Oracle® Hospitality Kitchen Display Controller 210
Security Guide

ORACLE®

Oracle Hospitality Kitchen Display Controller 210 Security Guide Release 1.0

F29161-01

Contents

Preface

Audience

This document is intended for those who set up, install, and operate the Oracle MICROS Kitchen Display Controller 210 (KDC 210). It is not specific to a particular software 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 recreate
- Exact error message received
- 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/food-beverage/

Table 1-1 Revision History

Date	Description
March 2020	Initial publication.

1

KDC 210 Security Overview

This chapter provides an overview of KDC 210 security features and explains general device security principles.

Basic Security Considerations

The following principles are fundamental to using any hardware or software securely:

- Keep software up to date. This includes software and drivers specific to the product as well as the latest patches available from 3rd party vendors.

- Limit account privileges as much as possible. Users should only be given the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.

- Install software securely. For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See Performing a Secure KDC 210 Installation for more information.

- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.

- Learn about and use the KDC 210 security features. See Implementing KDC 210 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 Oracle Critical Patch Updates and Security Alerts web site: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of KDC 210 Security

The KDC 210 incorporates a mixture of hardware and software components commonly found in PC-based devices. For peripherals connectivity, both industry standard ports have been integrated on-board.

Table 1-1 KDC 210 Hardware Component Overview

Processor	Intel® Atom™ Quad Core, 1.44GHz (up to 1.92GHz)
RAM	4GB
OS	Windows 10 IoT Enterprise, Oracle Linux for MICROS
Display Resolution	Up to 1920x1080
Network Interface	10/100/1G Base T LAN
Peripheral Ports	3x USB, 1x DisplayPort, 1x High Definition 2nd Display Output Connector, 1x Com Port, 1x Audio Line Out
UAC/DC Adapter	Input: 100 – 240V AC; Output: 12V DC, 5.0A
Fanless Enclosure	Aluminum and steel
Dimensions and Weight	1.4 x 5.5 x 5.1 in/ 35 x 140 x 130 mm 0.88 lbs/400 g
Temperature and Humidity	Operation: 0°C – 40°C; Storage: -20°C – 60°C Humidity: 0% – 90% non-condensing

Table 1-2 KDC 210 Software Architecture Overview

Operating System	Microsoft Windows 10 IoT Enterprise (64-bit only), Oracle Linux for MICROS
Boot Firmware	InsydeH2O® Setup Utility (UEFI BIOS)

Understanding the KDC 210 Environment

When planning your KDC 210 implementation, consider the following:

- Which resources must be protected?

- You must restrict access to external ports, such as USB ports or serial ports.

- You must protect customer data, such as credit card numbers.

- You must protect internal data, such as proprietary source code.

- You must 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 a strategic resource 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.

Physical Security

The KDC 210 is installed in environments where physical access to the devices can be difficult or impossible to control. It is typically installed in publicly accessible areas based on optimal usage for employees rather than secured computer rooms.

Factory UEFI Firmware Settings

The UEFI Firmware provides several security settings that are not enabled or configured securely by default. For a secure configuration, you must create installation environment-specific settings, such as passwords. The following settings are available in the firmware and should be enabled/configured during the installation:

- Secure Boot
- Supervisor Password

The UEFI firmware will enable the following ports by default:

- USB Ports 1-3

Factory Microsoft Windows Installation Settings

The factory operating system installation includes several changes to settings, policies, and services that are installed by default in Windows. The following items have modified from the defaults in order to improve operating system security out of the box:

- Local Security Policy modifications
    - o Enabled clear pagefile at shutdown
    - o Disabled Internet Explorer legacy TLS and SSL protocols
    - o Enabled Windows Update auto-install daily at 3:00AM
    - o Default Administrative shares removed
    - o Disabled the default lock screen
    - o Disabled password entry on Wake
- Windows Applications/Services modifications
    - o Windows store uninstalled
    - o Internet Information Services uninstalled
    - o Homegroup Provider disabled
    - o Windows Media Services disabled
    - o UPnP disabled
    - o Autoplay disabled
    - o WifiSense disabled
    - o OneDrive disabled
    - o Auto Defragment drives disabled

User Accounts in Factory Installations

The preinstalled factory operating system should not contain any default user accounts or passwords. During the first boot, you must create an administrative user account and provide a password. Administrative users should not be used for day-to-day operation of the device.

Windows Defender and Windows Firewall in the Factory Installations

Windows Defender and Windows Firewall are provided in the factory operating system installation for all configurations of the KDC 210. The definitions are updated with the current version available at the time the factory operating system was created.

Factory Recovery

The KDC 210 can be restored to its out-of-box state using a recovery routine. In situations where the device or its operating system is believed to be compromised, this feature can be used to quickly restore the operating system to the factory settings. **Note that performing a system recovery removes all data and the current operating system.**

2
Performing a Secure KDC 210 Installation

This chapter presents planning information and basic guidance for your KDC 210 installation. Consult your IT Security Officer for any security decisions or requirements that pertain to your operating environment.

Pre-Installation Security

- Review a network diagram for the installation environment. Verify the device will only be installed on secured networks behind a hardware firewall.

- Determine how the device will be physically secured. Wall or cabinetry mounts may need to be installed in order to physically secure the device.

- **Microsoft Windows**: Determine out of box operating system security settings. Some information is required for Windows out-of-box setup. The first boot requires configuring an administrative account, network connection settings, and the computer name.

- **Oracle Linux for MICROS**: When migrating from Microsoft Windows to Oracle Linux for MICROS, information is required to complete the operating system setup. Oracle Linux for MICROS setup requires configuring a super user account with a user-configurable password, network connection settings, and the computer name.

Installing the KDC 210 Securely

Physically Securing the Device

To maximize the time and complexity involved for an attacker to physically access the device, do not install the KDC 210 in easily accessible common areas. In addition, do not operate the KDC 210 with its housing disassembled.

Microsoft Windows Out-of-Box Setup

The first time the device is booted, the Windows Out-of-Box Experience will launch in order to capture operating system configuration information including user accounts, computer name, and network connection settings.

General guidance for Microsoft Windows out-of-box setup:

- **Selecting a network connection.**
  Only connect to secure networks. Networks using older key exchange protocols, such as WEP, are not secure.

- **Choose to Customize Settings.**
  The Windows Express installation settings are convenient but may enable

unnecessary operating system features for the use case of the device. Features such as WifiSense or Location Services are examples of settings that are configurable using these setup screens.

- **Creating an account for the PC.**
  The initial user created by Windows Setup will have administrative privileges in the system. Avoid choosing user names that leak information, such as the privilege level. Use complex passwords for all Administrative and Standard user accounts.

- **Computer Name.**
  The default computer name supplied by Windows Setup is randomly generated. In some cases, this naming scheme will be undesirable. When changing the computer name of the device, avoid choosing a computer name that leaks information about device. For example, Windows10POSTerminal1 allows an attacker with network access to immediately determine the operating system version and the purpose of the device.

Oracle Linux for MICROS Setup

The first time the device is booted, the Oracle Linux for MICROS setup process begins. This setup requires configuration information including Support user account name and network connection settings.

General guidance for Oracle Linux for MICROS:

- **Creating a Support user account name and password.**
  The Oracle Linux for MICROS installation process provides instructions for naming Support user accounts. For the Support user account password, use complex passwords.

- **Selecting a network connection.**
  Only connect to secure networks.

- **Configure Network Settings.**
  Oracle Linux for MICROS setup does not automatically name the device. Avoid choosing a computer name that leaks information about device. For example, Linux10POSTerminal2 allows an attacker with network access to immediately determine the operating system version and the purpose of the device.

- Oracle Linux provides firewall protection for both inbound and outbound traffic. Only select ports for transmitting data in/out are open; all other ports are closed.

3

Implementing KDC 210 Security

Physical Security

- Regularly inspect that physical security controls, such as covers and screws, are present.

- Regularly inspect the device and its peripherals for signs of tampering.

- Regularly inspect the device for any unusual devices that have been attached to the workstation.

UEFI Firmware Security

- **Set a Supervisor Password.**
  A supervisor password will prevent unauthorized access to the UEFI firmware setup and configuration user interface. This ensures that only authorized users can modify any settings configured after the installation. Users will have three attempts at keying the correct password. After three failed attempts to enter the supervisor password, entry to the UEFI setup will become locked.

  If the supervisor password is forgotten or lost, it cannot be recovered or cleared. If further UEFI setup changes need to be made, the device must be repaired by a qualified Oracle repair facility.

- **Enable secure boot.**
  Secure boot is an effective defense against low-level malware that attacks the boot code used to start the operating system. Malware at this level can remain completely undetected by some security software installed at the operating system level, and cannot be easily removed.

  A firmware supervisor password is required to enable secure boot. If enabling a supervisor password is undesired, set the password temporarily to enable secure boot. Once secure boot has been enabled, the password can be cleared (not recommended) as long as the current password is known.

- **Set a HDD Password.**
  A hard drive password will prevent unauthorized access to a bootable hard drive. This ensures that only authorized users can boot the password protected drive after the installation. Users will have three attempts at keying the correct password. After three failed attempts to enter the HDD password, the HDD will become permanently locked.

  If the HDD password is forgotten or lost, it cannot be recovered or cleared. If further UEFI setup changes need to be made, the device must be repaired by a qualified Oracle repair facility.

- **Disable unused USB Ports.** Disabling the USB ports on the device can be an effective defense against attempts to install malware or hardware components used to gain access to the device.

  See the *Configuring System Security Settings* section of the *Oracle MICROS Kitchen Display Controller 210 Setup Guide* for information about security settings.

Microsoft Windows 10 IoT Enterprise 64-bit Operating System Security

- **Drive Encryption.**
  Drive encryption can protect data stored on the hard drive when physical security controls have failed. The KDC 210 ships with Microsoft Windows 10 IoT Enterprise, which supports Bitlocker drive encryption.

- **Application Whitelisting.**
  Application whitelisting allows administrators to define the applications permitted to run on the device. The KDC 210 ships with Microsoft Windows 10 IoT Enterprise, which supports the AppLocker feature.

Refer to the vendor documentation for operating system security information and features.

- Windows 10 IoT Enterprise Edition Security Features:
  https://docs.microsoft.com/en-us/windows/security/

Oracle Linux for MICROS Operating System Security

Refer to the vendor documentation for operating system security information and features.

- Oracle Linux 7.x Security Guide:
  https://docs.oracle.com/cd/E52668_01/E54670/html/index.html

- Oracle Linux Security page:
  https://linux.oracle.com/security/

Additional Reference Documents

The following documents provide standards and additional guidance for operating system hardening and maintaining a secure operating system environment:

- PCI DSS

  https://www.pcisecuritystandards.org/security_standards/index.php

- Center for Internet Security (CIS) Benchmarks (used for OS hardening)
  https://benchmarks.cisecurity.org/downloads/multiform/

4

Secure Deployment Checklist

The following security checklist includes guidelines that help secure your device:

- Ensure the device is physically and securely mounted to a stationary object.
- Ensure all covers and security screws are installed.
- Monitor system access.
- Use Secure Boot.
- Disable unused external I/O ports.
- Enforce access controls effectively.
  - Lock and expire default or temporary user accounts used during installation.
  - Enforce password management.
  - Practice the principle of least privilege.
  - Grant necessary privileges only.
  - Do not use administrator accounts for daily operations.
  - Ensure unnecessary network shares have been removed.
- Only install system components required for the use case.
- Ensure remote access software has been disabled.
- Use a firewall to restrict network access.
- Use malware protection software.
- Use drive encryption to protect data at rest.
- Ensure the system receives operating system updates automatically.
- Ensure the system receives virus definition updates automatically.