Oracle® Hospitality e7 Point-of-Sale

Release Notes

Release 4.4 EU

E95128-01

May 2018

Oracle Hospitality e7 Point-of-Sale Release Notes, Release 4.4 EU

E95128-01

Contents

Preface

Oracle Hospitality e7 Point-of-Sale is a Point-of-Sale (POS) solution that provides business management capabilities for smaller enterprises with simple configuration and maintenance.

Purpose

These Release Notes provide a brief overview of additions, enhancements, and corrections implemented in this software release. Their intent is informative, not instructional. Review e7 Point-of-Sale's product documentation, including technical and application advisories for previous versions, for detailed information on installation, upgrade, configuration, and general use.

Audience

This document is for e7 Point-of-Sale technicians, administrators, and users.

Important Information

The information contained in these Release Notes pertains to the EU version of Oracle Hospitality 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
- 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

Table 1 Revision History

Date	Description of Change
May 2018	Initial Publication

1

Features and Updates

This chapter describes the features and updates contained in this release.

Security Module

This release adds the Security Module, which lets employees with the correct privileges:

- Monitor and configure e7 application logs.
- Anonymize and remove records on request.

Configure access to the Security Module

1. Log in to e7 using Manager credentials.
2. Click **Configurator**, click the **Menu** drop-down list, and then click **Jobs**.
3. For each job that you want to allow access to the Security Module:
    a. Select the job category and job.
    b. Click the **Privileges** tab, select **Use Security** in the **Module Access** group, and then click **Save**.

Add the Security Module touchscreen key

1. In the e7 Configurator, click the **Menu** drop-down list, and then click **Touchscreens**.
2. For each touchscreen that you want to add the key:
    a. Select the **Touchscreen**, click **New Button**, and then place the button on the screen.
    b. Select **Security** from the **Function** drop-down list, configure the button, and then click **Save**.

Retention Period for Inactive Employees, Customers, and Vendors

This release lets administrators configure data retention period in the **Restaurant** settings.

1. In the e7 Configurator, click the **Menu** drop-down list, and then click **Restaurant**.
2. Click the **Data Privacy** tab, and then configure the **Number of Days to Keep** for inactive employees, inactive customers, and inactive vendors.

Purging Inactive Records

This release adds an autosequence job to purge or anonymize employee, customer, and vendor records that have been inactive for longer than the configured data retention period. Retention Period for Inactive Employees, Customers, and Vendors contains more information about setting the retention periods.

1. In the e7 Configurator, click the **Menu** drop-down list, and then click **Autosequences**.
2. Click **End of Day manually**, add a new action with the following settings, and then click **Save**:
   - **Action**: `Purge Inactive Records`
   - **Parameters**: Using a comma-separated list, enter `1` to purge employee records, `2` to purge vendor records, and `3` to purge customer records. For example, enter `1,2,3` to purge all three records.

Configuring the Fields to Anonymize for Employee Data

This release lets administrators configure the employee Personally Identifiable Information fields that are anonymized by the Security Module in the **Restaurant** settings.

1. In the e7 Configurator, click the **Menu** drop-down list, and then click **Restaurant**.
2. Click the **Data Privacy** tab, and then select or deselect the fields that should be anonymized by the Security Module in the **Employee Sensitive Data** group.

Deleting or Anonymizing Employees, Customers, or Vendors

The Security Module lets employees with the correct privileges delete or anonymize employee, customer, or vendor data on request.

1. Log in to e7 using the appropriate credentials, and then click on the Security Module touchscreen key.

   Security Module contains more information about access and touchscreen key for the Security Module.
2. On the e7 Security window, click **Record Erasure**.

3. Use the **First Name**, **Last Name**, and **Phone Number** fields to search for the employee, customer, or vendor that requested their data be removed from the system.

   This search does not return a result set, and shows the following error message if it finds more than one matching result. You must add specificity to the search until e7 finds one matching result:

   ```
   More than 1 record available. Please provide more information.
   ```

4. Verify the search result, and then click **Delete/Anonymize**. e7 deletes or anonymizes depending on the record type:

   - `Customer`: e7 deletes all customer data from the application. This operation cannot be reversed.
   - `Vendor`: e7 does not delete the vendor record, but the application replaces the existing **Contact Person** and **Phone Number** data with anonymizing values.
   - `Employee`: e7 replaces the Personally Identifiable Information fields selected in the Restaurant configurations with anonymizing values. Configuring the Fields to Anonymize for Employee Data contains more information and instructions for changing the employee anonymization settings.

Property Management System Integration

After dining at a hotel restaurant, a customer may want the option to add the restaurant check to their hotel bill or customer account. e7 allows an employee at a workstation to access the property management system (PMS) and post a restaurant charge to the customer's folio. The PMS decides whether or not to accept the charge based on the status of the customer's account in the PMS, and then sends a message to the e7 Point-of-Sale based on the following criteria:

- If the charge is accepted, the tender is complete. Assuming the charge was for the full amount, the transaction is then closed.
- If the charge is not accepted, a denial message appears on the workstation display, and the transaction remains open.

The message sent to the PMS is:

- In un-encrypted text format.
- Contains the reference field to enter a credit card number or room number details for posting to PMS for identifying the customer folio and complete the transaction

The *Oracle Hospitality Food and Beverage Property Management System Interface Reference* contains more information about the message data.

User Consent and Notice

This release lets administrators enable requiring customer consent before e7 stores customer data. When adding a new customer through Customer Management or using the **Add New Customer** touchscreen key, e7 shows a dialog box with customizable message requiring a customer to provide consent. If the customer does not click **Yes**, e7 does not store the customer's information.

1. In the e7 Configurator, click the **Menu** drop-down list, and then click **Restaurant**.

2. Click the **Data Privacy** tab.
3. To enable requiring customer consent, select **Enable Consent**.
4. Enter the message to be shown in the dialog box in **Consent Text**.

Logging

By default, e7 Point-of-Sale:

- Saves log files in *`install_path`*`\etc\e7Log_`*`node_name`*`.log`.
- Appends new messages to a log file until reaching the default maximum file size of 64kb, and then begins another log file with the same `e7Log_`*`node_name`* name.
- Stores up to 16 log files, after which it deletes the oldest log file when beginning a new file.

You can make the following changes in *`install_path`*`\cfg\e7config.txt` to configure e7 logging:

- **Export Location**: set `<add key="LogRootDir" value="`*`target_folder_path`*`" />`

  For example, `value="C:\Users\Public\Micros\e7\etc\e7logs"`
- **Minimum Free Space Required**: set `<add key="DiskThreshold" value="`*`size_in_bytes`*`" />`

  For example, `value="1024"` to require 1 kilobyte of free space before logging can begin.
- **Maximum Space Allocated**: set `<add key="TotalLogSize" value="`*`size_in_bytes`*`" />`

  For example, `value="1048576"` to allocate a maximum of 1 megabyte of space to log files. Once the log files reach this threshold, e7 deletes the oldest file to continue logging.
- **Maximum Size for Each Log**: set `<add key="MaxLogFileSize" value="`*`size_in_bytes`*`" />`

  For example, `value="10240"` to store messages in each file until it reaches a size of 10 kilobytes. Once the log file reaches this size, e7 begins logging in a new file.

Log Verbosity

The Security Module lets employees with the correct privileges to configure the amount of detail displayed in the log files.

1. Log in to e7 using the appropriate credentials, and then click on the Security Module touchscreen key.

   Security Module contains more information about access and touchscreen key for the Security Module.
2. On the e7 Security window, click **Log Verbosity**.
3. For each module, select the **Modules** and **Verbosity**, and then click **Save**.

Viewing Logs

The Security Module lets employees with the correct privileges access a consolidated view of log files by timestamp.

1. Log in to e7 using the appropriate credentials, and then click on the Security Module touchscreen key.

   Security Module contains more information about access and touchscreen key for the Security Module.

2. On the e7 Security window, click **Log Viewer**. This shows a window with all log files except for Transaction Interface (TIF) logs and configuration logs.
3. To view TIF or configuration logs, select **TIF Logs** or **Config Logs**. By default, both options are deselected.
4. To refresh the logs, click **Refresh**. The log viewer does not automatically refresh..
5. To export the logs in a `.zip` archive, click **Export Logs**, navigate to the export location, and then click **Save**.

2

System Requirements, Supported Systems, and Compatibility

This chapter describes e7 compatibility and requirements.

Supported Credit Card Driver Hosts

Your environment must contain at least one of the following devices for hosting the credit card drivers:

Device	Operating System	Microsoft .NET Framework
PC	• Microsoft Windows 10 (32-bit and 64-bit) Oracle Hospitality Enterprise Back Office 8.5.0 and older do not support Microsoft Windows 10. If you are using e7 with Enterprise Back Office 8.5.0 or older, you must use the Electronic Transfer Account (ETA) transport mode. • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 7 Professional (32-bit and 64-bit)	• Microsoft .NET Framework 4.6 or later

Supported Workstations

The following table lists the workstations supported by e7:

Device	Operating System or Workstation Platform
Oracle MICROS Tablet R-Series • e7 does not support the concessions edition.	• Platform 1.3.1
Oracle MICROS Workstation 5A	• Platform 1.2 • Platform 1.3 for Protégé
Oracle MICROS Workstation 5	• Platform 1.3 • Platform 3.0 for Protégé

Device	Operating System or Workstation Platform
Oracle MICROS Workstation 4LX	• Platform 2.9 • Platform 4.0 for Protégé

3
Installation and Upgrade

This release contains changes that impact the installation and upgrade process. The *Oracle Hospitality e7 Point-of-Sale Installation Guide* contains instructions that must be followed when performing new installations and upgrades.

Oracle Payment Interface Driver

If you are upgrading from version 4.2.*x* or earlier, you must reconfigure the Oracle Payment Interface driver because of significant changes made in this version.

Security Requirement

If you are upgrading from version 4.2.*x* or earlier, you must generate the encryption key for securing the database. You cannot ring transactions until you generate the key and enable enhanced security.