

Oracle® Hospitality e7 Point-of-Sale
Security Guide
Release 4.3 EU
E88908-01

August 2017

Copyright © 2004, 2017, Oracle and/or its affiliates. All rights reserved.

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
Audience	4
Customer Support.....	4
Documentation.....	4
Revision History.....	4
1 e7 Point-of-Sale Security Overview	5
Basic Security Considerations	5
Overview of e7 Point-of-Sale Security.....	5
e7 Component Model.....	5
Understanding the e7 Point-of-Sale Environment	6
e7 Security	7
Operating System Security	7
Database Encryption Implementation	8
Network Encryption Implementation.....	9
2 Performing a Secure e7 Point-of-Sale Installation	10
Pre-Installation Configuration	Error! Bookmark not defined.
Installing e7 Point-of-Sale	10
Post-Installation Configuration.....	10
Create a Database Account.....	10
Generate Encryption Key.....	10
3 Implementing e7 Point-of-Sale Security	11
Encryption Key Maintenance.....	11
Employee and Job Category Access Control.....	11
Masking Employee Categories.....	11
Masking Job Categories	12
Configuring Access to Configurator Sections	12
Enable Microsoft Windows Complex Passwords.....	12

Preface

This document provides security reference and guidance for the following e7 Point-of-Sale components:

- e7 Point-of-Sales
- e7 Gift Card Interface
- e7 Transaction Services
- e7 Fiscal Interface

Audience

This document is intended for:

- System administrators installing e7 Point-of-Sale.
- End users of e7 Point-of-Sale.

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 and any associated log files
 - Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at <http://docs.oracle.com/en/industries/hospitality/>

Revision History

Date	Description of Change
August 2017	<ul style="list-style-type: none">• Initial publication

1 e7 Point-of-Sale Security Overview

This chapter provides an overview of Oracle Hospitality e7 Point-of-Sale security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

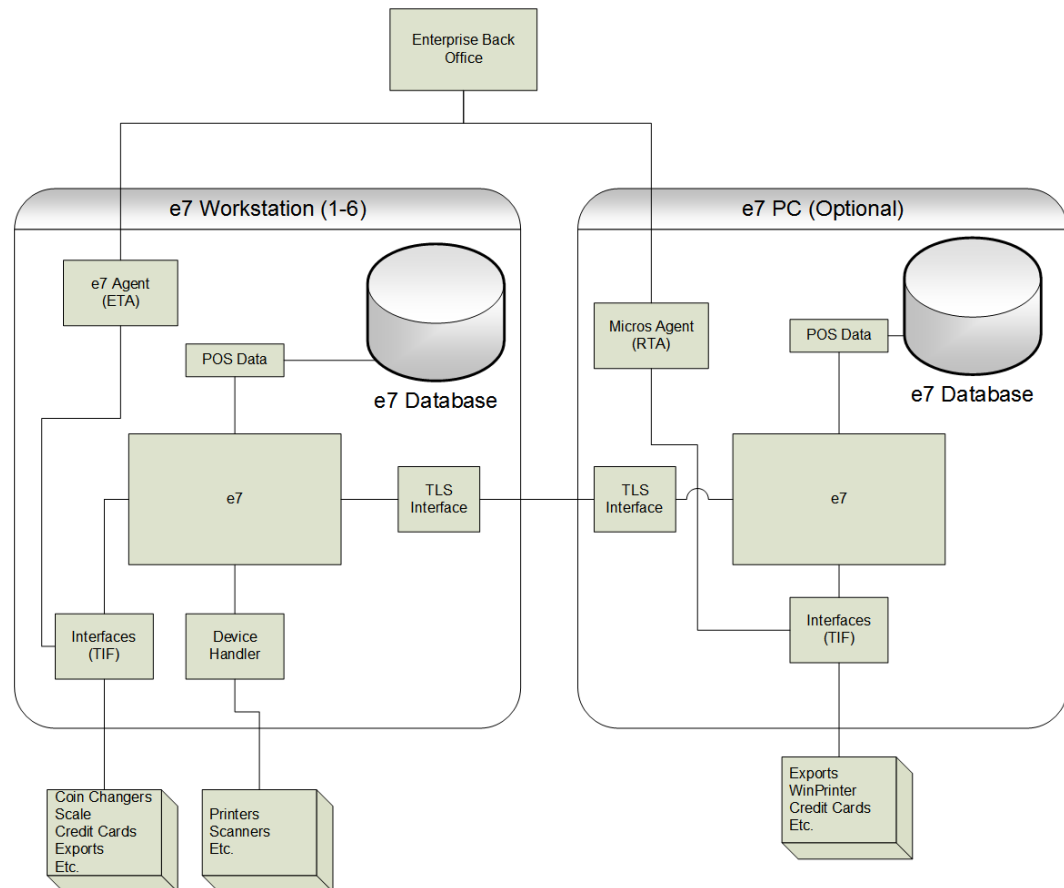
- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See [Performing a Secure e7 Point-of-Sale Installation](#) for more information.
- **Learn about and use the e7 Point-of-Sale security features.** See [Implementing e7 Point-of-Sale Security](#) for more information.
- **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 “Critical Patch Updates and Security Alerts” Web site: <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Overview of e7 Point-of-Sale Security

Oracle Hospitality e7 uses a role-based access control for employees to configure the system.

e7 Component Model

The following diagram models the interaction between e7 components, optional peripherals, and optionally the Enterprise Back Office backend database.



Understanding the e7 Point-of-Sale Environment

When planning your e7 Point-of-Sale implementation, consider the following:

- **Which resources need to be protected?**
 - You need to protect customer data.
 - 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?** For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.

- **What will happen if protections on strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly

e7 Security

Oracle Hospitality e7 includes several interface drivers that perform a variety of point-of-sales functions. When configuring the database, administrators only need to configure the drivers that relate to the functions used by the restaurant.

Operating System Security

The follow table lists the recommended settings and actions to secure Microsoft Windows operating systems. You do not need to follow these recommendations for Microsoft Windows Compact Edition.

Setting	Description
Microsoft Updates	Not configured. Windows Malicious Software Removal Toolx64 (kb890830) not installed.
Clear Virtual Memory Pagefile on shutdown	Enabled
Autoplay	Disabled for e7admin. Enabled for new accounts.
Firewall	On
Restore Points	Disabled
Power control settings	
Turn off the display	Never
Put the computer to sleep	Never
Hard disk / Turn off hard disk after	Never
Wireless Adapter Settings / Power Saving Mode	Maximum Performance
Sleep / Sleep after	Never
Sleep / Allow hybrid sleep	Off
Sleep / Hibernate after	Never
USB / USB selective suspend setting	Disabled
Power buttons and lid / Power button action	Shut down

Setting	Description
PCI Express / Link State Power Management	Off
Performance Options	
Visual Effects	Adjust for best performance.
Advanced / Processor scheduling	Programs
Data Execution Prevention	Turn on DEP for essential Windows programs and services only.
Local Area Connection 1 Properties	
Internet Protocol Version 6 (TCP/IPv6)	Deselected
Internet Protocol Version 4 (TCP/IPv4)	IP: 192.168.100.250 Subnet mask: 255.255.255.0
Global policy settings	
Always use classic logon	Enabled
Enforce password history	Enabled and set to 4.
Maximum password age	60
Password must meet complexity	Enabled
Audit account logon events policy	Enabled for both Success and Failure.
Audit logon events policy	Enabled for both Success and Failure.
Shutdown settings	
Allow system to be shut down without having to log on	Disabled
Do not display Install Updates and Shut Down Option	Enabled
Do not adjust default option to Install Updates and Shut down in the...	Enabled

Database Encryption Implementation

Oracle Hospitality e7 encrypts the database using a key derived from a randomly-generated data encryption key (DEK).

A user creates the DEK by clicking **Generate New Key** in the Configurator. The passphrase is stored in the SYSTEM_DETAIL table in the e7 database using the AES algorithm with a randomly-generated key encryption key (KEK) and initialization vector (IV). The key is stored in the `dbconfig.txt` file locally on a USB drive to be stored

securely, encrypted by Microsoft's DPAPI using machine-specific encryption. Throughout the e7 GUI and documentation, the passphrase is referred to as the “encryption key” or “key”. [Generate Encryption Key](#) contains instructions for generating the key.

Network Encryption Implementation

e7 uses the Transport Layer Security (TLS) protocol to protect all network communication between nodes. Both asymmetric and symmetric encryption is used. All related encryption keys are dynamically and randomly generated during the application life cycle. As a result, encryption keys protecting the network communication are never stored on disk and kept only in memory.

2 Performing a Secure e7 Point-of-Sale Installation

For information about installing e7, see the *Oracle Hospitality e7 Point-of-Sale Installation Guide*.

Installing e7 Point-of-Sale

e7 does not have options or customizations during installation. Follow the instructions in the *Oracle Hospitality e7 Point-of-Sale Installation Guide* when installing on the workstations and optionally the PC server.

Post-Installation Configuration

Create a Database Account

Create a user account for accessing the database. Do not use an existing employee, because this credential cannot perform Point-of-Sale functions.

1. In the e7 Configurator, click **Add New Employee**.
2. On the General tab, enter a last name.
3. On the Job Information tab, select a default job.
4. On the Security tab, select **Update Enhanced Security**, create login credentials, select **This is a database user**, and then click **Save**.

Generate Encryption Key

You must generate an encryption key after completing all installation processes.

1. Make sure there are no open checks in the system and no offline workstations, or the operation will fail.
2. Insert a USB drive to the PC or workstation generating the key.
3. In the e7 Configurator, navigate to the Restaurant form.
4. On the Security tab, click **Generate New Key**, enter the database user's credentials, and then click **Yes** each time you are prompted by the key generator.
5. Store the USB drive in a secure location so that it can be retrieved when a database restoration is required.

3 Implementing e7 Point-of-Sale Security

Encryption Key Maintenance

Change the passphrase used by e7 to generate the encryption key at least once per calendar year. You do not need to generate the key more than once in the store.

1. Make sure there are no open checks in the system and no offline workstations, or the operation will fail.
2. Insert a USB drive to the PC or workstation generating the key.
3. In the e7 Configurator, navigate to the Restaurant form.
4. On the Security tab, click **Generate New Key**, enter the database user's credentials, and then click **Yes** each time you are prompted by the key generator.
5. Store the USB drive in a secure location so that it can be retrieved when a database restoration is required.

Employee and Job Category Access Control

Warning: If you are not careful when configuring access control, you may lock yourself out and require reloading the database from a backup or a full reinstallation.

Masking Employee Categories

You can configure an employee category hierarchy and select **Hide from others** to restrict access to employee records belonging to the employee category to which they belong and to employee categories lower in the hierarchy.

For example, if you have the following employee categories:

Object Number	Employee Category
1	Superuser
2	Management
3	Front of House

An employee belonging to the Management category can view their Management and Front of House employee records. This access control also:

- Prevents changing the **Number** field of the employee category to prevent employees from modifying the hierarchy.
- Allows employees to modify the **Password ID** and **Alternate Password ID** fields for themselves and for employees belonging to lower employee categories.
- Removes hidden jobs from the **Default job** and **Job** drop-down lists in the Job Information tab.

To configure the employee category hierarchy:

1. Navigate to **Employees** from the menu, select an employee category, and then click the **General** tab.
2. Enter the hierarchy level in the **Number** field, where 1 is the highest level.

3. Select **Hide from others**.

Masking Job Categories

You can configure a job category hierarchy and select **Hide from others** to restrict employee access to job records belonging to the job category to which they belong and to job categories lower in the hierarchy.

For example, if you have the following job categories:

Object Number	Job Category	Jobs
1	Superuser	Superuser, Administrator
2	Management	Manager, Shift Manager
3	Front of House	Bar, Bar/Manager, Cashier, Host/Bus, QSR, Runner, Server

An employee working as a Manager can view and edit the Manager job record and Front of House job records such as the Bar.

To configure the job category hierarchy:

1. Navigate to **Jobs** from the menu, select a job category, and then click the **General** tab.
2. Enter the hierarchy level in the **Number** field, where 1 is the highest level.
3. Select **Hide from others**.

Configuring Access to Configurator Sections

You can configure access to specific forms in the e7 Configurator by job.

1. Navigate to **Configurator Access** from the menu.
2. Click **Add Record** to add a new access control rule.
3. Select a **Job**, and then select **Prevent form access**.
4. Select the form you want to prevent the job from accessing.

Enable Microsoft Windows Complex Passwords

1. Run `gpedit.msc` as an administrator.
2. Double-click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Account Policies**, and then double-click **Password Policy**.
3. Set the following values:
 - Enforce password history: 4 passwords remembered
 - Maximum password age: 60 days
 - Minimum password age: 0 days
 - Minimum password length: 8 characters
 - Password must meet complexity requirements: Enabled