Oracle® MICROS Edge Controller 2 Series

Security Guide

Release 1.0
F52702-02
March 2022

Oracle® MICROS Edge Controller 2 Series Security Guide Release 1.0

F52702-02

Oracle Legal Notices

Copyright Notice

License Restrictions Warranty/Consequential Damages Disclaimer

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.

Warranty Disclaimer

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.

Restricted Rights Notice

If this is software or related documentation that 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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Hazardous Applications Notice

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.

Trademark Notice

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information,
visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or
visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired, 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 Oracle MICROS Edge Controller 2 Series devices.

The Edge Controller 2 Series includes the following devices:

- Oracle MICROS Edge Controller 250 (EC250)

Note: This document 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 Food & Beverage 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 2022	Initial publication.

1 Edge Controller 2 Series Security Overview

This chapter provides an overview of Edge Controller 2 Series security features and explains general device security principles.

The Edge Controller 2 Series includes the following devices:

- Oracle MICROS Edge Controller 250 (EC250)

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 EC250 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 EC250 security features. See Implementing EC250 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 EC250 Security

The EC250 incorporates a mixture of hardware and software components commonly found in PC-based devices. For peripherals connectivity, industry standard ports have been integrated on-board.

Table 1-1 EC250 Hardware Component Overview

Processor	Intel® Core i5 processor
RAM	16GB
Display Resolution	Up to 1920x1080
Network Interface	10/100/1000MB Base-T LAN
Peripheral Ports	4x USB 3.0, 1x DisplayPort, 2x HDMI, 3x Com Port, 1x 3.5mm audio jack, 2x Ethernet,
UAC/DC Adapter	Input: 100 – 240V AC; Output: 12V DC, 5.0A
Fanless Enclosure	Aluminum alloy
Dimensions and Weight	8 x 1.7 x 9.1 in/ 202 x 43.5 x 232 mm 4.6 lb / 2.1 kg (without the tabletop stand)
Temperature and Humidity	Operation: -10°C to 50°C (14°F to 122°F); Storage: -20°C to 60°C (-4°F to 140°F)

Table 1-2 EC250 Software Architecture Overview

Operating System	Microsoft Windows 10 Enterprise LTSC (64-bit only)
Boot Firmware	InsydeH2O® Setup Utility (UEFI BIOS)

Understanding the EC250 Environment

When planning your EC250 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 EC250 would typically be installed in secured computer rooms.

Factory UEFI Firmware Settings

The UEFI Firmware provides several security settings. 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 is enabled by default
- Supervisor Password is not set
- Hdd passwords are not set
- TPM is disabled by default
- USB boot is disabled by default

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
    - TLS 1.2 is enabled.
    - Enabled Windows Update auto-install daily at 3:00AM
    - Default Administrative shares removed
    - Disabled the default lock screen
    - Disabled password entry on Wake
- Windows Applications/Services modifications
    - Windows store uninstalled
    - Internet Information Services uninstalled
    - Homegroup Provider disabled
    - Windows Media Services disabled
    - UPnP disabled
    - Autoplay disabled
    - OneDrive disabled
    - 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 EC250. The definitions are updated with the current version available at the time the factory operating system was created.

Factory Recovery

The EC250 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.**

Steps to Restore OS:

1. Power on EC250 by pressing the power button for 1 full second.
2. Select the “OS Restore” option that will appear for approximately 3 seconds.

2

Performing a Secure EC250 Installation

This chapter presents planning information and basic guidance for your EC250 installation. Consult your IT Security Officer for any security decisions or requirements that pertain to your operating environment.

Preinstallation 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.

Installing the EC250 Securely

Physically Securing the Device

To maximize the time and complexity involved for an attacker to physically access the device, do not install the EC250 in easily accessible common areas. In addition, do not operate the EC250 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.
- **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.

3 Implementing EC250 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. NOTE: Secure Boot is enabled by default.**
  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. This can be accomplished in Windows 10 Device Manager under Universal Serial Bus Controller.

Microsoft Windows 10 Enterprise LTSC 64-bit Operating System Security

- **Drive Encryption.**
  Drive encryption can protect data stored on the hard drive when physical security controls have failed. The EC250 ships with Microsoft Windows 10 Enterprise, which supports Bitlocker drive encryption.
- **Application Whitelisting.**
  Application whitelisting allows administrators to define the applications permitted to run on the device. The EC250 ships with Microsoft Windows 10 Enterprise LTSC, which supports the AppLocker feature.

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

- Windows 10 Enterprise Edition Security Features:
  https://docs.microsoft.com/en-us/windows/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.(**NOTE**: Ports can be disabled/enabled via Windows Device Manager.)
- 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.