Payment Card Industry Data Security Standard

Are you compliant with PCI DSS?

This white paper presents information about the Payment Card Industry (PCI) Data Security Standard (DSS). PCI DSS is applicable to any entity that accepts credit cards as a payment method or that stores, processes, or transmits a cardholder's data.

PCI DSS overview

The PCI Security Standards Council is a global organization founded in 2006 by American Express, Discover, JCB International, MasterCard, and Visa Inc. The council maintains, evolves, and promotes Payment Card Industry standards for the safety of cardholder data. The individual payment brands share equally in the governance and execution of the council's work.

What is PCI DSS?

- PCI DSS provides a baseline of 12 technical and operational requirements, which are designed to protect cardholder data and mirror security best practices (Table 1).
- PCI DSS applies to all entities that engage in card processing, including merchants, processors, acquirers, issuers, and all other payment service providers.
- PCI DSS also applies to all entities that store, process, or transmit Cardholder Data (CHD) and/or Sensitive Authentication Data (SAD).

Note: This white paper does not discuss the entire set of PCI DSS requirements. It focuses mainly on requirements 2 and 4, which have the greatest impact on Cisco® collaboration endpoints and systems.

Contents

Table 1. PCI DSS goals and requirements

Goals	Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors

Cisco Unified Communications

What are the implications?

PCI DSS requirements have been in place since June 2018. The individual payment brands enforce compliance with PCI DSS and determine any penalties for noncompliance.

The payment brands may, at their discretion, fine a bank or finance institution from $5,000 to $100,000 per month for PCI compliance violations. Penalties are not openly discussed or widely publicized.

Qualified Security Assessor (QSA) companies are independent security organizations that have been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS. QSA companies leverage certified assessment tools such as Nessus or Qualys to validate adherence to PCI DSS. For a complete list of vendors, refer to the QSA approved scanning vendors on the PCI security standards website.

How are on-premises unified communications affected by PCI DSS?

The PCI DSS v3.2 Frequently Asked Questions (FAQ) states:

"PCI DSS requirements apply wherever account data is stored, processed, or transmitted. While PCI DSS does not explicitly reference the use of VoIP, VoIP traffic that contains cardholder data is in scope for applicable PCI DSS controls, in the same way that other IP network traffic containing cardholder data would be. [...] VoIP traffic containing account data that is stored, processed or transmitted internally over an entity's network, or transmitted externally by the entity, is in scope for applicable PCI DSS controls."

Note: While VoIP is in scope for PCI DSS, the lack of explicit and in-depth considerations for VoIP systems has led to varied interpretations of what is required for PCI DSS compliance for VoIP systems.

What PCI DSS controls can be used to protect VoIP telephony systems?

Transport Layer Security

Since June 2018, all entities must end use of Secure Sockets Layer (SSL) and early versions of Transport Layer Security (TLS) as a security control and use only secure versions of the protocol.

POS and POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as being not susceptible to any known exploits for SSL and early TLS may continue using these as a security control.

Two major PCI DSS requirements are highlighted as part of the migration:

2.3 - Encrypt all non-console administrative access with strong cryptography.

4.1 - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

For more details on the migration from SSL and early TLS, refer to the PCI Security Standards Council Information Supplement.

Recommendations

The PCI DSS Council considers strong encryption to be a security best practice. It recommends the use of TLS 1.2. SSL and early TLS (1.0) are not allowed under PCI DSS v3.2.

Cisco Collaboration Secured Architecture

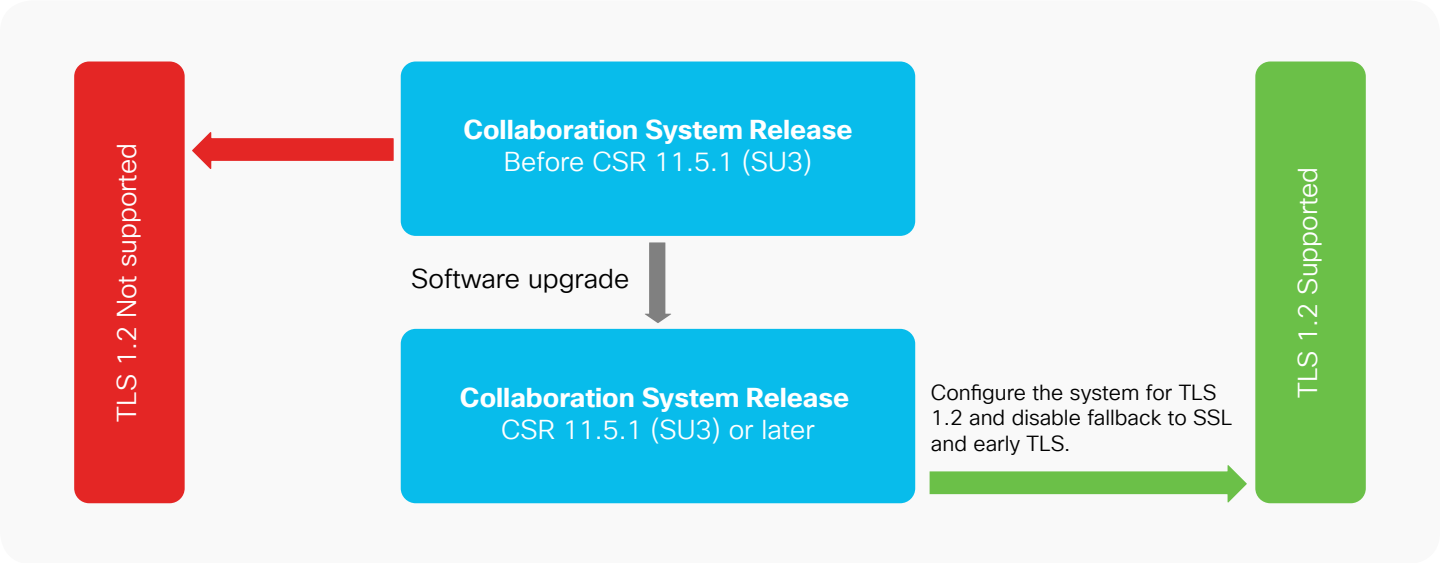
Cisco is committed to a strong focus on security beyond PCI DSS compliance. You can find more details about Cisco Collaboration Secured Architecture at Cisco Preferred Architectures.

Cisco Collaboration Software

To support TLS 1.2, administrators should update the collaboration environment to software release 11.5.1 (SU3), and contact center software to release 11.6(1).

A software upgrade is required for the following applications:

- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise solutions
  - Cisco Unified Customer Voice Portal
  - Cisco Virtualized Voice Browser
  - Cisco Finesse
  - Cisco Unified Intelligence Center
  - Cisco Live Data
  - Cisco SocialMiner
  - Cisco Enterprise Chat and Email
  - Cisco Remote Expert Mobile
  - Cisco Unified Contact Center Management Portal
- Cisco Unified Contact Center Express solutions
- Cisco Customer Journey Platform
- IM and Presence
- Cisco Unity® Connection
- Cisco Prime® Collaboration Deployment for releases earlier than 11.5.1 (SU3)



Cisco voice endpoints

- **Legacy Cisco IP phones**

Consider replacing any legacy Cisco IP phones (6900, 7900, 8900, and 9900 Series) with newer models such as the 7800 or 8800 Series. The 7800 and 8800 Series phones support TLS 1.2. For more information, see Table 2 and the Cisco Endpoints portfolio page.

Alternatively, to comply with PCI DSS, administrators can configure and modify several parameters in legacy devices and servers. After these changes are applied to achieve compliance, the phones will lose some advanced functionalities and will become similar to a basic analog phone.

For more details about impacts on functionality due to modification of parameters, see Table 3.

- **Cisco IP Phones 7800 and 8800 Series**

Cisco IP Phones 7800 and 8800 Series should be upgraded with firmware release 12.1 in order to support TLS 1.2.

Table 2 lists the TLS support in Cisco IP phone models.

For more details on security improvements in the latest Cisco IP phones, please refer to the Cisco IP Phone 7800 and 8800 Series Security Overview.

Table 2. TLS support in Cisco IP phone series

	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

- **Cisco Jabber**

To support TLS 1.2, administrators should upgrade Cisco Jabber® to Release 11.7 or later.

Cisco IP Communicator does not support TLS 1.2. Cisco recommends upgrading to Cisco Jabber Release 11.7 or later instead of using IP Communicator.

Table 3. Restrictions and Workarounds for Legacy Voice Endpoints in an environment where TLS 1.0/1.1 are disabled

Feature	Restriction
Legacy phones in Encrypted mode	Legacy phones in Encrypted mode will not work. There is no workaround.
Legacy phones in Authenticated mode	Legacy phones in Authenticated mode will not work. There is no workaround.

Feature	Restriction
IP phone services using secure URLs based on HTTPS	IP phone services using secure URLs based on HTTPS will not work. Workaround to use IP phone services: Use HTTP for all underlying service options (for example, corporate directory and personal directory). HTTP is not recommended, since it is not secure for sensitive data for features such as Extension Mobility. Drawbacks of using HTTP include: ▪ Provisioning challenges when configuring HTTP for legacy phones and HTTPS for supported phones. ▪ No resiliency for IP phone services. ▪ Performance impacts on the server handling IP phone services.
Extension Mobility Cross Cluster (EMCC) on legacy phones	EMCC is not supported with TLS 1.2 on legacy phones. Workaround to enable EMCC: 1. Enable EMCC over HTTP instead of HTTPS. 2. Turn on mixed mode on all Cisco Unified Communications Manager clusters. 3. Use the same USB e-tokens for all Cisco Unified Communications Manager clusters.
Locally Significant Certificates (LSC) on legacy phones	LSC is not supported with TLS 1.2 on legacy phones. As a result, 802.1X and phone VPN authentication based on LSC are not available. Workaround for 802.1X: Authentication based on MIC or password with EAP-MD5 on older phones. However, those are not recommended. Workaround for VPN: Use phone VPN authentication based on end-user username and password.
Encrypted Trivial File Transfer Protocol (TFTP) configuration files	Encrypted TFTP configuration files are not supported with TLS 1.2 on legacy phones, even with a Manufacturer Installed Certificate (MIC). There is no workaround.
Cisco Unified Communications Manager certificate renewal causes legacy phones to lose trust	Legacy phones lose trust when the Cisco Unified Communications Manager certificate is renewed. For example, a phone cannot get new configurations after renewing the certificate. This is applicable only in Cisco Unified Communications Manager 11.5.1. Workaround: To prevent legacy phones from losing trust, complete one of the following steps: 1. Temporarily allow TLS 1.0 (multiple Cisco Unified Communications Manager reboots). 2. Before enabling the CUCM certificate, set the Cluster For Roll Back to Pre 8.0 enterprise parameter to True. By default, this setting disables the security.

Feature	Restriction
Connections to nonsupported versions of Cisco Unified Communications Manager	TLS 1.2 connections to older versions of Cisco Unified Communications Manager that do not support the higher TLS version do not work. For example, a TLS 1.2 SIP trunk connection to Cisco Unified Communications Manager Release 9.x does not work because that release does not support TLS 1.2. You can use one of the following workarounds: • Use nonsecure trunks, although this is not recommended. • Upgrade the nonsupported version to a release that does support TLS 1.2.
Certificate Trust List (CTL) client	The CTL client does not support TLS 1.2. Workarounds: • Temporarily allow TLS 1.0 when using the CTL client and then move the cluster to Common Criteria mode. Configure the Minimum TLS to 1.1 or 1.2. • Migrate to the Tokenless CTL by using the CLI command utils ctl setcluster mixed-mode in Common Criteria mode. Configure the Minimum TLS to 1.1 or 1.2.
Address book synchronizer	There is no workaround.

Cisco video endpoints

- **Legacy Cisco TelePresence**
  - Newer Tandberg Codec (TC) endpoints support Collaboration Endpoint Software (CE) Release 9.1(3).
  - For legacy TC endpoints such as C-Series, EX, MX200 or MX300 G1, or Profile, consider upgrading to Cisco TelePresence® TC software release 7.3(11).
  - Legacy immersive systems such as the TX9000 series and Cisco TelePresence System will not support TLS 1.2.
- **Cisco Collaboration Endpoint Software**

Consider upgrading any CE endpoints (Cisco DX70 or DX80 or Cisco TelePresence MX200 or MX300 G2, MX700 or MX800, or SX Series) to Cisco CE software release 9.1(3).

*Note: Cisco DX650 endpoints on Android should be replaced with newer hardware. This model is not PCI DSS compliant.

For a summary of endpoint considerations and details on all other components, please refer to the Compatibility Matrix.

Table 4. Suggested hardware migrations

If you have...	Cisco recommends...
Legacy telephones: 9900, 8900, 7900, 6900 Series	Replace legacy phones with Cisco IP. Phone 8800 or 7800 Series that support TLS 1.2.
Legacy video systems: TX or CTS Series, DX 650	Replace legacy video systems with Cisco DX Series, SX Series, MX Series, or Cisco Webex Room Series.
Software clients: Cisco Jabber or IP Communicator	Replace legacy IP Communicator with Cisco Jabber Release 11.7 or later.

Find more information about the current portfolio on the Cisco Endpoints portfolio page.

Summary

Since June 2018, the PCI Data Security Standard v3.2 requires systems handling card data to comply. Customers using Cisco endpoints, Cisco Unified Communications, Cisco Unified Contact Center, and Customer Journey Platform are encouraged to develop action plans to comply with this standard by identifying potentially noncompliant devices and software versions and making any necessary changes, including upgrading hardware and software if needed.

Please contact your Cisco account team or Cisco partner for additional information and support.

Additional information

PCI DSS resources

- PCI DSS official website
- PCI DSS document library
- Qualified Security Assessors
- Approved scanning vendors
- SSL and early TLS migration
- Telephone based payment
- Best practices

Cisco resources

- PCI DSS Compliance for Cisco Collaboration
- TLS 1.2 Compatibility Matrix for Cisco Collaboration Products
- TLS 1.2 for On-Premises Cisco Collaboration Deployments
- Cisco Contact Center Enterprise Solution Security Whitepaper
- Cisco IP Phone Security White Paper
- Cisco IP Phone Matrix

For Cisco partners

- PCI on Cisco SalesConnect
- Collaboration Upgrade Scanner (perform readiness assessments)
- Migration FX (zero-touch desk phone replacement)

C11-740445-02 07/19