizes memory locations for system and application files, making it harder for attackers to predictably exploit memory-based vulnerabilities. Built-in Object Size Checking (BOSC) is another defense mechanism that ensures the integrity of memory buffers by checking object sizes, which helps prevent buffer overflow attacks. Additionally, X-space Runtime defenses serve as an additional layer of security, working in conjunction with the other measures to fortify the system against unauthorized code execution and other runtime threats. Together, these defenses form a robust barrier against runtime exploits.

9. Mandatory Access Control – SE Linux

PhoneOS incorporates the Security-Enhanced Linux (SELinux) framework to apply mandatory access control (MAC) across every process within the system.

Operating on a least-privilege basis, SELinux ensures that all operations are blocked by default unless explicitly authorized. This minimizes the risk of damage if a process is compromised because the process can only access resources that are absolutely necessary for its function.

As a result, PhoneOS is able to bolster its defenses, providing a more secure environment that effectively protects and confines network and system services, isolate potentially compromised applications and protect from potential security vulnerabilities.

10. Secure User Data at Rest and in Use

User sensitive data, such as SIP proxy passwords and access tokens, is safeguarded through encryption and housed within a secure data repository that utilizes the Cisco Trust Anchor module (backed by TPM2 module). This module is engineered to provide a highly secure enclave for the preservation of encryption keys, passwords, user credentials, and other vital security data pertinent to the device.

Upon conducting a factory reset of the device, all user-sensitive data is subject to cryptographic erase, effectively making any previously stored data inaccessible.

For real time data such as audio and video information for an active video call, they are stored in volatile Memory. The encryption keys are removed between calls and all data is wiped when the system is restarted.

Locally stored user data on the device are encrypted using AES (Advanced Encryption Standard) with a 256-bit key for secure storage.

11. End-to-End Encryption of User Data

Cisco Desk phone can request end-to-end encryption keys to access the data created by users of Webex services. Cisco Desk phones participate in end-to-end encryption for the following services:

- Webex calendaring and One Button to Push (OBTP) meeting join functionality.
- More services will be added over time.

Like Webex apps, Cisco desk phone can request end-to-end encryption keys from the Webex Key Management Service and use these keys to encrypt and decrypt content. End-to-end encryption keys, OAuth access tokens, and content for calendar events are not persistently stored in PhoneOS. OAuth Refresh Tokens are securely stored by PhoneOS and are renewed when access tokens are renewed.

For more information on how end-to-end encryption works for Webex calendaring services see: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf.

12. Stateful Firewall

With PhoneOS firmware, Cisco has improved phone security by hardening the operating system with a stateful firewall. The firewall protects the phone from malicious incoming traffic. The firewall tracks the ports for incoming and outgoing data. It detects incoming traffic from unexpected sources and blocks access. The 9800 Series and the 8875 support the stateful firewall. Note: Stateful Firewall is not operational when registered to Unified CM.

13. DoS Protection

PhoneOS provides built-in DoS (Denial of Service) protection, ensuring that PhoneOS remains resilient against the disruption attempts of DoS attacks. It includes two specific mechanisms as below.

- Traffic Storm Control: Protects against broadcast storm attacks.

- Rate limiting: It limits the number of incoming unicast packets within a certain time frame, preventing overloading by excessive traffic.

Note: The Desk Phone 9800 Series and the 8875 both have DoS Protection. DOS Protection is operational when registered to either Unified CM or Webex Calling.

14. Secure Onboarding to Webex Cloud Services

Cisco Webex Control Hub provides a simple interface to onboard and activate Cisco Desk phone. Device onboarding can be done easily using a 16-digit activation code generated in Webex Control Hub. Once the devices are onboarded, an administrator has visibility into the details and states of those devices. An administrator is also able to update selected configuration settings from Webex Control Hub.

At the beginning of the onboarding process the device establishes a TLS connection with the Webex Global Discovery service (certificate trust anchors for the TLS connection are installed on the device during manufacture) and send the service its activation code. The 16-digit activation code identifies the organization that the device belongs as well as the machine account for the device. The organizational information in the code is used by the Webex discovery service to redirect the device to the Webex calling or identity service.

The Desk Phone 9800 Series device establishes an encrypted TLS connection to the Webex calling or identity service. To provide an extra layer of security against TLS interception attacks, the device uses Secure Remote Password protocol (SRP) to create an additional encrypted connection to the identity service and then, uses this tunnel to download the OAuth tokens and additional Certificate trust anchors that the device needs to register to and use Webex services.

Secure Remote Password protocol (SRP) is an augmented password-authenticated key agreement (PAKE) protocol (https://tools.ietf.org/html/rfc2945). The device's activation code is used to authenticate the device with the identity service and also to establish a password-entangled SRP session key between the device and the identity service. A key derivation function (KDF) uses the session key as input to create a symmetric AES encryption key that is used to encrypt data exchanged between the device and identity service.

15. Secure Call

As shown in Figure 2, with Webex Calling, SIP call control signaling between SIP endpoints and the service are encrypted using Transport Layer Security (TLS) and strong cipher suites.

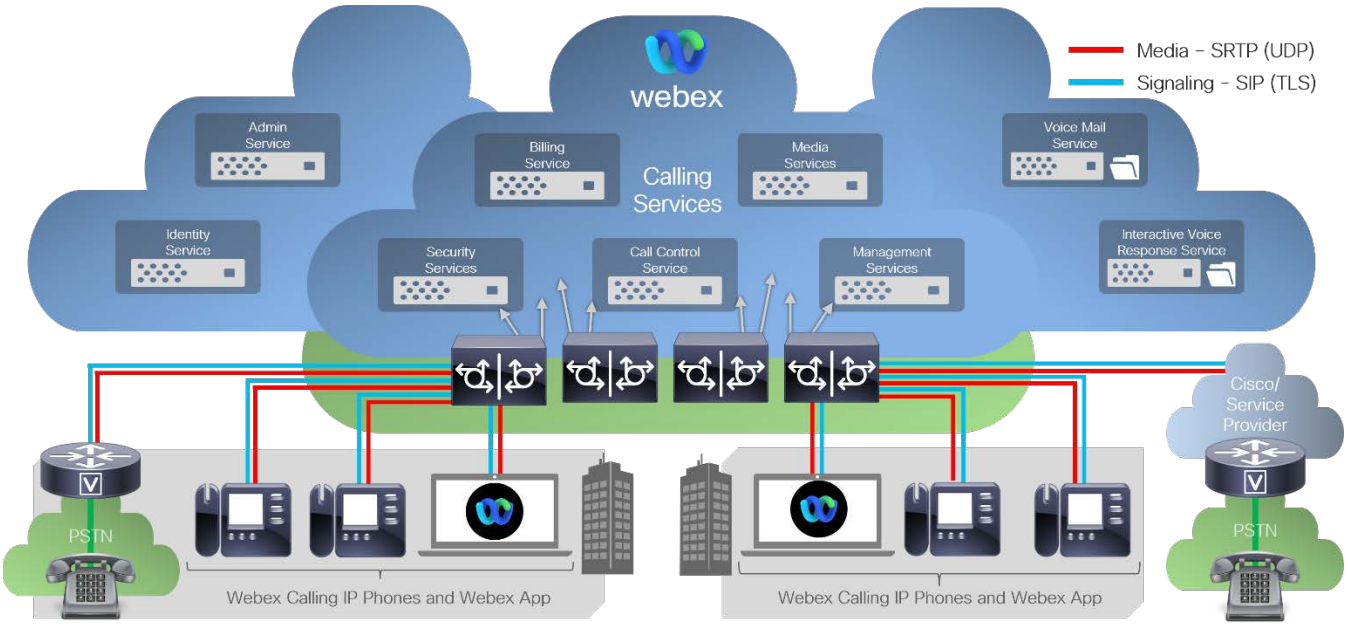

Figure 2. Webex Calling: SIP TLS Signaling and SRTP UDP Media

During onboarding, connections from the 9800 Series are outbound only and use fully qualified domain names to establish sessions to Webex Calling services. Signaling traffic is protected by TLS using strong encryption suites and Webex services only support TLS versions 1.2 and 1.3. The cipher selection for each connection is based on the Webex server's TLS preference.

Webex services prefer the following:

- ECDHE for key negotiation
- RSA-based certificates (2048-bit or higher key size)
- SHA2 authentication (SHA384 or SHA256)
- Strong encryption ciphers using 128 or 256 bits (for example, AES_256_GCM and AES_128_GCM)

  Example:
  TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

These cipher suites meet the guidelines defined in the US National Institute of Standards and Technology (NIST) Special Publication 800-52 Revision 2. For more information, see Guidelines for the Selection, Configuration, and Use of Transport 4 Layer Security (TLS) Implementations.

Media streams between SIP endpoints and the service are secured using the Secure Real-Time Transport Protocol (SRTP), as described in RFC 3711.

16. Anti-Spam (Webex Calling)

Cisco has improved phone security by providing Anti-Spam support.

Cisco supports the new technology standard Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted information using tokens (SHAKEN) for the Webex call logs, local call logs, and local call sessions when the phone is in Webex environment. STIR/SHAKEN has been mandated by Federal Communications Commission (FCC). These standards define procedures to authenticate and verify caller identification for calls carried over the IP network. The STIR-SHAKEN framework is developed to provide the end

user with a great degree of identification and control over the type of calls they receive. These sets of standards are intended to provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end. Illegitimate callers can easily be identified.

To protect consumers against spam calls, service providers are implementing STIR/SHAKEN in their network. This is already in place in United States and Canada in adherence with FCC guidelines. This helps to identify suspect calls giving users confidence in answering calls from unknown numbers. The end users benefit from service providers verification of caller-ID.

When STIR/SHAKEN support is implemented on the Webex server, the phone displays an extra icon next to the caller ID based on the caller's STIR/SHAKEN verification result.

17. Secure Meetings

When registered to Webex Calling, the Cisco Desk Phone 9800 and 8875 can protect the merging of meetings with traditional calls. These security features protect the integrity and confidentiality of meetings.

For example, a call and a meeting cannot coexist together, and the phone prohibits merging the two together. Likewise, you cannot join two meetings together or transfer a meeting to another call (see Figure 3).

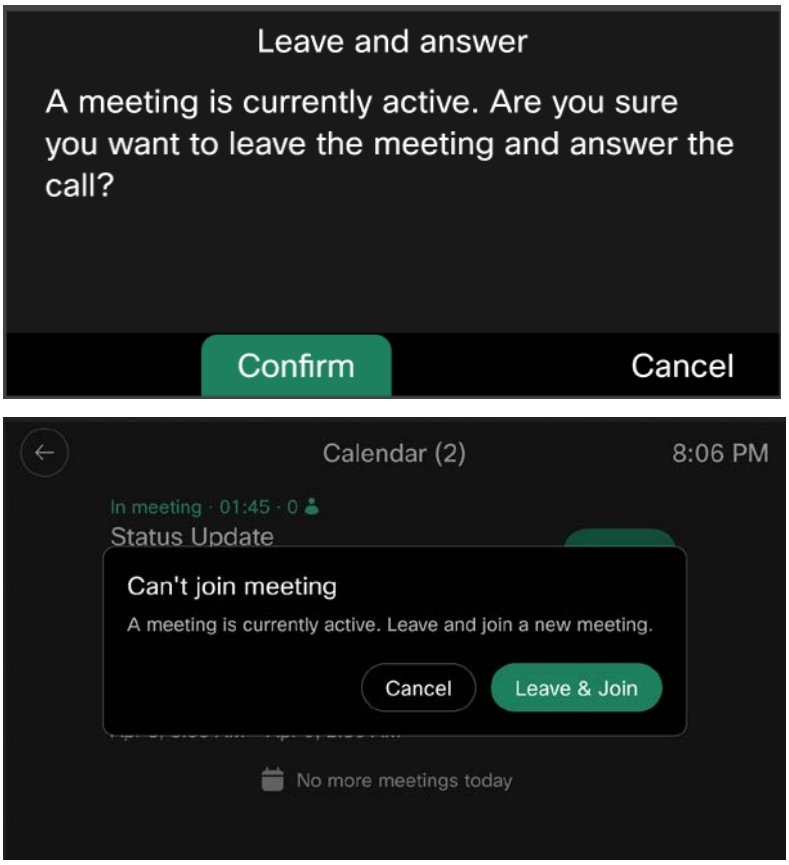

Figure 3. Meeting and Call Merge Protection

18. Ciphers

You can specify the cipher suites that the phone TLS applications use. The specified cipher list applies to all the applications that use the TLS protocol. You can also specify the cipher suites with the configuration file.

1. TLS cipher suites used to connect with Webex Calling Services

   TLS signaling connections from 9800 series phone and 8875 to Webex Calling services can negotiate only the following strong cipher suites, in following order of preference:

   - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
   - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
   - TLS_RSA_WITH_AES_256_GCM_SHA384

2. TLS cipher suites used to connect with Unified CM

   TLS signaling connections from 9800 series phone to Unified CM can negotiate only the following strong cipher suites with Webex services, in following order of preference:

   TLS 1.2 cipher suites

   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_RSA_WITH_AES_256_CBC_SHA
   - TLS_RSA_WITH_AES_128_CBC_SHA

   TLS 1.3 cipher suites

   - TLS_AES_128_GCM_SHA256
   - TLS_AES_256_GCM_SHA384
   - TLS_CHACHA20_POLY1305_SHA256

   TLS 1.3 key exchange

   - X25519 [RFC7748]
   - secp256r1 (NIST P-256)
   - secp521r1
   - secp384r1

   TLS 1.3 digital signature

   - ecdsa_secp256r1_sha256
   - ecdsa_secp384r1_sha384
   - ecdsa_secp521r1_sha512
   - rsa_pss_rsae_sha256
   - rsa_pss_rsae_sha384

- rsa_pss_rsae_sha512
- rsa_pkcs1_sha256
- rsa_pkcs1_sha384
- rsa_pkcs1_sha512

19. Security Compliance

FedRAMP* and FIPS support improves phone security. The 9800 Series and the 8875 all provide support for FedRAMP and FIPS 140-2.

* Coming soon.

20. Unified CM – Secure Media and Signaling

- Cisco Desk Phone 9800 Series can utilize SIP OAuth.
- X.509v3 certificates are used for device authentication in a number of security contexts.
- Each Desk Phone 9800 Series contains a unique Manufacturing Installed Certificate (MIC).
- The MIC provides a factory-installed unique identity.
- Desk Phone 9800 Series also support a 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.

21. Unified CM – Cisco Expressway Mobile and Remote Access (MRA)

Cisco Expressway MRA allows for secure, VPN-less access to Unified Communications (UC) services from outside the organization's private network. It facilitates firewall and NAT traversal for remote endpoints that are registered with Cisco Unified Communication Manager.

- Encrypted signaling and media can be established between a remote endpoint and Expressway-C without requiring Unified CM to be in mixed-mode.

- For encrypted signaling directly between a remote endpoint and Unified CM, as well as for encrypted media between a remote endpoint and on-premises endpoints, gateways, or conference bridges, Unified CM mixed-mode configuration is necessary unless using SIP OAuth.
- TLS encryption is used to protect the privacy and integrity of SIP signaling, as well as to secure visual voicemail access, directory lookups, and the downloading of configuration files.

22. Transport Layer Security (TLS)

- TLS (Transport Layer Security) is used to both authenticate and encrypt all SIP signaling messages between the phone and the Unified CM or Webex Calling when the phone is set up with an encrypted security profile.
- For phones with an authenticated security profile, TLS is used only for authentication purposes, without encrypting the SIP signaling messages.
- SIP TLS communication with the Unified CM or Webex Calling is mutually authenticated, ensuring that the signaling occurs between trusted entities and is protected from tampering.
- Media encryption is negotiated and enabled only when the signaling has been established over encrypted TLS sessions.
- A padlock icon is displayed to the user to indicate that the call is encrypted when media encryption is successfully negotiated between encrypted devices.
- Encrypted SRTP (Secure Real-time Transport Protocol) media streams provide integrity, authenticity, and confidentiality for the media data.

Table 1. TLS Support

FEATURE	7811, 7821, 7841, 7861	8811, 8841, 8845, 8851, 8861, 8865	8875, 9841, 9851, 9861, 9871
TLS 1.0	Yes	Yes	Yes
TLS 1.2	Yes	Yes	Yes
TLS 1.3*	No	No	Yes

* The 8875 will support TLS 1.3, yet it will not take advantage of the TPM 2.0 hardware module. Unified CM 15 SU2 and higher will support TLS 1.3. For more information, please visit: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15/cucm_m_tls-setup_2.html

23. Wired 802.1x

The Desk Phone 9800 Series supports standard 802.1X supplicant options for network authentication, which include:

- EAP-FAST (Flexible Authentication via Secure Tunneling)
    - EAP-TLS (Transport Layer Security)
    - EAP-FAST and EAP-MD5 use a username and password for client authentication to grant network access.
- EAP-TLS requires a client certificate to authenticate and allow network access.
- For wired connections using EAP-TLS, the client certificate can be either the phone's Manufacturer Installed Certificate (MIC) or a Locally Significant Certificate (LSC) in Unified CM
- The Locally Significant Certificate (LSC) in Unified CM is recommended as the client authentication certificate for wired EAP-TLS.

24. Wireless 802.1x

The Desk Phone 9861 and 9871 includes the following security features and authentication methods for wireless (WLAN) 802.1X networks:

- 802.1X wireless provides AES (Advanced Encryption Standard) encryption for secure data transmission.
- Wireless authentication support includes 802.1X (EAP) and Wi-Fi Protected Access (WPA) versions 3 Personal and Enterprise
- Supported EAP types for 802.1X wireless are:
    - EAP-FAST
    - PEAP (Protected EAP) with MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2) or GTC (Generic Token Card), with optional server validation
- EAP-TLS
- EAP-FAST and PEAP use a 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 the phone's Manufacturer Installed Certificate (MIC) or a user-installed certificate from either an enterprise Certificate Authority (CA) or a public CA.
- User-installed certificates can be added manually via the phone's web interface or automatically using the Simple Client Enrollment Protocol (SCEP).

With Unified CM version 10.5.2 or higher, administrators can provision WLAN profiles that prevent end users from altering settings such as the Service Set Identifier (SSID), frequency band, credentials, passwords, and keys.

25. Device and Peripheral Control

Unified CM and Webex Calling provide the ability to disable the following:

- Enable/disable Wi-Fi (9861, 9871).
- Lock administrator-controlled wallpaper on 9851, 9861, 9871. (Unified CM).
- Enable/disable/restrict access to phone settings (Unified CM)
- Enable/disable built-in web server (for supportability and diagnostics); it is disabled by default.
- Enable/disable PC voice VLAN access.
- Re-mark QoS from PC port
- Enable/disable USB ports
- The USB port is restricted to audio devices
    - USB audio devices are enabled by default
    - USB can be disabled via Unified CM or Webex Calling on the device page
- Enable/disable Bluetooth (9861, 9871)
- Enable/disable PC port.

26. Cisco Security and Trust

Cisco Security Tools and Processes

Cisco Secure Development Lifecycle (CSDL)

At Cisco, security is not an afterthought. It is a disciplined approach to building and delivering world-class products and services from the ground up. All Cisco product development teams are required to follow the Cisco Secure Development Lifecycle (CSDL). It is a repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products. The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle helps ensure defense in depth. It also provides a holistic approach to product resiliency. The Webex Product Development team passionately follows this lifecycle in every aspect of product development.

For more information, refer to the Cisco Secure Development Lifecycle Overview.

Cisco Foundational Security Tools

The Cisco Security and Trust Organization provides the process and the necessary tools that give every developer the ability to take a consistent position when facing a security decision.

Having dedicated teams to build and provide such tools takes away uncertainty from the process of product development.

Some examples of tools include:

- Product Security Baseline (PSB) requirements that products must comply with
- Threat-builder tools used during threat modeling.
- Coding guidelines.
- Validated or certified libraries that developers can use instead of writing their own security code.

- Security vulnerability testing tools (for static and dynamic analysis) used after development to test against security defects.
- Software tracking that monitors Cisco and third-party libraries and notifies the product teams when a vulnerability is identified.

Organizational Structure that Instills Security in Cisco Processes

Cisco has dedicated departments in place to instill and manage security processes throughout the entire company. To constantly stay abreast of security threats and challenges, Cisco relies on:

- Cisco Information Security (InfoSec) Cloud team
- Cisco Product Security Incident Response Team (PSIRT)
- Shared security responsibility

Cisco InfoSec Cloud

Led by the chief security officer for cloud, this team is responsible for delivering a safe Webex environment to customers. InfoSec achieves this by defining and enforcing security processes and tools for all functions involved in the delivery of Webex into customers' hands.

Additionally, Cisco InfoSec Cloud works with other teams across Cisco to respond to any security threats to the Webex service.

Cisco InfoSec is also responsible for continuous improvement in Webex's security posture.

Cisco Product Security Incident Response Team (PSIRT)

Cisco PSIRT is a dedicated global team that manages the inflow, investigation, and reporting of security issues related to Cisco products and services. PSIRT uses different mediums to publish information, depending on the severity of the security issue. The type of reporting varies according to the following conditions:

- Software patches or workarounds exist to address the vulnerability, or a subsequent public disclosure of code fixes is planned to address high-severity vulnerabilities.
- PSIRT has observed active exploitation of a vulnerability that could lead to a greater risk for Cisco customers. PSIRT may accelerate the publication of a security announcement describing the vulnerability in this case without full availability of patches.
- Public awareness of a vulnerability affecting Cisco products may lead to a greater risk for Cisco customers. Again, PSIRT may alert customers, even without full availability of patches.

In all cases, PSIRT discloses the minimum amount of information that end users will need to assess the impact of a vulnerability and to take steps needed to protect their environment. PSIRT uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. PSIRT does not provide vulnerability details that could enable someone to craft an exploit.

Refer to the PSIRT infographic to learn more about PSIRT.

Security responsibility

Although every person in Webex group is responsible for security, the following are the main roles:

- Chief security officer, Cloud
- Vice president and general manager, Cisco Cloud Collaboration Applications

- Vice president, engineering, Cisco Cloud Collaboration Applications
- Vice president, product management, Cisco Cloud Collaboration Applications

Internal and external penetration tests

The Webex group conducts rigorous penetration testing regularly, using internal assessors. Beyond its own stringent internal procedures, Cisco InfoSec also engages multiple independent third parties to conduct rigorous audits against Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. Cisco also uses third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. As part of the engagement, a third party performs the following security evaluations:

- Identifying critical application and service vulnerabilities and proposing solutions
- Recommending general areas for architectural improvement
- Identifying coding errors and providing guidance on coding practice improvements

Third-party assessors work directly with the Webex engineering staff to explain findings and validate the remediation. Penetration test letters of attestation for Webex services are available under NDA on the Cisco Trust Portal.

27. Transparency

Webex users and customers should understand what their choices are and how Cisco manages and protects the data they entrust to Cisco. Cisco uses a layered model of transparency to make this happen. Short disclosures that help users make real-time decisions are provided within the Webex App itself. Further information is available on the support pages, which are updated on a regular basis. And for all the details of what information Cisco collects, how it is used, and how it is protected including privacy for Personally Identifiable Information (PII), refer to the Webex Calling Privacy Data Sheet and/or the Cisco Unified Communications Manager Privacy Data Sheet available on Cisco Trustportal.

Cisco is also committed to publishing data regarding requests or demands for customer data that are received from law enforcement and national security agencies around the world. Cisco publishes this data twice yearly (covering a reporting period of either January-to-June or July-to-December). Like other technology companies, Cisco will publish this data six months after the end of a given reporting period in compliance with restrictions on the timing of such reports.

More information can be found at in the transparency section of the Cisco Trust Center available at https://trust.cisco.com.

Cisco has also invested in several transfer mechanisms to enable the lawful use of data across jurisdictions, including:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

28. Summary

Cisco Desk Phone 9800 Series provide a rich set of security features. These security features can be customized by administrators to meet the requirements of their deployment.

29. How to Buy

To view buying options and speak with a Cisco sales representative, visit How to Buy Cisco Products.

30. For More Information

- Cisco Trustworthy Technologies Data Sheet