CONVERSANT® System

Release 9.0

J2SE Runtime Environment (JRE)

Upgrade Procedures

Comcode: 700282007
Document number: 585-310-329
Issue 1.0
Publication Date: June 2003

© 2003, Avaya Inc.
All Rights Reserved

Notice
Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Preventing Toll Fraud
“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention
If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1 800 643 2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com

Click on Support, then click on Escalation Lists US and International. This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, click on Global Escalation List.

Providing Telecommunications Security
Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's “telecommunications equipment” includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, “networked equipment”).

An “outside party” is anyone who is not a corporate employee, agent, subcontractor, or working on your company's behalf. Whereas, a “malicious party” is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Your Responsibility for Your Company's Telecommunications Security
The final responsibility for securing both this system and its networked equipment rests with you - an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

your Avaya-provided telecommunications systems and their interfaces

your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces

any other equipment networked to your Avaya products.

Trademarks
CONVERSANT and Intuity are registered trademarks of Avaya, Inc.

ORACLE is a registered trademark of Oracle Corporation.

Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-242-2121 in the United States and Canada. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com

Click on Support, then select Escalation Management. This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, select on International Services.

Acknowledgment
This document was written by the CRM Information Development group.

CONVERSANT R9 JRE Upgrade Procedures
Contents

Introduction 5

- **Requirements for the upgrade** 6
- **Checking for RFU+A on your system** 7

Upgrading JRE 9

- **Decompressing the JRE upgrade file** 10
- **Contents of the JRE upgrade software** 11
- **Installing the JRE upgrade software** 12
- **Fixing links to remote Oracle servers** 15

Introduction

This document describes the process for upgrading to J2SE Runtime Environment (JRE) version 1.3.1 for CONVERSANT System Release 9.0 or Version 8.0 with Remote Field Update A (RFU+A).

This upgrade to the JRE software improves the overall performance of Java processes running on the CONVERSANT system and is required to resolve a CPU bottleneck problem that some systems experience.

This section includes the following topics:

- Requirements for the upgrade on page 6
- Checking for RFU+A on your system on page 7

Requirements for the upgrade

The JRE upgrade software requires

- CONVERSANT System Release 9.0
- CONVERSANT System Version 8.0 with Remote Field Update A (RFU+A).

If you have Version 8.0, you may need to check your system to determine if RFU+A has been installed. See Checking for RFU+A on your system on page 7 for more information. If you need to install RFU+A, contact Avaya.

- In the United States: call 1-800-242-2121.
- For international support, go to http://support.avaya.com, select **Escalation Management** > **International Services** for regional contact information.

Checking for RFU+A on your system

The indication of RFU+A on your system is the presence of the UnixWare Release 7.1.1 Maintenance Pack 1 (the uw711m1 package), which is a part of RFU+A.

To check for RFU+A on your system:

1. On the CONVERSANT system, log in as root.
2. Enter **pkginfo -l uw711m1**

   If RFU+A is on the system, the system displays the following message indicating that the uw711m1 package has been installed:

```
   PKGINST:  uw711m1
      NAME:  UnixWare 7.1.1 , Release 7.1.1 Maintenance Pack 1
  CATEGORY:  patch
      ARCH:  IA32
   VERSION:  7.1.1
   BASEDIR:  /
    VENDOR:  Caldera International, Inc.
    PSTAMP:  uw711m1 03/11/2002 bl2
  INSTDATE:  Oct 12 2002 05:03 AM
    STATUS:  completely installed
     FILES:    371 installed pathnames
               356 shared pathnames
                26 linked files
                14 symbolic links
                 2 directories
               187 executables
                29 setuid/setgid executables
             44336 blocks used (22168K)(approx)
```

   If RFU+A is not on your system, the system displays the following messages indicating that the uw711m1 package is not installed:

```
UX:pkginfo: ERROR: information for "uw711m1" was not found
```

Upgrading JRE

The JRE upgrade software is available from Avaya on CD or as a downloadable file. The downloadable file is compressed and contains the same software packages as the CD. This section describes how to upgrade JRE using both the CD and the downloadable file.

Note:
The preferred method of upgrading JRE is to use the downloadable file.

This section includes the following topics:

- Decompressing the JRE upgrade file on page 10
- Contents of the JRE upgrade software on page 11
- Installing the JRE upgrade software on page 12
- Fixing links to remote Oracle servers on page 15

Decompressing the JRE upgrade file

The JRE upgrade software is available on a CD or as a downloable file. If you are using the downloadable file, follow the steps in this topic to download the file and decompress it before you begin installing the packages. If you are using the CD, go to Installing the JRE upgrade software on page 12 to begin installing the packages from the CD.

To decompress the JRE upgrade file:

1. Using **ftp**, transfer the upgrade file, jre131.cpio.Z, to a temporary directory on the CONVERSANT system.
2. On the CONVERSANT system, log in as root.
3. At the command prompt, enter **cd /update/pkgs**
4. Enter **dfspace**

   The system displays disk space available on each partition of the CONVERSANT system. Verify that the partition for the /update/pkgs directory (partition "/") has at least 150 Mb available. It must be big enough to contain all of the decompressed package files. If the partition is big enough, go to Step 5. If not, go to Step 7.
5. Enter **cd *partition*; mkdir *directory*** where *partition* is a partition on the CONVERSANT system with at least 150 Mb and *directory* is the name of the directory you want to contain the decompressed package files.
6. Enter **cd *directory*** where *directory* is the directory you created in the previous step.
7. Enter **cp /*temp_dir*/jre131.cpio.Z $PWD** where *temp_dir* is the directory to which you transferred the JRE upgrade file after you downloaded it from Avaya (in Step 1 of this procedure).

   The JRE upgrade file is copied to the install directory.
8. Enter **uncompress jre131.cpio.Z**

   The file decompresses into a cpio archive file.
9. Enter **cpio -icvBd < jre131.cpio**

   The system extracts the JRE upgrade packages and installation script from the archive. For more information on the JRE upgrade software, see Contents of the JRE upgrade software on page 11. If you are ready to install the JRE upgrade software, see Installing the JRE upgrade software on page 12.

Contents of the JRE upgrade software

The JRE upgrade software consists of several packages and a script for installing them.

The following packages are included as part of the JRE upgrade software:

- UnixWare/OpenServer Development Kit (UDK) Feature Supplement (IA32) 7.1.1b (udkfs.image)
- UnixWare/OpenServer Development Kit (UDK) Runtime Feature Supplement (IA32) 7.1.1b (udkrtfs.image)
- libc Shared Library Set (ptf7689b)
- libthread supplement (ptf7410j)
- X11 fonts (urwfonts)
- J2SE Runtime Environment 1.3.1.06 (j2jre131.06)

The installation script, install_jre.sh, that is included with the JRE upgrade software performs the following actions:

- Installs the packages listed above
- Checks Oracle MTS and disables it if necessary
- Rebuilds the system kernel
- Prompts you to reboot the system

To run the script and install the JRE upgrade software, see Installing the JRE upgrade software on page 12.

Installing the JRE upgrade software

Installing the JRE upgrade software involves installing several packages related to the upgrade and rebooting the CONVERSANT system. The entire process takes approximately 30 minutes.

IMPORTANT:
The installation script stops the voice system before installing the JRE upgrade packages. Make sure to install the software during an appropriate time in which call traffic can be disrupted on the system with minimal impact.

To install the JRE upgrade software:

1. Log in as root, if necessary.
2. If you are installing the JRE upgrade software from the CD, do the following steps:

   a) At the command prompt, enter **mount –F cdfs –o ro /dev/cdrom/cdrom1 /cdrom**

   b) Enter **cd /cdrom**

   If you have downloaded the JRE upgrade file and decompressed it, do the following:

   Enter **cd /*partition*** where *partition* is the directory you created to store the decompressed the JRE upgrade file (see Decompressing the JRE upgrade file on page 10).

3. Enter **install_jre.sh** to run the installation script.

   The system displays the following message:

   ```
   The Voice System needs to be stopped before running install_jre.sh
   Do you want to stop the voice system & continue? (y/n)?
   ```

4. Enter **y** for Yes.

   The installation process begins. The system displays messages indicating that the UDK Feature Supplement package is installing. During this time, the system displays the following error messages:

   ```
   ## Executing preinstall script.
   ```

```
UX:ls: ERROR: Cannot access /usr/ccs/lib/libm.so: No such file or
directory
UX:ls: ERROR: Cannot access /usr/ccs/lib/libp/libm.so: No such
file or directory
UX:ls: ERROR: Cannot access /usr/include/alloca.h: No such file or
directory
UX:ls: ERROR: Cannot access /usr/include/fenv.h: No such file or
directory
UX:ls: ERROR: Cannot access /usr/include/inttypes.h: No such file
or directory
UX:ls: ERROR: Cannot access /usr/include/rbtree.h: No such file or
directory
UX:ls: ERROR: Cannot access /usr/include/stdbool.h: No such file
or directory
UX:ls: ERROR: Cannot access /usr/include/stdint.h: No such file or
directory
UX:ls: ERROR: Cannot access /usr/include/tgmath.h: No such file or
directory
```

Ignore these messages. The files referenced in the message are actually copied successfully to the system.

As the installation process continues, the script checks for a valid license for the previously installed version of the package. If a valid license does not exist, the system displays the following message (this message does not appear if a valid license exists on the system):

```
The system does not have a valid license for

UnixWare/OpenServer Development Kit

This product requires a license. Licensing information
is contained on the Certificate of License Authority (COLA).

A license may be entered after installation is completed
using the SCOAdmin License Manager.

Press enter key to continue ...
```

5. If the system displays this message, press **Enter**.

   The installation of the UDK Feature Supplement package completes. The script continues without interruption, installing the following packages:

   — UDK Runtime Feature Supplement package

   — libc Shared Library Set

   — libthread supplement

   — X11 fonts

   — J2SE Runtime Environment (JRE) package

As part of the running display of installation messages, the system displays the follow message at the end of each package installation:

```
The installation was a success.

Processing of packages for set <package_name> is completed.


WARNING: NOTICE: Reapply update711 pkg, followed by uw711m1, in
this order.
Failure to do so may leave your system in an inconsistent state.
```

This message indicates that installation of the named package (*package_name* in the message) is complete. Ignore the warning in the message. It is not required for upgrading JRE.

When installation of the final package, the JRE package, completes, the script checks to see if Oracle MTS is enabled. If it is enabled, the system displays the following message:

```
Mts_dispatchers =
"(PROTOCOL=TCP)(PRE=oracle.aurora.server.SgiopServer)"
mts_servers = 1

It is recommended that above lines from /oracle/dbs/initA.ora file
be commented.
Do you wish to comment out the suggested entries? (y/n)?
```

6. If the system displays this message, Enter **y** for Yes**.**

   The lines are commented and the installation process continues and begins rebuilding the system kernel. When the process of rebuilding the kernel is complete, the system displays the following message:

   ```
   It is recommended that you reboot the system to complete the
   upgrade.
   Do you wish to shutdown the system now? (y/n)?
   ```

7. Enter **y** for Yes**.**

   The system shuts down and restarts. The JRE upgrade process is complete. After JRE is installed, database links that use host names to specify remote Oracle servers will no longer work. The correct this problem see Fixing links to remote Oracle servers on page 15.

Fixing links to remote Oracle servers

After installing the JRE upgrade software, database links that use host names to specify remote Oracle servers no longer work. To correct this problem, you must edit the $ORACLE_HOME/network/admin/tnsnames.ora file and replace the host name with the server's IP address.

To fix links to remote Oracle servers:

1. Log in as root (if necessary).
2. Enter **cd $ORACLE_HOME/network/admin/**
3. Enter **vi tnsnames.ora**

   The tnsnames.ora file open in the vi editor.
4. Using vi editing commands, find the section of the file (similar to the following example) that references the host name of the Oracle server.

```
ivrsv3.world =
  (DESCRIPTION =
    (ADDRESS_LIST =
        (ADDRESS =
          (COMMUNITY = TCP.world)
          (PROTOCOL = TCP)
          (Host = host_name)
          (Port = 1521)
        )
    )
    (CONNECT_DATA =
       (SID = A)
    )
  )
```

5. Replace the *host_name* with the IP address of the Oracle server.
6. Repeat Steps 4 and 5 for other Oracle servers referenced in the file.
7. Save and close the file.