

Oracle Hospitality Food & Beverage Solutions – TLS 1.2 Update (Doc ID 2311832.1)

Modified: 21-Jun-2018 Type: BULLETIN

In this Document

[Purpose](#)

[Details](#)

APPLIES TO:

Oracle Hospitality Symphony
Oracle Hospitality Symphony First Edition
Oracle Hospitality RES 3700
Oracle Hospitality e7
Oracle Hospitality 9700
Information in this document applies to any platform.

PURPOSE

This document explains the encryption payment data requirement for Oracle Hospitality Food & Beverage POS products, actions needed to comply with the TLS v1.2 requirement, upgrade and PCI-DSS compliance considerations, and where to obtain the compliant versions of Oracle Hospitality POS software.

DETAILS

About the Encryption Requirement

Many Oracle Hospitality Point of Sale (POS) systems transmit credit card transactions using one of the Secure Socket Layer (SSL) encryption protocols. On June 30, 2018, all SSL protocols will lose their secure encryption method status.

All payment systems must encrypt payment data using Transport Layer Security (TLS) v1.1 or v1.2.

While both TLS versions meet the encryption requirements, most gateways and processors will only support TLS v1.2 (the most current standard) after June 30, 2018.

For more information about the TLS v1.2 requirement, see the Transport Layer Security (TLS) and Oracle Hospitality web site at <https://www.oracle.com/industries/hospitality/transport-layer-security.html>.

How does the encryption upgrade requirement affect Oracle F&B POS customers?

Systems that process credit payments must use the approved, secure encryption method supported by their processor or gateway by June 30, 2018.

The payment vendors will reject payment requests that do not use the new standard.

What actions must be taken for each affected product to comply with the TLS v1.2 requirement?

The Oracle Hospitality POS portfolio includes systems utilizing different technologies and methods of credit card processing.

The following table lists the products affected and the minimum version required to comply with TLS v1.2 for each product:

POS Product	Minimum Version Required for TLS v1.2 Support
Symphony	Symphony v2.8.2 or higher
	Note: If you are using Merchant Link, TVS driver v4.18.1.11 Hot Fix 1 is required. Contact Merchant Link for more information.
Symphony First Edition	Symphony First Edition v1.7.1 or higher
RES 3700	5.0 or higher
	Credit Card Interface Drivers v5.1 or higher
	Note: It is necessary to use both versions to comply with the TLS v1.2 requirement.
e7	e7 v4.2 or higher
9700	9700 v4.0 or higher

Does every customer have to upgrade?

Systems that process payments using external devices integrated with the Oracle Payment Interface (OPI) do not need to upgrade to comply with this mandate.

Customers must validate that the payment devices use the TLS v1.2 standard with their payment service provider.

Upgrade and PCI-DSS compliance considerations

Customers should closely consider the version of Oracle F&B POS they plan to run and maintain. Prior versions of POS systems are documented in their individual Lifetime Support Policies. However, most of these versions will not support the TLS v1.2 compliance requirements. These legacy versions are supported as per Oracle's support policies and may be appropriate for systems outside the scope of PA-DSS compliance, but should not be used by those who process credit cards through their POS system.

Using a PA-DSS compliant payment application does not ensure PCI DSS compliance. A Qualified Security Assessor (QSA) reviews the application, environment, and configuration when validating operations for PCI-DSS compliance.

All environments that store, process, or transmit cardholder data are in scope for an entity's PCI DSS assessment, including applications that have been validated to PA-DSS. The PCI DSS assessment should verify that the PA-DSS validated payment application is properly configured and securely implemented per PCI DSS requirements. If the payment application has undergone any customization, a more in-depth review will be required during the PCI DSS assessment, as the application may no longer be representative of the version that was validated to PA-DSS.

Where can you get the compliant versions of Oracle Hospitality POS software?

Download general availability software from the Oracle Software Delivery Cloud:
<https://edelivery.oracle.com/>

Download patch sets from My Oracle Support:
<https://support.oracle.com>

Didn't find what you are looking for?