Oracle® Hospitality e7 Point-of-Sale

Security Guide

Release 4.4
E95070-01
May 2018

Oracle Hospitality e7 Point-of-Sale Security Guide, Release 4.4

E95070-01

Contents

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 Credit Card Interface
- 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
- Screenshots 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
May 2018	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. See “Security Considerations for Developers” for more information.
- 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” website: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

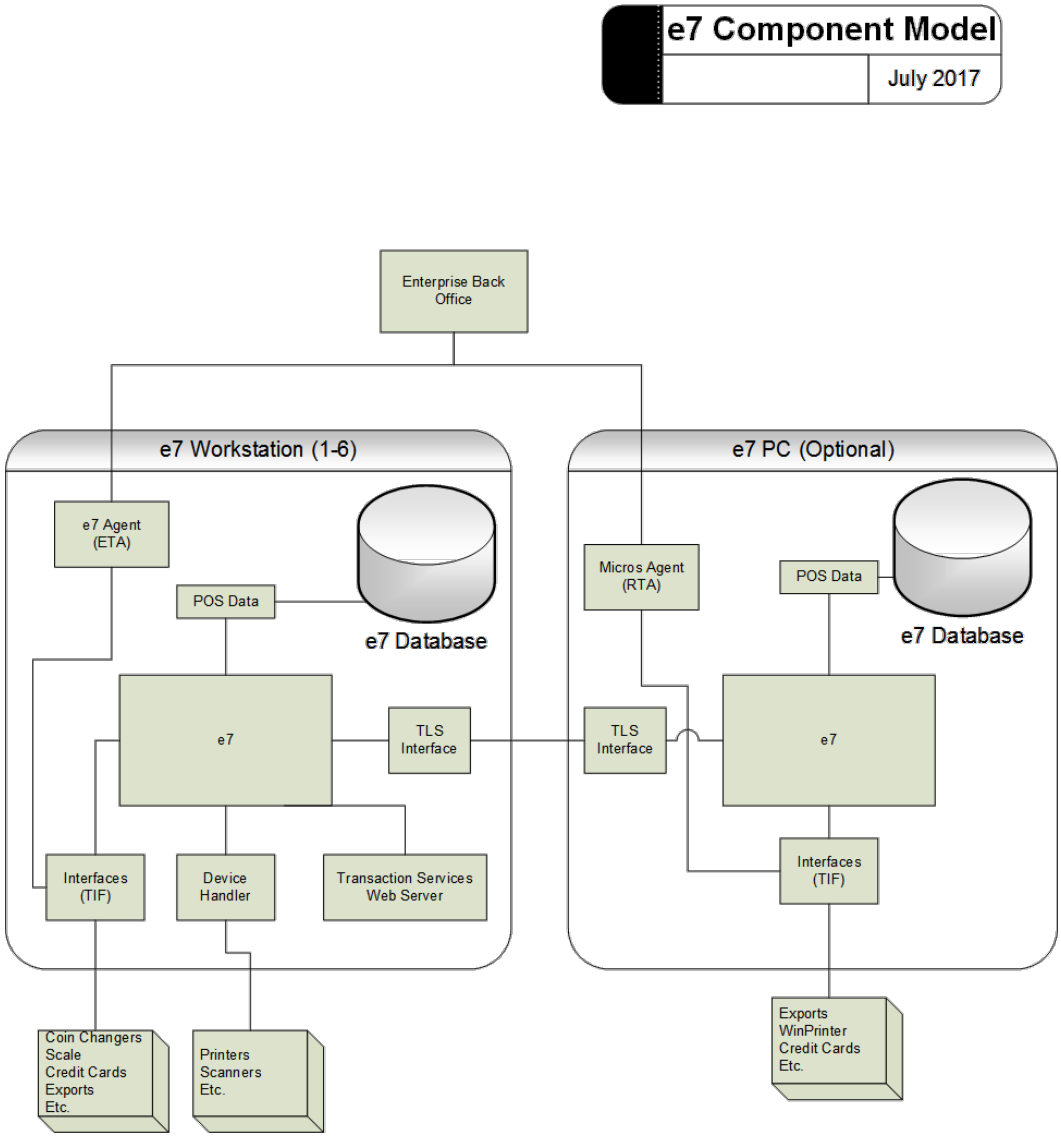
Overview of e7 Point-of-Sale Security

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

For credit card transactions, sensitive account data (SAD) may be transmitted between e7 nodes, the e7 PC, and the credit card processor. Messages are encrypted when transmitting SAD. When storing cardholder data in the e7 database, the data is first encrypted using a key managed by the administrator.

e7 Component Model

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



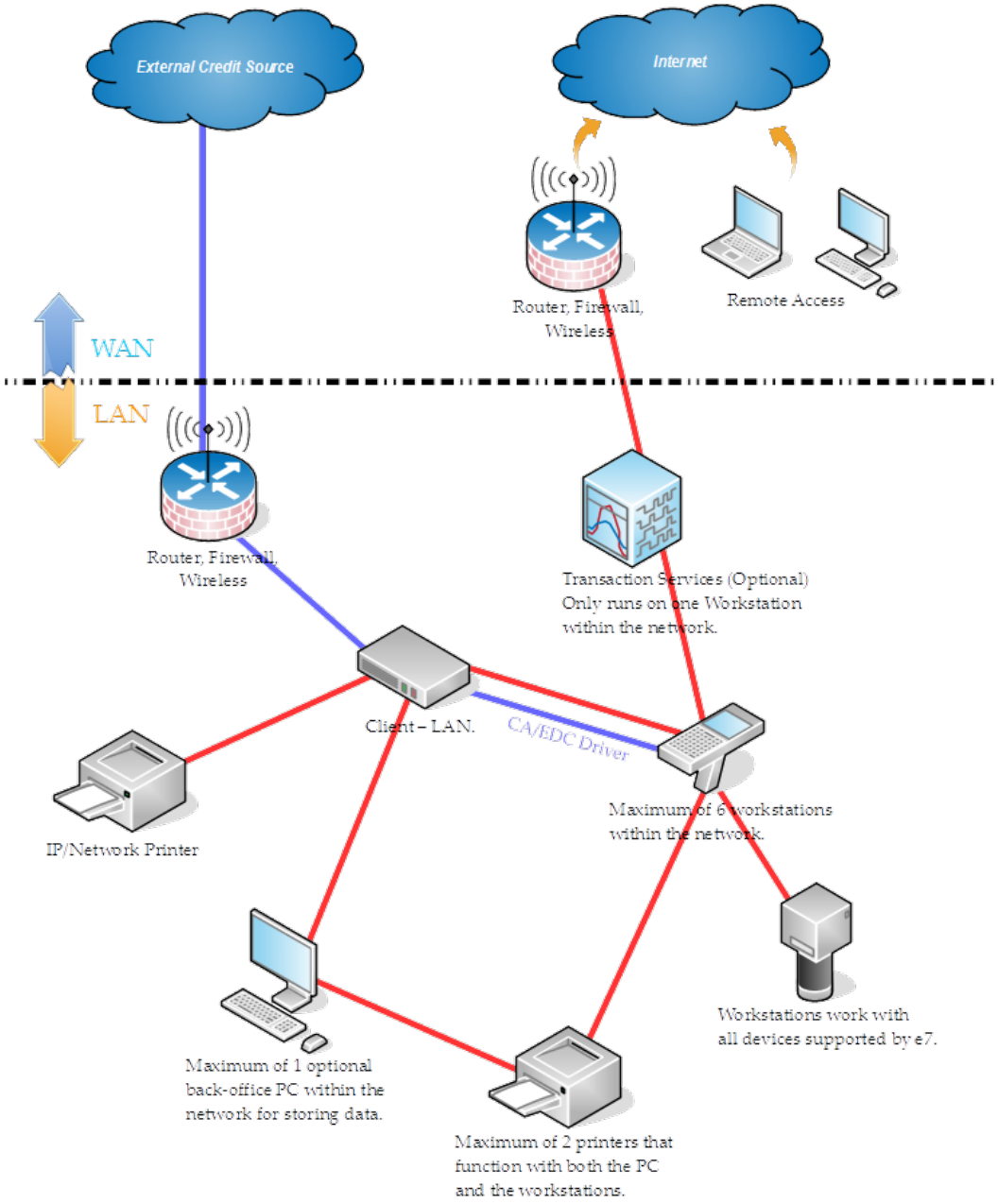
Understanding the e7 Point-of-Sale Environment

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

- **Which resources need to be protected?**
  - You need to protect customer data, 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?** 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.

Recommended Deployment Configurations



The blue lines represent encrypted credit card transactions to the host.

The red lines represent other traffic.

e7 Security

Oracle Hospitality e7 includes:

- Credit Card Drivers that communicate with several host processors. When configuring the system, administrators typically only need to configure one driver to communicate with the processor used by the restaurant.
- 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
PCI Express / Link State Power Management	Off

Setting	Description
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: *STATIC_IP* Subnet mask: *SUBNET_MASK*
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 sensitive data fields in the database using an AES encryption algorithm (AES128, AES192, or AES256) and 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.

The following database fields are encrypted due to their containing payment account data:

Table	Column
ReferenceDbDetailTable	ExpDate
	RefEntry
ReferenceTransDetailTable	ExpDate
	RefEntry
CcBatchItemTable	Track2Data
	CardAccountNumber
	ExpirationDate
	CustomerName
CcBatchTransferItemStatusTable	CardAccountNumber
	ExpirationDate
CreditAuthDbDetailTable	ExpDate
	AcctNum
	Track2
	CustName
	AcctNum

- The e7 application uses the `SpecialBytes` class found within the `MicrosSystems.E7.MicrosData` assembly to encapsulate encryption operations. The `SpecialBytes` class contains routines for managing the passphrase as well as for encrypting and decrypting data using the passphrase.
- When a user changes the key, each node decrypts existing data using the old key, and then encrypts data using the new 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*.

Pre-Installation Configuration

If you are upgrading from one of the following versions:

- 1.0
- 1.5 and 1.5 Patch 1
- 2.0
- 2.0, 2.0 Patch 1, and 2.0 Patch 2
- 2.7

You must remove historical sensitive data. See the *Oracle Hospitality e7 Point-of-Sale PA-DSS Implementation Guide* for more information and instructions about removing historical sensitive data and securing your system for processing credit card payments.

e7 Point-of-Sale Installation

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. Select **Enable Enhanced Security** to enable ringing credit card transactions.
6. Store the USB drive in a secure location so that it can be retrieved when a database restoration is required.

Configure Restaurant and Employee Access Control Settings

See the *Oracle Hospitality e7 Point-of-Sale PA-DSS Implementation Guide* for more information about securing the restaurant and employee accounts.

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 Configuration 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