Oracle® Java ME Embedded

Windows Platform Release Notes

Release 3.2

E36309-01

September 2012

Table of Contents

Introduction

The Oracle® Java ME Embedded software is an optimized platform stack for small embedded devices, which includes the Connected Limited Device Configuration (CLDC) HotSpot Implementation (Java Virtual Machine), Information Module Profile - New Generation (IMP-NG) application environment, and enhanced support for a reduced set of optional package functionalities through compatible Java Specification Requests (JSRs).

The following new features are included in the Oracle® Java ME Embedded software:

- Ongoing support for the following JSRs:
  - JSR 139 CLDC 1.1
  - JSR 228 IMP-NG
  - JSR 75 FileConnection APIs
  - JSR 120 Wireless Messaging API (WMA) 1.0
  - JSR 172 Web Services
  - JSR 177 Security and Trust Services
  - JSR 179 Location 1.0
  - JSR 280 XML API for Java ME

Usage Notes

The Oracle® Java ME Embedded software for the Windows Platform includes an IMP-NG emulator with a high-performance Java virtual machine that can run IMlets and simulate input-output ports of an embedded device.

The *Getting Started Guide for the Windows 32 Platform* describes how to install and run the emulator on the development host computer.

Installation and Runtime Security Guidelines

The Oracle® Java ME Embedded software requires an execution model that makes certain networked resources available for device emulator execution. These required resources might include, but are not limited to, a variety of communication capabilities between the product's installed components. It is extremely important to note that the product's installation and runtime system is fundamentally a developer system that is not specifically designed to guard against any malicious attacks from outside intruders. Given this, the product's architecture can present an insecure operating environment to the installation file system itself, as well as 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 nonetheless 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, meaning the software system 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 when it is possible. Running the development environment does not necessarily require an “Intranet” connection that supports network connections to systems outside the development architecture to intra-company resources.

An example of a requirement for an Internet connection is when the system must run wireless functionality that requires a connection to the Internet to support the communications with a wireless network infrastructure that is part of the Java ME application execution process under development. Whether or not an Internet connection is required depends on the particular Java ME application running in the development environment. For example, some Java ME applications can use an HTTP connection. In any case, if the environment is open to any 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 bi-directional 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 data sensitive information on the same file system that is hosting the installation.
- To maintain the maximum level of security, make sure the operating system patches are up-to-date on any host machines in the development environment.

Security Certificate Precautions

The Oracle® Java ME Embedded distribution bundle contains security certificates that are needed for testing purposes 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. MIDlets signed by these certificates get high privileges to access restricted APIs, and so these certificates present a security vulnerability if they are released to end users on a customer's device. Care should be taken to remove these certificates after final testing of the product is completed when the product is being prepared for release to end users. This does not apply to certificates issued by universally recognized certificate authorities (CAs), because these are used only for signature verification and do not present a vulnerability.

Command-Line Interface Precautions

The command-line interface (CLI) feature in this Oracle Java ME Embedded release is provided only as a concept for your reference. It uses insecure connections with no encryption or authentication or authorization. If you decide to implement this feature in any product deployment, it is your responsibility to incorporate adequate security measures around the CLI.

Known Bugs

The following are known bugs in this release of the Oracle Java Wireless Client software:

Table 1 Known Bugs

Bug Number	Bug Description
MERT-1907	The CPU and memory profiler have been postponed to the next release.
MERT-2024	Trying to stop an IMlet from the command line immediately after the IMlet is started may fail. Workaround: ■ It takes some time for an IMlet to start running. If a user tries to stop an IMlet before it starts running the stop command will fail. ■ Wait a few seconds after starting an IMlet before trying to stop it.
MERT-2081	When an uncaught exception occurs in an IMlet, the IMlet terminates and it is restarted automatically. However, when an exception occurs in a thread of an IMlet, the thread terminates but the IMlet does not.

Product Documentation

The following documentation is included with this release of the Oracle® Java ME Embedded. Click on the Format to open in a browser.

Application	Title	Format
All (This document)	*Release Notes*	HTML
Introduction to running Oracle® Java ME Embedded software on Win32	*Getting Started for the Windows 32 Platform*	PDF HTML

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 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.

Oracle® Java ME Embedded, Windows Platform Release Notes, Release 3.2
E36309-01