Oracle® MICROS Express Station 4 Series

Security Guide

Release 1.0
F34934-03
November 2021

Oracle Hospitality Express Station 4 Series Security Guide Release 1.0

F34934-03

Copyright © 2020, 2021 Oracle and/or its affiliates.

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

Audience

This document is intended for those who set up, install, and operate the Oracle MICROS Express Station 4 Series. 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
September 2020	Initial publication
October 2020	Added Express Station 410

1

Express Station 4 Series Security Overview

This chapter provides an overview of Express Station 4 Series 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 Express Station 4 Series 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 Express Station 4 Series security features. See Implementing Express Station 4 Series 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 Express Station 4 Series Security

The Express Station 4 Series terminals are devices that incorporate a mixture of hardware and software components commonly found in PC-based devices. For peripherals connectivity, both industry standard and Oracle MICROS proprietary ports have been integrated on-board.

Table 1-1 Express Station 4 Series Hardware Component Overview

Processor	Intel Atom x5 Dual Core Processor (Express Station 400) / Quad-Core Processors (Express Station 410)
TPM	Intel Platform Trust Technology (TCG 2.0 compliant)
Storage	64 GB SATA 3.0 SSD (Express Station 400) / 128 GB SATA 3.0 SSD (Express Station 410)
Magnetic Stripe Reader (optional)	• Modular Integrated 3-Track Magnetic Stripe Reader; Capable of Hardware Encryption at the Swipe • Triple Data Encryption (TDES/3DES or AES algorithm • Derived Unique Key per Transaction (DUKPT) key rotation algorithm • Merchant Link encryption key pre-injected
RFID (optional)	(Express Station 410)
Network	10/100/1G RJ45 Ethernet
USB	5 Total: • 2 USB • 3 High-speed USB
Serial Ports	2 Total: • 1 - RJ45 RS232 Powered (0/5/9/12V Powered) • 1 - RJ45 RS422/RS232 IDN

Table 1-2 Express Station 4 Series Software Architecture Overview

Operating System	Two configurations available: • Microsoft Windows 10 IoT Enterprise (64-bit only) • Oracle Linux for MICROS
Boot Firmware	UEFI - SecureCore Technology (SCT 4.0) for Intel Apollo Lake-I platform Release: 4.0.1.765

Understanding the Express Station 4 Series Environment

When planning your Express Station 4 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

Point of Sale terminals are installed in environments where physical access to the devices can be difficult or impossible to control. The devices are typically installed in publicly accessible areas based on optimal usage for employees rather than secured computer rooms.

All Express Station 4 Series configurations incorporate mechanical design features that can mitigate physical security risks. Security screws have been provided for each removable cover and for all available mounting options. These features cannot prevent all physical intrusions, but they can increase the time and complexity involved in gaining access to the device.

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
- Hard Drive Password

The UEFI firmware will enable the following hardware devices by default:

- USB Ports 1 – 5

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
    - Enabled clear pagefile at shutdown
    - Disabled Internet Explorer legacy TLS and SSL protocols
- Windows Applications/Services modifications
    - Windows store uninstalled

    - Internet Information Services uninstalled
    - Homegroup Provider disabled
    - Windows Media Services disabled
    - UPnP disabled
    - Autoplay disabled
    - WifiSense disabled
- Network Shares
    - Default Administrative shares removed

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 Express Station 4 Series.The definitions are updated with the current version available at the time the factory operating system was created.

Factory Recovery

All Express Station 4 configurations include a built-in factory recovery feature. The recovery operating system resides on a primary disk, so no additional installation media is required. 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 the factory recovery feature will wipe the contents of the operating system partition.**

2

Performing a Secure Express Station 4 Series Installation

This chapter presents planning information and basic guidance for your Express Station 4 Series installation. Please consult your IT Security Officer for any security decisions or requirements that pertain to your operating environment.

Pre-Installation Security

- Review the Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide if the wireless add-on card will be installed.
- 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 Express Station 4 Series Securely

Physically Securing the Device

The *Oracle MICROS Express Station 4 Series Setup Guide* provides detailed instructions for securely assembling the device. To maximize the time and complexity involved for an attacker to physically access the device, install the security screws on all removable covers and mounting configurations. The Oracle MICROS *Express Station 4 Series Setup* Guide provides detailed instructions for securely assembling and installing the device.

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 wireless 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 Express Station 4 Series Security

Physical Security

- Regularly inspect that physical security controls, such as covers and screws, are present.
- Regularly inspect the Express Station and its peripherals for signs of tampering.
- Regularly inspect the device for any unusual devices that have been attached to the Express Station.

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.

  See the *Configuring System Security Settings* sections of the *Oracle MICROS Express Station 4 Series Setup Guide* for information on enabling this setting.
- **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. All models of the Express Station 4 Series support the secure boot feature.

  See the *Configuring System Security Settings* sections of the *Oracle MICROS Express Station 4 Series Setup Guide* for information on enabling this setting.

  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.

See the *Configuring System Security Settings* section of the *Oracle MICROS Express Station 4 Series Setup Guide* for information on enabling this setting.

- **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. When USB ports are disabled through UEFI firmware on the Express Station 4 Series devices, the respective port will not supply power to attached USB peripherals.

  See the *Configuring Express Station Settings* section of the *Oracle MICROS Express Station 4 Series Setup Guide* for information on enabling these settings.

Operating System Security

- **Drive Encryption.**
  Drive encryption can protect data stored on the hard drive when physical security controls have failed. Microsoft Windows-based Express Station 4 Series models support Bitlocker drive encryption.
- **Application Whitelisting.**
  Application whitelisting allows administrators to define the applications permitted to run on the device. All models of the Express Station 4 Series come with versions of Microsoft Windows that support 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 7.x Security Guide:
  https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/
- 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 Express Station 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.