

Oracle® Hospitality POS Printer Security Guide



Release 1.0
F20355-01
June 2019

ORACLE®

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	4
<hr/>	
1 POS Printer Security Overview	1-1
<hr/>	
Basic Security Considerations	1-1
Overview of POS Printers	1-1
<hr/>	
2 Performing a Secure POS Printer Installation	2-1
<hr/>	
Pre-Installation Security	2-1
Installing Printers Securely	2-1
<hr/>	
3 Vendor Links	3-1
<hr/>	

Preface

Audience

This document is intended for those who set up, install, and operate Point of Sale (POS) printers in a networked environment. Printers in this category include thermal (receipt) printers, impact (kitchen) printers, and mobile printers.

Important Information

Use this guide as a reference for secure implementation of POS printers, but refer to the printer vendor product specific documentation for detailed instructions. This guide is not specific to a particular software application.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
<https://support.oracle.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to recreate
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

Oracle Food and Beverage product documentation is available on the Oracle Help Center at <https://docs.oracle.com/en/industries/food-beverage/>

Revision History

Date	Description of Change
June 2019	Initial publication.

POS Printer Security Overview

This chapter provides an overview of Oracle Food and Beverage POS Printer features and explains the device security principles.

Basic Security Considerations

The following principles are fundamental to using any hardware or software securely:

- Keep software up to date. This includes software and drivers specific to the product as well as the latest patches available from 3rd party vendors.
- Limit account privileges as much as possible. Users should only be given the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- Install software and hardware securely. Do not expose printers to the public internet. For example, use firewalls, secure protocols using TLS (SSL), and secure passwords.
- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.
- Use secure development practices. For example, take advantage of existing database security functionality instead of creating your own application security.
- Keep up to date on security information. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the Oracle Critical Patch Updates and Security Alerts web site: <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Overview of POS Printers

POS printers are manufactured for Oracle with specific compatibility requirements for Oracle POS applications. These devices are ruggedized, specialized hardware with a range of features and capabilities to address specific use cases.

Table 1 - Oracle POS Printers

Feature	TM-T88	TM-U220	TM-P60II
Print Technology	Thermal	Impact	Thermal
Available Interfaces	Serial	Serial	Bluetooth
	IDN	IDN	Wi-Fi
	Ethernet	Ethernet	
Typical Use Case	Check/Receipt Printing	Order (Kitchen) Printing	Receipt (Mobile) Printing

Understanding the POS Printer Environment

When planning your POS printer implementation, consider the following:

- Which resources need to be protected?
- You need to restrict access to external ports, such as USB, Ethernet and Serial ports.
- You need to protect customer data, such as credit card numbers.
- You need to protect internal data, such as proprietary source code.
- You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from?
- What will happen if protections on a strategic resource fail?

Physical Security

POS hardware is typically installed in environments where physical access to the devices can be difficult or impossible to control. The devices are commonly in publically accessible areas for optimal usage by employees. When possible, POS printers should be situated in locations where non-employees do not have easy physical access to the device or its interface connections. Ideally, the area should be securable when employees are not present.

Ethernet Interfaces

Ethernet interface modules incorporate firmware that contains Oracle-specified factory default security settings to not only be compatible with the POS system, but include enhanced security settings. Examples include turning off SNMP, or making use of TLS 1.2.

Setup Tool User Authentication

Changes to the default settings can be made using the printer's Ethernet interface setup tool. Refer to the specific printer vendor product documentation for guidance on using the setup tools.



NOTE:

Oracle Food and Beverage recommends changing the default authentication passwords for setup tools during installation.






Simple Network Message Management Protocol (SNMP)

Ethernet interface cards have the capability to run the Simple Network Management Protocol (SNMP). Older versions of SNMP were known to contain vulnerabilities. To eliminate the associated SNMP risk, Oracle disables SNMP by default. The table below provides information on how to identify the Ethernet interfaces sold by Oracle (and MICROS prior to the Oracle acquisition).

IMPORTANT:

Ethernet IV cards do not support disabling SNMP and must be replaced.

Table 2 – Epson Ethernet Module Hardware

Module	Ethernet IV (EOL)	UB-E03	UB-E04	UB-EML01 Multilingual (EOL)	UB-EML02 Multilingual
Identification					
Minimum F/W Required	V1.07a	V1.03+M_2.00	V1.09_r09-O	V2.10	V1.05
SNMP Setting	Enabled	Disabled	Disabled	Disabled	Disabled

Certificates for POS Printers

NOTE:

Update the self-signed certificate present in Ethernet POS printers to avoid security warnings/failures on a corporate network.

A TLS 1.2 compliant security certificate acquired from a Certificate Authority (CA) is recommended. Refer to the vendor's printer documentation and utilities for guidance on importing certificates.

See [Chapter 3 – Vendor Links](#) for additional information about current Oracle POS printer vendors.

2

Performing a Secure POS Printer Installation

This chapter presents planning information and basic guidance for your POS printer installation. Please consult your IT Security Officer for any security decisions or requirements that pertain to your operating environment.

Pre-Installation Security

- Review the *Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide* if the printer uses wireless communications.
- Review a network diagram for the installation environment. Verify the device will only be installed on secured networks behind a hardware firewall.
- Determine how the device will be physically secured. Wall, shelving, or counter mounts may need to be installed in order to physically secure the device.

Installing Printers Securely

Physical Placement

POS printers are often located in areas that make physical access difficult or impossible to control. When possible, the units should be placed in locations that limit the possibility of unattended access or in locations that can be secured when not in use. Provided covers should be used to conceal the printer I/O panel.

Out-of-Box Setup

General guidance for out-of-box setup:

- **Ethernet Printers:**
 - Only connect Ethernet POS printers to secure networks located behind a firewall.
 - Update certificates on printer with TLS 1.2 compliant certificates from a trusted Certificate Authority.
 - Ensure SNMP is disabled.
 - Check for updates to printer/interface firmware and apply as needed.
 - Change the printer setup utility access password.
- **Wireless (Wi-Fi) Printers:**
 - Only connect to secure wireless networks. Networks using older key exchange protocols, such as WEP, are considered insecure.
 - Check for updates to printer/interface firmware and apply as needed.
 - Change the printer setup utility access password.

3

Vendor Links

Epson

Epson POS Printer Support:

<https://epson.com/Support/Point-of-Sale/sh/s5>

Epson Network Configuration Utility:

<https://download.epson-biz.com/modules/pos/index.php?page=soft&pcat=3&scat=43>

Epson Ethernet Interfaces:

UB-E03

https://download.epson-biz.com/modules/pos/index.php?page=single_doc&cid=2739

UB-E04

https://files.support.epson.com/pdf/ube04_/ube04_trg.pdf

Epson Guide to Securing Printers:

<https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/FBLP/Epson/Epson-103018-Guide%20to%20Securing%20Printers%20Whitepaper.pdf>