Oracle® Hospitality RES 3700

Security Guide

Release 5.5

E76231-01

May 2016

Contents

Preface

This document provides security reference and guidance for Oracle Hospitality RES 3700.

Audience

This document is intended for administrators, developers, and system integrators who perform the following functions:

- Document specific security features and configuration details for the Oracle Hospitality RES 3700, in order to facilitate and support the secure operation of the product and any external compliance standards.
- Guide administrators, developers, and system integrators on secure product implementation, integration, and administration.

It is assumed that the readers have general knowledge of administering the underlying technologies and the 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 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

Date	Description of Change
May 2016	• Initial publication.

1 RES 3700 Security Overview

This chapter provides an overview of Oracle Hospitality RES 3700 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 RES 3700 Installation for more information.
- **Learn about and use the RES 3700 security features.** See Implementing RES 3700 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 RES 3700 Security

Oracle Hospitality RES 3700 (or RES) is an on premise client/server architecture. The POS server is a dedicated machine where the database server, supporting applications, POS middleware and infrastructure is installed and running. The POS clients run the POS Operations application, Kitchen Display application, the Configuration applications and/or the Back Office applications.

RES uses role-based access control for employees to configure the system. Employees are required to have a unique username and a password. Password complexity rules are enforced, and passwords must be changed and not repeated per specific requirements. Employee passwords are hashed using a modern and secure algorithm and stored in the RES database.

The RES database and transaction log are encrypted using AES-128. This database encryption key is derived from a generated random passphrase. This passphrase can be rotated using the Database Manager Application; it is referred to as the "Database Key".

Sensitive data stored within the database is also encrypted at the column level. This data is encrypted using AES-128. The encryption key used for this data is derived from a random passphrase. This passphrase can be rotated using the Database Manager Application; it is referred to as the “Sensitive Data Key”.

A Client Trust Passphrase must be entered at every network node (PC, workstation, RDC/KDS Display, Handheld) that is part of a RES system. This passphrase is user-defined, intended to be unique per site, it should be kept secret and known only to trusted personnel. This passphrase is entered via the Client Trust Passphrase Utility; this application is launched automatically at startup on a properly configured RES client when the client does not match the server’s Client Trust Passphrase. When the passphrase is changed at the server, existing clients will automatically get updated with the new passphrase. This passphrase is encrypted using the Microsoft Data Protection API (DPAPI) and stored in the machine’s local registry. Network nodes must have matching Client Trust Passphrases in order to communicate successfully.

Database backup files are encrypted using AES-256. The encryption key for this data is derived from the Database Restore Passphrase. This passphrase is user-defined, intended to be unique per site, it should be kept secret and known only to trusted personnel. This passphrase is entered via the Database Manager application. This passphrase is encrypted using the DPAPI and stored in the machine’s local registry.

Sensitive data transmitted on the local POS network is encrypted using RSA-2048. This encryption algorithm uses public keys at each POS client to encrypt the sensitive data and then a private key at the server to decrypt the data. These key pairs are generated using the Microsoft Crypto API. They are encrypted using the DPAPI. The public key is sent securely to the POS clients using AES-256 encryption in a session that uses a unique key which is derived from the Client Trust Passphrase.

Understanding the RES 3700 Environment

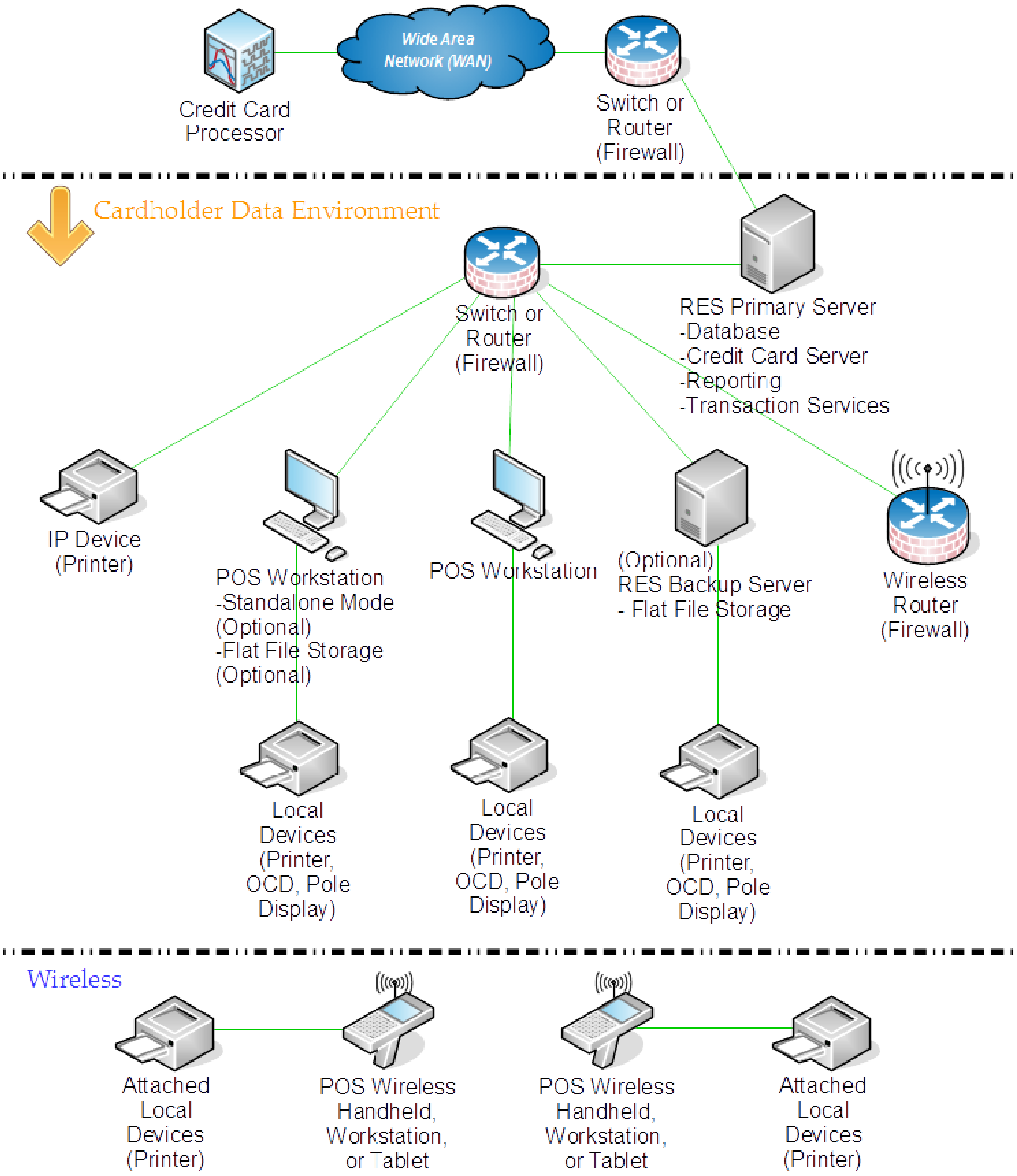
When planning your Oracle Hospitality RES 3700 implementation, consider the following:

- **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, 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 RES Primary Server should be configured with a firewall blocking inbound traffic from the public internet. The firewall should block outbound access except for what may be necessary to run your business. The most common examples of exceptions would be the URLs used for Credit Card processing, the URL used for integration with mymicros.net, other URLs for specific corporate websites.

RES Network Diagram


Credit Card Processor
Wide Area Network (WAN)
Switch or Router (Firewall)
Cardholder Data Environment
Switch or Router (Firewall)
RES Primary Server
-Database
-Credit Card Server
-Reporting
-Transaction Services
IP Device (Printer)
POS Workstation
-Standalone Mode (Optional)
-Flat File Storage (Optional)
POS Workstation
(Optional)
RES Backup Server
- Flat File Storage
Wireless Router (Firewall)
Local Devices (Printer, OCD, Pole Display)
Local Devices (Printer, OCD, Pole Display)
Local Devices (Printer, OCD, Pole Display)
Wireless
Attached Local Devices (Printer)
POS Wireless Handheld, Workstation, or Tablet
POS Wireless Handheld, Workstation, or Tablet
Attached Local Devices (Printer)

Oracle Hospitality RES 3700 Security

When installing RES 3700, see instructions in these documents:

- RES 5.0 Install Readme First
- RES 5.5 Release Note
- RES 3700 5.5 PA-DSS Implementation Guide

RES 3700 uses the following ports:

Port	**Protocol**	**Comment**
2638	TCP	SAP Sybase database Server
7300	TCP	CAL Server
7301	UDP	CAL Server
5101	TCP	Alert Manager, optional
5102	TCP	Alert Manager, optional
5103	TCP	Alert Manager, optional
80	TCP	Manager Procedures
50123	TCP	MDS Http Service
5100	TCP	Cash Management
6000	TCP	International Liquor Dispensing System
5022	TCP	KDS Display
5023	TCP	KDS Controller
7019	TCP	Caller ID Service
5021	TCP	Distributed Service Manager
23230	TCP	Stored Value Card Service
50200	TCP	Table Management Service
50201	TCP	Table Management Service

RES 3700 uses the following Microsoft Services:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- World Wide Web Publishing Service

2 Performing a Secure RES 3700 Installation

For information about installing RES 3700, see the *Oracle Hospitality RES 5.0 Install Readme First*.

Pre-Installation Configuration

On the RES 3700 Server, you must perform the following configurations.

Disable System Restore

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **System Protection** tab, click **Configure**.
4. Select **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

Your hard disk must be formatted using NTFS to perform this operation.

1. Click the **Start** button and enter `cmd` in the search field.
2. Right-click `cmd.exe` and select **Run as Administrator**.
3. Enter the command: `fsutil behavior set EncryptPagingFile 1`

   To disable encryption, enter 0 instead of 1.
4. Enter the command: `fsutil behavior query EncryptPagingFile`
5. Verify that the command prompt returns: `EncryptPagingFile = 1`

Clear the System PageFile.sys on Shutdown

You can enable the option to clear PageFile.sys on system shutdown to purge temporary data. This ensures that information such as system and application passwords and cardholder data are not inadvertently kept in the temporary files. Enabling this feature may increase the time it takes for system shutdown.

1. Click the **Start** button and enter `regedit` in the search field.
2. Right-click `regedit.exe` and select **Run as Administrator**.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
4. Right-click **ClearPageFileAtShutdown** and select **Modify**.

   If **ClearPageFileAtShutdown** does not exist, right-click the **Memory Management** folder, select **New**, and select **DWORD (32-bit) Value**.
5. Set the **Value data** field to 1 and click **OK**.

Disable System Management of PageFile.sys

1. Right-click **Computer** and select **Properties**.

2. On the System dialog box, click **Advanced system settings**.
3. On the **Advanced** tab, click **Settings for Performance**.
4. On the **Advanced** tab, click **Change**.
5. Deselect **Automatically manage page file size for all drives**, select **Custom size**, and set the following fields:
    a. **Initial Size**: the amount of Random Access Memory (RAM) available.
    b. **Maximum Size**: 2x the amount of RAM.
6. Click **OK** until you return to the System dialog box.
7. Restart the computer.

Disable Error Reporting

1. Click the **Start** button, select **Control Panel**, and then click **Action Center**.
2. Click **Change Action Center settings**, then click **Problem reporting settings**.
3. Select **Never check for solutions**, then click **OK**.

Installing RES 3700 Securely

When installing RES 3700, the setup program will prompt you for some necessary parameters. Provide them in a manner consistent with configuration you desire.

At the end of the Setup process, you will be asked for a Client Trust Passphrase. This should be a unique phase for each installation. It should be difficult to guess, but must be remembered to complete the installation at EACH client in the system.

After each client installs the software, the user is prompted to enter the Client Trust Passphrase. If this passphrase does not match the Server, then the RES Applications will not operate at the client.

Post-Installation Configuration

This section explains security configuration to complete after Oracle Hospitality RES 3700 is installed. POS Operations will not function until ALL of these steps are performed.

A privileged user must use Database Manager to perform the following:

- Change the DBA and MICROS database user passwords
- Change the Database Encryption Key (passphrase)
- Change the Sensitive Data Encryption Key (passphrase)
- Set the Transport Encryption Keys

A privileged user must use POS Configurator to perform the following:

- CA/EDC Tenders must Mask CC Account Number and Expiration Date
- Classic Security must be turned OFF
- Password Expiration must be set for 90 days or less
- Password Length must be 7 or more
- Password Repeat Interval must be 4 or more
- Password must be set to require Alpha characters
- Maximum Failed Logins must be <= 6 and not zero
- Maximum Idle Time must be <= 15 minutes and not zero

3 Implementing RES 3700 Security

Database Manager Pass Phrase Encryption and Storage

Database Manager allows you to set and change pass phrases for the Client Trust Utility and for the database. Pass phrases must follow the following complexity guidelines:

- Minimum 15 characters,
- Maximum 32 characters,
- Mixed case,
- Contain alpha and numeric and special characters

You can set, change, and perform actions using the pass phrases through the Database Manager utility or through the command line.

Client Trust Pass Phrase

When run for the first time, Database Manager prompts you to approve the Auto Discovery Mode. This allows the Client Trust Utility to allow new clients to securely download the client trust pass phrase without performing manual creation and maintenance.

Encrypted Key File

Database Manager uses AES 128/256 and a randomly-generated passphrase to store and encrypt passwords and encryption keys in the `MICROSKeyBackup.mbz5g3` key file. Database Manager generates a new encryption passphrase after every database backup, and the key file stores the passphrase and a text file named `MICROSKeyBackup.regx` containing the following encrypted passwords and keys:

- dba database password (DataS5)
- micros database password (DataS6)
- transportation public key (DataS3)
- transportation private key (DataS4)
- database encryption key (DataS1)
- sensitive data pass phrase (DataS2)

When Database Manager restores the database using the backup file, it uses the encryption passphrase to decrypt the sensitive data.

4 Security Considerations for Developers

RES 3700 is built with an industry standard relational database. This makes it possible for third party developers to create applications that access the RES database. These applications must NOT use the built-in database users, DBA and MICROS, to connect to the RES database. The RES Utility, Database Manager, can be used to create custom database users. Third party applications are responsible for managing their own password securely.

Appendix A Secure Deployment Checklist

The following security guideline checklist to help you secure RES 3700 and its components:

- Make sure the operating system is secured according to the security recommendations of the operating system security guide.
- Follow the Oracle Database Security checklist for Oracle Database installation.
- Follow the Internet Information Services (IIS) Security checklist.