Oracle® Retail EFTLink

Security Guide

Release 15.0

E69277-01

December 2015

ORACLE®

Oracle Retail EFTLink Security Guide, Release 15.0

E69277-01

Primary Author: Tony Manda

Contributing Author: Phil Wells

Contents

Send Us Your Comments

Oracle Retail EFTLink Security Guide, Release 15.0.

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at http://www.oracle.com.

Preface

This guide serves as a best practice guide for ensuring secure operation of Oracle Retail EFTLink. Installation and configuration are covered in more detail in separate guides as listed in the Related Documents section below.

Audience

This document is intended for administrators and engineers who are responsible for secure deployment of EFTLink.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Retail EFTLink documentation set:

- *Oracle Retail EFTLink Release Notes*
- *Oracle Retail EFTLink Framework Implementation and Configuration Guide*
- *Oracle Retail EFTLink Core Implementation and Configuration Guide*

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 re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 15.0) or a later patch release (for example, 15.1). If you are installing the base release and additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Documentation is packaged with each Oracle Retail product release. Oracle Retail product documentation is also available on the following Web site:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

(Data Model documents are not available through Oracle Technology Network. These documents are packaged with released code, or you can obtain them through My Oracle Support.)

Documentation should be available on this Web site within a month after a product release.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Security Guidelines

This chapter describes retailer and solution specific responsibilities for ensuring EFTLink is securely implemented and configured.

Oracle Support

It is considered to be a best practice to have all Oracle Retail EFTLink support requests submitted through a single point of contact for that customer environment; the client designated administrator is usually designated to perform this role.

The link to use when submitting Service Requests (SR) is:

https://support.oracle.com

General Principles

This section describes general principles to be observed.

Securing Sensitive Data

The protection of sensitive data during transit and processing is paramount. Sensitive data includes personally identifiable information such as PAN Numbers and track 2 data. Ensure that if configurable, the EPS/payment terminal is set for PCI compliant masking of card PAN and track 2 data.

Retailer Responsibilities

An instance of EFTLink and any third party EFT software (dependent on solution) will typically run on the POS hardware and communicate with each other to process EFT transactions when requested by the POS software.

The POS Terminals are located in the customer facing areas of the store in proximity to both customers and employees. Physical security of the hardware is the responsibility of the retailer in addition to operational practices like provisioning employees to appropriate application roles and shutting registers down when not in use.

Securing the in store network is a responsibility of the retailer and is assumed to be compliant with PCI-DSS requirements for topology, wireless access, and wan

connections. The connection to the corporate data centers and the external credit authorizers also are assumed to follow PCI-DSS requirements for secured connections.

The PCI-DSS standards are available at https://www.pcisecuritystandards.org/security_standards/index.php

It is recommended that all machines on the store network be kept up to date with vendor supplied patches, especially security patches. The operating systems on POS Terminals should be locked down by removing or disabling unneeded functionality, in particular ensure that the system cannot be used for browsing the internet.

POS Security Considerations

POS security recommendations will vary according to the POS software being used. Please refer to the appropriate POS Security Guide or the POS Implementation Guide for your product.

Solution Specific Responsibilities

This section gives core specific security guidance.

AJB FiPay

AJBFiPay has an *enable.signature.logging* option. Enabling this property (setting to **True**) results in exposing the PII (customer signature). The *enable. signature.logging* option should therefore only be enabled when requested by Oralce Support for debugging purposes and shoud be turned off **immediately** debugging has been complete.

VeriFone Ocius Sentinel

Specific security considerations for EFTLink currently center around the Verifone Ocius Sentinel solution which requires a user login ID and PIN to be stored on the POS system. These are transmitted by EFTLink to the Ocius Sentinel application as part of a login process which is required before Ocius Sentinel can accept EFT requests.

When it is running the Ocius Sentinel application also offers a GUI (Graphical User Interface) which can be accessed by an operator via a login screen. The login screen accepts the same ID and PIN as stored in the EFTLink core configuration file. Having manually logged in to Ocius Sentinel a number of functions are available to the user, including processing payments and refunds which bypass the POS software.

In order to prevent unauthorized use of the Ocius Sentinel application the user login ID and PIN should be stored encrypted in the EFTLink core configuration file. An encryption tool is provided for this purpose and details on its use can be found in the EFTLink Core Configuration Guide.

It is recommended that batch encryption of user login ID and PIN data be carried out at a central location and the encrypted data then be distributed to stores as required. Once encryption has taken place the clear text copy of the data can be deleted.

Note: EFTLink is configured to expect encrypted ID and PIN data by default.
