

Oracle® Java ME Embedded

Reference Platform Release Notes (Intel Galileo Gen2)

Release 8.3 Developer Preview

E71183-01

April 2016

This document provides release information for Oracle Java ME Embedded Release 8.3 for the Reference Platform (Intel Galileo Gen2).

It contains the following sections:

- [Introduction](#)
- [What's Supported in This Release](#)
- [Usage Notes](#)
- [Installation and Runtime Security Guidelines](#)
- [Known Bugs](#)
- [Product Documentation](#)

Introduction

The Oracle Java ME Embedded release 8.3 software for the Intel Galileo Gen2 platform is a ready-to-run binary for use with an Intel Galileo Gen2 board. See the [Usage Notes](#) for more details.

The Oracle Java ME Embedded software uses an optimized platform stack for small embedded devices, which includes the Connected Limited Device Configuration (CLDC) HotSpot Implementation (Java Virtual Machine) version 8, the Micro Edition Embedded Profile (MEEP) application environment, the Generic Connection Framework (GCF) API, and enhanced support for various Java Specification Requests (JSRs).

What's Supported in This Release

The following features are included in the Oracle Java ME Embedded software on the Intel Galileo Gen2 platform:

- OS Yocto Linux v2.1
- CLDC 8 (JSR 360)
 - Full API set including MVM support
- General Connection Framework (GCF) 8

ORACLE CONFIDENTIAL

For authorized use only.

Do not distribute to third parties.

ORACLE®

- File protocol (file: scheme)
- Datagram (datagram: scheme)
- TCP/IP client socket (socket: scheme)
- TCP/IP server socket (socket: scheme)
- Secure client socket (ssl: scheme)
- HTTP (http: scheme)
- HTTPS (https: scheme)
- Secure datagram (dtls: scheme)
- Secure server socket (ssl: scheme)
- Access points
- The `NetworkUtilities` class
- `javax.microedition.pki` package and other security-related enhancements
- TLS v1, v1.1, v1.2
- Java ME Embedded Profile (MEEP) 8:
 - `javax.microedition.event`
 - `javax.microedition.power`
 - `javax.microedition.io` (IMC, PushRegistry)
 - `javax.microedition.midlet`
 - `javax.microedition.rms`
 - `javax.microedition.swm`
- Device I/O APIs, which provide enhanced device controls and improved input/output (I/O) for small embedded devices:
 - General-purpose input/output (GPIO)
 - Inter-Integrated Circuit (I2C)
 - Serial Peripheral Interface (SPI)
 - Universal Asynchronous Receiver/Transmitter (UART)
 - Watchdog Timer
- Ongoing support for the following optional packages:
 - JSR 172 - Web Services
 - JSR 177 - Security and Trust Services API (SATSA-CRYPTO package only)

- JSR 280 - XML API for Java ME
- Tooling includes:
 - Command-line interface (CLI)
 - Logging
 - File system commands
 - Debugging
- Memory monitoring is fully supported in this release and provides:
 - Contents of the Java heap
 - A call context for each object at its creation
- CPU profiling is fully enabled in this release and provides:
 - A way to identify bottlenecks in applications
 - The following data for each method: an execution duration, exact number of calls, and a method context
- Network monitoring support

Usage Notes

The Oracle Java ME Embedded software for the reference board platform includes an CLDC implementation with a high-performance Java Virtual Machine that can run IMlets and access input/output ports. This runtime is optimized for the reference board platform.

Getting Started Guide for the Reference Platform (Intel Galileo Gen2) describes how to install the Yocto Linux operating system and Oracle Java ME Embedded 8.3 distribution on the SD card, how to connect to the board from the development host computer, and how to install, run, and debug IMlets on the board.

Note the following important information before running the Oracle Java ME Embedded software on the Intel Galileo Gen2 board:

- This release does not support running multiple instances of its executable; avoid simultaneously starting several instances of any of scripts or executable files, regardless of whether these are from the same installation of the software or from different installations. The software can run multiple IMlets in the same instance of a virtual machine; you do not need to start multiple VMs to run several applications at a time. Not following this precaution can result in malfunctions with uninformative error messages and might cause corruption of the installation files.
- No generic device is implemented, as would be accessed using the package `jdk.dio.generic`.
- Access points are one-to-one mapped to network interfaces. However, the access point management functionality is implemented with a limitation which does not

allow to change the state of the Linux network interface from Java. The state can only be read. The proxy setting is also available through an environment variable.

Installation and Runtime Security Guidelines

The Oracle Java ME Embedded release 8.3 software installation requires an execution model that ensures certain networked resources available. These required resources might include, but are not limited to, a variety of communication capabilities between the product's installed components.

It is important to note that the product's installation and runtime system is fundamentally a developer system that is not specifically designed to guard against malicious attacks from outside intruders. Given this, the product's architecture can present an insecure operating environment to the installation file system and its runtime environment, during execution. For this reason, it is critically important to observe the precautions outlined in the following security guidelines when installing and running the software.

Note:

The security-related functionality of a final developed application for release into the field is supported by the available components of the Oracle Java ME Embedded software stack incorporated by the developer into the application. The security precautions required by applications in the field are beyond the scope of these recommendations, but must be observed by the application developer.

To maintain optimum network security, the software package can be installed and run in a *closed* network operating environment; the software system that is not connected directly to the Internet or to a company intranet environment that could introduce unwanted exposure to malicious intrusion. This is the ideal secure operating environment whenever the application under development does not require an Internet connection.

When the application under development requires an Internet connection, you must conform to the guidelines highlighted in [Protecting Operating Environment From Malicious Intrusion](#).

Protecting Operating Environment From Malicious Intrusion

If the operating environment is open to network access, you must observe the following precautions to protect valuable resources from malicious intrusion:

- Locate the development environment behind a secure firewall that strictly limits unauthorized network access to its file system and services. Limit access privileges to those that are required for development while allowing all the bidirectional local network communications that are necessary for the application's functionality. The firewall configuration must support these requirements to run the software while also addressing them from a security standpoint.
- Follow the principle of least privilege by assigning the minimum set of system access permissions required for installation and execution of the software.

- Do not store any sensitive information on the same file system that hosts the installation.
- Ensure that the operating system patches are up-to-date on host machines in the development environment.

Handling Security Certificate Precautions

The Oracle Java ME Embedded software distribution bundle contains security certificates that are needed for testing during development of products for final release to customers. Some of these certificates are self-signed security certificates generated by Oracle that are mapped to privileged security domains. IMlets or MIDlets signed by these certificates get high privileges to access restricted APIs; these certificates present a security vulnerability if they are released to end users on a customer's device. Other certificates issued by universally recognized certificate authorities (CAs) are used only for signature verification and they do not present a vulnerability.

After final testing of the product is completed and the product is being prepared for release to end users, you must remove self-signed security certificates that present a security vulnerability.

Developer Agent Precautions

The CLI is incorporated in the Developer Agent, which communicates with a device through an unsecured protocol. The Developer Agent is a Java SE application that can be reverse engineered to tamper with or to get information about the communication protocol, which might be used by an untrusted entity to manipulate the device. If you decide to implement the Developer Agent in a product deployment, it is your responsibility to incorporate adequate security measures around the Developer Agent communication channel. This channel uses TCP port 2201 on the Raspberry Pi device for the communication.

Known Bugs

For generic bugs in this release of the Oracle Java ME SDK that might affect the Intel Galileo Gen2 platform, see [Oracle Java ME Software Development Kit Release Notes](#).

At the time of release no bugs are found in the Oracle Java ME Embedded 8.3 software for the Reference Platform (Intel Galileo Gen2).

Product Documentation

The following documentation is included with this release of the Oracle Java ME Embedded software. See <http://docs.oracle.com/javame/>.

Application	Title	Format
All (this document)	<i>Reference Platform Release Notes (Intel Galileo Gen2)</i>	HTML PDF ePub Mobi
Demonstrates how to install, run, and troubleshoot the Oracle Java ME Embedded software on the Raspberry Pi platform.	<i>Getting Started Guide for the Reference Platform (Intel Galileo Gen2)</i>	HTML PDF ePub Mobi

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

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 is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, 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.

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.