# Orbix 3.3 SP13

Release Notes

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

http://www.microfocus.com

2016-02-10

# Contents

# Orbix 3.3.13 Release Notes

Orbix 3.3.13 is a service pack release of Orbix 3.3 from Micro Focus.

These release notes contain information about the Orbix 3.3.13 release. They contain information that might not appear elsewhere in the documentation. Read them in their entirety before you install the product.

For details of the changes that were made in earlier releases of Orbix 3.3, see:

- For changes made in Orbix 3.3.12, see the ***Orbix 3.3 SP12 Release Notes***, available at http://supportline.microfocus.com/Documentation/Orbix/Orbix33sp12.htm
- For changes made between Orbix 3.0.1 and Orbix 3.3.11, see the ***Orbix 3.3 SP11 Release Notes***, available at http://supportline.microfocus.com/Documentation/Orbix/Orbix33sp11.htm

## CORBA Compliance

Orbix 3.3.13 complies with the following specifications:

- CORBA 2.1.
- GIOP 1.1 and 1.0
- C++ Language Mapping (formal/99-07-41)
- IDL-to-Java Language Mapping (formal/99-07-53)

## Interoperability with Other Products

The Java and C++ editions of Orbix 3.3 SP 13 are tested and are interoperable with each other except for those areas that are documented as Known Issues for each edition.

The Java and C++ editions of Orbix 3.3 SP 13 have also been tested and are interoperable with the following Orbix products:

- Previous Orbix 3.3 C++ and Java editions
- Orbix E2A Application Server Platform 6.0 SP3 C++ and Java
- Orbix Trader 1.2.1 Java edition (no C++ edition available)
- Orbacus 4.0.5
- Orbix 3.0.1
- OrbixWeb 3.2

# Product Structure

The distinction between "Orbix Core Services" and the "Orbix Full Services" product, which was made in previous release, no longer applies. Some components that formed part of the previous "Orbix Full Services" are no longer supported.

All components still supported are part of the single Orbix 3.3.13 product. Orbix 3.3.13 includes:

- Orbix 3.3.13 C++ edition
- Orbix 3.3.13 Java edition
- OrbixNames 3.3.13

The following features of previous Orbix 3 versions are **no longer supported** in Orbix 3.3.13:

- Orbix Code Generation Toolkit
- OrbixEvents
- OrbixOTS
- Orbix Wonderwall

# New Features

Orbix 3.3.13 includes the following new features:

- Support for certificates that use SHA 256 has been added to OrbixSSL 3.3.13 C++ and OrbixSSL 3.3.13 Java.
- Support for TLS 1.2 has been added to OrbixSSL 3.3.13 C++ and OrbixSSL 3.3.13 Java.
- The configuration variable `OrbixSSL.IT_PROTOCOLS` was added to control the security transport protocol version. It defaults to TLS version 1. See OrbixSSL 3.3.13 C++ for details.
- New cipher suite values are supported. See OrbixSSL 3.3.13 C++ for details.
- OrbixSSL 3.3.13 Java now supports the JCA/JSSE security toolkit bundled in the JDK. The Baltimore security toolkit bundled in previous releases has been removed and support for it has been dropped.
- A new flag for the IDL compiler in the Orbix 3.3.13 C++ Edition.
- The loading mechanism of the JNI library `kdmjj` has changed. See OrbixSSL 3.3.13 Java for details.

# Platforms and Compilers

For the latest information on supported platforms, compilers, and Java versions, see the Product Availability page.

The following platforms and protocols are no longer supported at Orbix 3.3.13:

- HP-UX on PA-RISC
- Java 8 on 32-bit Solaris

## Java 8 on 32-bit Solaris

Starting with Java 8, Oracle no longer ship the 32-bit Java runtime on Solaris platforms. See "Known Issues" for details.

# Migration from Previous Versions

For information on migrating from an earlier version of Orbix to Orbix 3.3 SP 13, see ***Migrating Orbix Applications to Orbix 3.3*** available with the rest of the Orbix 3.3 SP13 documentation at https://supportline.microfocus.com/productdoc.aspx.

To upgrade to Orbix 3.3.13 from existing Orbix 3.3.x installations, carry out the following procedure:

> **Note:** The services that made up the "Orbix Full Services" product in previous releases are no longer supported, as described in "Product Structure". For customers who are upgrading from a full services installation of Orbix to Orbix 3.3.13, such as Solaris Sparc or HP-UX Itanium (32-bit), Micro Focus recommends some additional steps in the upgrade procedure, which are noted below.

- Ensure that all Orbix services are stopped.
- Back up existing installations before you upgrade to Orbix 3.3.13.
- If you are upgrading from a full services installation of Orbix to Orbix 3.3.13, such as on Solaris Sparc or HP-UX Itanium (32-bit):
    - Rename the installation folder of the Orbix 3.3.12 installation, so that it is not overwritten.
    - Install Orbix 3.3.13 to the old location of the Orbix 3.3.12 installation.
    - Overlay the **config** folder of the Orbix 3.3.12 installation to the **config** folder of the Orbix 3.3.13 installation, in order to preserve the previous configuration and databases (such as IMR, NamesRep).
- In other circumstances, simply run the Orbix 3.3.13 installer. The Orbix installer overwrites the existing version.

For details on installing Orbix 3.3.x service packs, see the ***Orbix Installation Guide***, available with the rest of the Orbix 3.3.13 documentation at:

https://supportline.microfocus.com/productdoc.aspx.

# Deprecated Features Policy

When a feature is deprecated it means that:

- No support for this feature is given for the current version and for subsequent versions (we do not explain how to use it, and we do not fix any bugs in this feature).
- If you have not used this feature before, DO NOT start using it with this release.
- If you are already using this feature, you should remove it if at all possible.
- The feature may not be present in future versions of the product.

# Other Resources

The following additional resources are available:

- For the latest information on supported platforms and compilers, see the Orbix Supported Platforms page.
- The most up-to-date versions of Orbix technical documentation are available at:

  https://supportline.microfocus.com/productdoc.aspx
- The Orbix Knowledge Base is a database of articles that contain practical advice on specific development issues, contributed by developers, support specialists, and customers. This is available at: http://community.microfocus.com/microfocus/corba/orbix/w/knowledge_base/
- Contact Micro Focus technical support at:

  http://www.microfocus.com

# Orbix 3.3.13 C++ Edition

This section describes changes made specifically to Orbix C++ Edition that are relevant to Orbix 3.3 SP 13.

## New Features

Orbix 3.3 SP 13 C++ Edition is binary compatible with Orbix 3.3 C++ Edition. Orbix 3.3.13 C++ edition includes the following new features:

- New flag for IDL Compiler

## New flag for IDL Compiler

A new flag for the IDL compiler in the Orbix C++ Edition, `-bound_seq_check`, generates additional index checking code for bounded sequences.

## Deprecated Features

The following is a list of deprecated features in Orbix C++ Edition:

| Feature | Description | Feature Removed | When Deprecated |
|---|---|---|---|
| _bind() | Should use other means. | No | Orbix 3.0 |
| Transformers | Can use SSL for security. | No | Orbix 3.0 |
| Piggy backing data with filters | Should use Service Contexts. | No | Orbix 3.0 |
| Opaque data type | | No | Orbix 3.0 |
| Orbix network protocol (POOP) | Must use IIOP instead. | No | Orbix 3.0 |
| IDL compiler options `-i` and `-f` | | No | Orbix 3.0 |
| IR | Replaced with the IFR. | Yes | Orbix 3.0 |
| Locator | Can implement own load balancing solution. | Yes | Orbix 3.3 |
| Non-native exceptions | Must use Native Exceptions | Yes | Orbix 3.3 |
| TIE macro DEF_TIE(I,X) | Use other form | Yes | Orbix 3.3 |
| Configuration Explorer (`ConfigurationExplorer.bat`) | Configure Orbix components without modifying the configuration files directly. | No | Orbix 3.3 SP 5 |
| Server Manager (ServerManager.bat) | Allows you to manage the Implementation Repository. | No | Orbix 3.3 SP 5 |

**Note:** Orbix 3.0 was released February 1999 and Orbix 3.3 was released September 2000.

## Known Issues

The following table summarizes known issues for Orbix 3.3.13 C++ Edition.

| Incident ID | Synopsis |
|---|---|
| ORBTHREE-1 | Orbix daemon memory leak. |
| 64992 | There is a known problem with foreign FDs (File Descriptors) on HPUX 11. When Orbix is asked to manage foreign FDs, there are some situations where the process hangs. It is not typical to ask Orbix to manage foreign FDs, and this problem can be avoided by not asking Orbix to manage foreign FDs. |
| 64991 | There is a known problem using C++ keywords in various situations in the IDL file. Using C++ keywords for attribute names, operations names and field names (of structures and exceptions) works. However, using C++ keywords as the type name of a module, interface, exception, or struct does not work. Customers should avoid using C++ keywords in the IDL as the type names of modules, interfaces, exceptions, and structs. |
| 56121 | The IDL compiler issues warnings if the IDL contains identifiers that are reserved keywords but not all lower case. For example, the IDL `interface Attribute{};` causes `Warning: identifier Attribute clashes with keyword` even though it is a valid interface name and is case-different from the reserved keyword `attribute`. |
| 55600 | No overloaded output-streaming operator (<<) is provided for the unsigned long long CORBA type (`CORBA::ULongLong`) in Orbix 3.3. |
| 55599 | No overloaded output-streaming operator (<<) is provided for the signed long long CORBA type (`CORBA::LongLong`) in Orbix 3.3. |
| 55547 | Orbix 3.3 generated IDL stub code on Windows NT for multi-dimensional arrays as in parameters should work around known VC6 multidimensional array const bug. |
| 56334 | When service context handlers in Orbix runtime encounter an abnormal condition, the diagnostic messages are not very informative. |
| - | Oracle Solaris Studio 12.4 compiler is not supported with Orbix 3.3.13. A compiler issue was uncovered while certifying Orbix 3.3.13 with Studio 12.4. The compiler issue relates to an inconsistent behavior in passing parameters on function calls between Studio 12.4 and earlier compiler versions.<br>Micro Focus is working with the compiler vendor towards a resolution of this issue.<br>Micro Focus advises customers to refrain from using Oracle Solaris Studio 12.4 with Orbix 3.3.13 until this issue is resolved. |

## Compilation problems on Windows

Compilation problems on Windows may result in the following error message:

```
Warning: Orbix wants an fd_set of size 1024 or greater.
    Please include CORBA.h before winsock2.h
```

This may be resolved by defining `WIN32_LEAN_AND_MEAN` when compiling. For example:

```
CL /c ... -DWIN32_LEAN_AND_MEAN ... myFile.cpp
```

If you do not wish to use this option when compiling you may also resolve the problem by editing CORBA.h by moving line 22,

```
#include <corba/PreCORBA.h>
```

to the position immediately after line 15,

```
#define CORBA_INCLUDES
```

## Actional Integration

Usage of the Actional Integration feature in conjunction with a Thread Filter will result in the Actional Integration not reporting correctly when the ThreadFilter `inRequestPreMarshal()` method implementation returns -1. This is caused by the fact that the Actional Interceptor is implemented using Filters, and returning `-1` from a ThreadFilter `inRequestPreMarshal()` method causes all subsequent Filters in the Filter to not be invoked.

On HP-UX systems, the Actional Integration feature may fail to dynamically load within single-threaded processes.

The Actional Integration feature is implemented as a shared library that is dynamically loaded by the Orbix C++ runtime. This shared library links to a multi-threaded Actional C SDK library, used to communicate with the Actional Agent service. The HP-UX dynamic loader may fail to dynamically load this multi-threaded library within a single threaded process (that is, the orbix daemon).

In order to work around this issue, the LD_PRELOAD environment variable should be set so that the `pthread` library is preloaded.

To diagnose this issue and determine the location of the `pthread` library, perform the following on HP-UX Itanium systems:

1. Set the environment variable IT_SHLIB_VERBOSE to `1`
2. Execute your single-threaded process
3. Look for the following line in the output:
   - ♦ `/usr/lib/hpux32/dld.so: Cannot dlopen load module '/usr/lib/hpux32/libpthread.so.1' because it contains thread specific data`

To resolve the issue, set LD_PRELOAD as mentioned below:

```
LD_PRELOAD=/usr/lib/hpux32/libpthread.so.1
```

## IPv6 Enablement

Orbix 3.3 SP 13 has the following known issue in regarding to the use of the IPv6 enablement of the product:

- The POOP Protocol or Orbix Protocol is currently **not** supported with IPv6 communications, and IIOP should be used in its place.

## Stopping double deletion of CORBA::Any when un-marshaling CORBA::Anys during DSI invocation processing

Some applications use the following pattern for memory management of `CORBA::Any`s required for DSI request processing. This is incorrect and causes a memory corruption error with this version of Orbix:

```
CORBA::NVList_ptr pArgList;
if (CORBA::Orbix.create_list(1, pArgList))
 {
    CORBA::Short value_of_n = 0;
    // create an any on heap. This is the representative
    // of the in argument.  All of the arguments (anys)
    // will be stored in an NV list
    //
    CORBA::Any* pAny = new CORBA::Any(CORBA::_tc_short,
        &value_of_n, 0);
    // populate the NV list with the heap allocated any
    // and name of "n"
    //
    pArgList->add_value("n", *pany, CORBA::DSI_ARG_IN);
    // read all the arguments (values) from the request
    // into the NV list
    //
    rSrvReq.params(pArgList);
    // do invocation processing
    // ************* NOTE *****************
    // Deleting the CORBA::Any is an error as the Orbix
    // runtime will do so.
    //
    delete pAny;  // Error!  Don't do this.
}
```

This code would not have caused problems prior to Orbix 3.3.1, because Orbix 3.3 and earlier versions did not properly delete the `Any`. Since Orbix 3.3.1, Orbix deletes the `Any`, so it is no longer necessary to do it.

## Deploying an Orbix 3.3 SP 13 daemon in Orbix 3.0.1 environment

An Orbix 3.3 SP 13 daemon can launch Orbix 3.0.1 servers. For all Orbix 3.0.1 daemon utilities, your clients and servers work with the Orbix 3.3 SP 13 daemon. You need to append the library path in the environment with the Orbix 3.3 SP 13 library path.

**Note:** This does not apply if you are using AIX 4.3.3 and 4.3.2 because none of the Orbix binaries built on AIX 4.3.3 operate on 4.3.2 daemon utilities.

# Resolved Issues

The resolved issues for Orbix C++ Edition that customers have reported are listed in this section. The numbers that follow each issue are the Reported Problem Incident number followed by the Customer Incident Numbers (in parentheses). RPIs that have numbers only (and no text) are included to confirm that the RPIs have been fixed, since no further information is required.

- The documentation in the ***Orbix Administrator's Guide C++ Edition*** for the Orbix Multi-home feature has been clarified.

  RPI 607564
  RPI 607565
  RPI 1096963

- A valid licence was accidentally embedded inside the `orbixd` executable. Packaging changes mean that this can no longer happen.

  RPI 607849

- The description of the use of licence keys in silent mode installation has been clarified in the ***Orbix Installation Guide***.

  RPI 607850

- Documentation of the `Orbix.IT_KEYOBJECTTABLE_USINGPORT` variable has been added to the ***Orbix Administrator's Guide C++ Edition***.

  RPI 614228

- The Orbix daemon was crashing when `IT_ENABLE_MULTI_HOMED_SUPPORT` was enabled on AIX systems.

  RPI 1095871 (2790864)

- Orbix 3.3 improvement: Sanity check on generated "[]" operator code.

  RPI 1089425 (2647809)

- RPI 1094250 (2698442)

- The hostname would get pre-appended with the value of `IT_GIOP_VERSION` if the `IT_LOCAL_HOST` configuration variable was also set. This caused the Orbix 3 server to crash.

  RPI 1095935 (2790864)

- Orbix 3.3 improvement to debug “index out of bounds” in accessing a sequence.

  RPI 1096147 (2792541)

- The Orbix 3.3.12 AIX (32-bit) build missed a compiler option, which led to the compiler not placing a number of symbols into the Orbix shared libraries. This resulted in missing symbols when an application built with an older version of Orbix was run against the Orbix 3.3.12 libraries. The compiler option was re-enabled in Orbix 3.3.12 HF05. This ensures that the previous binary compatibility with earlier versions of Orbix 3.3 is maintained.

  RPI 1097447 (2805476)

# Orbix 3.3.13 Java Edition

This section describes changes made specifically to Orbix Java Edition that are relevant to Orbix 3.3 SP 13.

## New Features

Orbix 3.3 SP 13 Java Edition is binary compatible with Orbix 3.3 Java Edition. There are no new features.

## Deprecated Features

The following is a list of features deprecated in Orbix Java Edition:

| Feature | Description | Feature Removed | When Deprecated |
|---|---|---|---|
| _bind() | Use other means. | No | OrbixWeb 3.2 |
| Transformers | Can use SSL for security. | No | OrbixWeb 3.2 |
| Piggy backing data with filters | Should use Service Contexts. | No | OrbixWeb 3.2 |
| Opaque data type | | No | OrbixWeb 3.2 |
| Orbix network protocol (POOP) | Must use IIOP instead. | No | OrbixWeb 3.2 |
| IDL compiler options `-i` and `-f` | | No | OrbixWeb 3.2 |
| Orbix Java activator (`Orbixdj.bat`) | Java activator in graphical mode | No | Orbix 3.3 SP 5 |

**Note:** OrbixWeb 3.2 was released February 1999.

# Known Issues

The following table summarizes known issues for Orbix 3.3.13 Java Edition.

| Incident ID | Synopsis |
|---|---|
| 65605 | The Server Manager GUI does not update when a server is started and then stopped (affects Orbix 3.3.2 and upwards). This GUI is deprecated. |
| 64957 | Fragmentation error occurs on the client side if large chunk of data is sent in fragments from an ASP 5.*x* and higher server. The fragments received from the ASP server are malformed. This is an interoperability issue between ASP and Orbix Java 3.3 SP 5. |
| - | 32-bit Solaris runtimes require a 64-bit JDK. From Java 8, Oracle no longer ship the 32-bit Java runtime on Solaris platforms; see http://www.oracle.com/technetwork/java/javase/8-compatibility-guide-2156366.html for details.  This means that customers can no longer use Java 8 on Solaris to load any 32-bit JNI libraries.<br>• For **Java 8** users, Micro Focus supplies 64-bit counterparts of these JNI libraries on Solaris which ensure that they will continue to work with Java 8 on Solaris.<br>• Orbix 3.3 users using a **Java 7** who require a 64-bit JVM runtime can specify this by setting the "`-d64`" option to the Java VM executable, or by directly using the 64-bit Java process: *<JAVA_HOME>*`/bin/sparcv9/java`. |
| - | An exception may be thrown by the `orbixdj` utility with Java versions newer than 1.7 update 27. See "Orbixdj Security Permissions" for details. |

## Orbixdj Security Permissions

When using the `orbixdj` utility with Java versions newer than 1.7 update 27, the following exception may be thrown by the Java virtual machine.  This is because of a security vulnerability that requires an explicit policy to be set to allow the CORBA InputStream and OutputStream to be sub-classed.

```
Exception in thread "Request Processor" java.security.AccessControlException: access
        denied ("java.io.SerializablePermission" "enableSubclassImplementation")
   at java.security.AccessControlContext.checkPermission(AccessControlContext.java:457)
   at java.security.AccessController.checkPermission(AccessController.java:884)
   at java.lang.SecurityManager.checkPermission(SecurityManager.java:553)
   at org.omg.CORBA_2_3.portable.InputStream.checkPermission(InputStream.java:67)
   at org.omg.CORBA_2_3.portable.InputStream.<init>(InputStream.java:84)
   at IE.Iona.OrbixWeb.CORBA.InputCoder.<init>(Unknown Source)
   at IE.Iona.OrbixWeb.CORBA.MarshalBuffer.create_input_stream(Unknown Source)
   at IE.Iona.OrbixWeb.CORBA.Request.create_input_stream(Unknown Source)
   at IE.Iona.OrbixWeb.Activator.DJAuthenticationFilter.inRequestPreMarshal(Unknown
        Source)
   at IE.Iona.OrbixWeb.CORBA.ServerRequest.inRequestPreMarshal(Unknown Source)
   at IE.Iona.OrbixWeb.CORBA.ServerDispatcher.dispatchSpecial(Unknown Source)
   at IE.Iona.OrbixWeb.CORBA.BOAImpl.processRequest(Unknown Source)
   at IE.Iona.OrbixWeb.CORBA.BOAImpl.processOneEvent(Unknown Source)
   at IE.Iona.OrbixWeb.CORBA.BOAImpl.processEvents(Unknown Source)
   at IE.Iona.OrbixWeb.CORBA.EventHandler.run(Unknown Source)
   at java.lang.Thread.run(Thread.java:745)
```

To resolve this problem, you must update the `java.policy` file under `<JAVA_HOME>/jre/lib/security` as follows, to allow this subclassing to continue:

```
grant {
   // ...
   permission java.io.SerializablePermission "enableSubclassImplementation"; }
```

# Resolved Issues

The resolved issues for Orbix Java edition that customers have reported are listed in this section. The numbers that follow each issue are the Reported Problem Incident number followed by the Customer Incident Numbers (in parentheses). RPIs that have numbers only (and no text) are included to confirm that the RPIs have been fixed, since no further information is required.

- A valid licence was accidentally embedded inside the `orbixd` executable. Packaging changes mean that this can no longer happen.

  RPI 607849

- The description of the use of licence keys in silent mode installation has been clarified in the ***Orbix Installation Guide***.

  RPI 607850

- Documentation of the `Orbix.IT_KEYOBJECTTABLE_USINGPORT` variable has been added to the ***Orbix Administrator's Guide Java Edition***.

  RPI 614228

# OrbixNames 3.3.13

This section describes changes made specifically to the OrbixNames product that are relevant to OrbixNames 3.3 SP 13.

## New Features

OrbixNames 3.3 SP 13 is binary compatible with OrbixNames 3.3. There are no new features.

## Deprecated Features

The following is a list of features deprecated in OrbixNames:

| Feature | Description | Feature Removed | When Deprecated |
|---|---|---|---|
| Names Service browser (`NamesBrowser.bat`) | Allow you to monitor and manage the Naming Service externally to your applications. | No | Orbix 3.3 SP5 |

## Known Issues

The following table summarizes known issues for OrbixNames 3.3.13.

| Incident ID | Synopsis |
|---|---|
| Bug ID 4276129 in JDK1.3.1 | When the Naming Service is persistently launched, the Password dialog box is displayed at the same time as the missing font messages below:<br>`Font specified in font.properties not found [-urw-itc zapfdingbats-medium-r-normal--*-%d-*-*-p-*-sun-fontspecific]`<br>`Font specified in font.properties not found [-urw-itc zapfdingbats-medium-r-normal--*-%d-*-*-p-*-sun-fontspecific]`<br>`Font specified in font.properties not found [-urw-itc zapfdingbats-medium-r-normal--*-%d-*-*-p-*-sun-fontspecific]`<br>The fonts specified in font.properties need to be found on the host system. Otherwise these messages are displayed.<br>Workarounds:<br>• Customize the font.properties file for each machine.<br>• Install the SUNIWof font packages. |
| Bug ID 4285197 in JDK 1.3.1 | When the Naming Service is launched by semi-secure `orbixd`, `libkdmjj.so/libkdmjj.sl/kdmjj.dll` of SSL is used to supply `orbixd` with the Naming service password. The marker used to launch the Naming Service involves -`Xbootclasspath` argument to the Java interpreter.<br>As a result of this bug, `orbixd` cannot supply the password to the KDM as the kdmjj library cannot be loaded. This results in the Naming Service asking for user input for password when it is automatically launched. |

| Incident ID | Synopsis |
|---|---|
|  | Workarounds:<br>Solaris: Copy the .so into `${JDKHOME}/jre/lib/sparc` (or set a symbolic name).<br>HPUX: Copy the .sl into `${JDKHOME}/jre/lib/PA_RISC` (or set a symbolic name).<br>Windows: Copy the .dll into `${JDKHOME}\jre\bin`.<br>`${JDKHOME}` points to the JRE directory used in `IT_JAVA_INTERPRETER` used in `common.cfg`. This is the intended behavior.<br>The remaining steps are relevant for all systems:<br>All system classes only look up shared libraries in `$JAVA_HOME/bin`. If you do need to load custom libraries for the system classes, there are two choices:<br>1. Install custom libraries into `$JAVA_HOME/bin`;<br>2. Set the property `sun.boot.library.path` to include the user library path. The syntax is:<br>`java -Dsun.boot.library.path=`<br>`$JAVA_HOME/bin:$CUSTOM/bin ...`<br>When an SSL-enabled Names Server NS is run persistently or automatically launched by the Orbix Daemon, it listens on the port given by configuration variable `IT_SSL_IIOP_LISTEN_PORT` in `orbixnames3.cfg`.<br>Follow the steps below to automatically launch an SSL-enabled OrbixNames server by the Orbix daemon, and use the KDM utility to supply password to `orbixd`:<br>1. `orbixssl.cfg s`hould have the following entries and values for Naming Service:<br>`IT_AUTHENTICATE_CLIENTS = "TRUE";`<br>`IT_SECURITY_POLICY = "SECURE";`<br>`IT_DAEMON_POLICY = "SEMI_SECURE_DAEMON";`<br>`IT_KDM_ENABLED = "TRUE";`<br>2. `orbixnames.cfg` should have `IT_SSL IIOP_LISTEN_PORT` defined.<br>3. Start `orbixd`.<br>4. `putit NS -j -jdk2 -- -Xbootclasspath:[ … set of jars …]`<br>`IE.Iona.OrbixWeb.CosNaming.NS -secure`<br>5. Start `kdm`<br>6. `Putkdm NS kdm-password`<br>7. NS is the Implementation repository entry required for automatically launching the Naming Service.<br>8. Use the C++ utilities with the `-s` option. |

# Resolved Issues

The resolved issues for OrbixNames that customers have reported are listed in this section. The numbers that follow each issue are the Reported Problem Incident number followed by the Customer Incident Numbers (in parentheses). RPIs that have numbers only (and no text) are included to confirm that the RPIs have been fixed, since no further information is required.

- The timeout (`-t`) flag for the Orbix Names command line tools was not being honored. The option is now honored.

  RPI 608788

- The `bind_new_context()` method in the Orbix 3 Naming Service could in certain situations throw a Java `NullPointerException`, which would result in certain NamingContext objects not being created inside the Naming Service.

  RPI 1094371 (2696925)

# OrbixSSL 3.3.13 C++

This section describes changes made specifically to OrbixSSL C++ that are relevant to Orbix 3.3 SP 13.

## New Features

OrbixSSL 3.3 SP 13 C++ Edition is binary compatible with Orbix 3.3 C++ Edition.

OrbixSSL 3.3.13 C++ includes the following new features:

- Support for SHA256
- Support for TLS 1.2
- Security Protocols
- Cipher Suite Values

## Support for SHA256

Support for certificates that use SHA 256 is now enabled in Orbix 3.3.13. See RPI 1099424 (2820682) for details.

## Support for TLS 1.2

Support for TLS version 1.2 is enabled in OrbixSSL 3.3.13 C++.

## Security Protocols

### SSL v3 disabled

Starting with Orbix 3.3.13, Orbix 3 as delivered has the SSLv3 security protocol disabled by default.  SSLv3 can still be configured for backwards compatibility with older servers; however it should be noted that SSLv3 is susceptible to the POODLE exploit, and where possible customers should upgrade to the newer and more secure TLS protocols.

By default Orbix 3.3.13 supports the following TLS protocols:

- TLS v1.0
- TLS v1.1
- TLS v1.2

### Specifying the protocol version

At Orbix 3.3.12 HotFix 04, a new configuration variable was added to control the security transport protocol version: `OrbixSSL.IT_PROTOCOLS`. The `OrbixSSL.IT_PROTOCOLS` configuration variable is a comma-separated list of security transports that the product will try to use. Valid values are the strings:

- `SSLv3` (no longer supported  by default)
- `TLSv1`

- TLSv1.1
- TLSv1.2

The default security transport protocol version is TLSv1. This represents a change from previous versions, where SSLv3 was the default.

In order to interoperate with previous Orbix versions, it will be necessary to add SSLv3 to the list of enabled security protocol versions in the orbixssl.cfg file. It is recommended that you specify TLSv1 as the first option in the list of versions and only enable support for SSLv3 when it is needed to interoperate with previous Orbix versions, as illustrated in the following example:

```
# orbixssl.cfg for Orbix SSL C++ and Orbix SSL Java

    OrbixSSL {
        # [SNIP…]
            IT_PROTOCOLS = "TLS_V1", "SSL_V3";
    }
```

### TLS 1.2 with IBM JDKs

IBM Java, starting with versions 7 and 8, forbids the use of certificates that are signed with MD5 (MD5WithRSA). This is not an issue with other JCA implementations (Oracle and HP), nor with lower versions of the TLS protocols.

This excerpt from the TLS 1.2 specification does signify that MD5 should no longer be considered a safe hashing algorithm:

> ***MD5***
>
> *MD5 [MD5] is a hashing function that converts an arbitrarily long data stream into a hash of fixed size (16 bytes). Due to significant progress in cryptanalysis, at the time of publication of this document, MD5 no longer can be considered a 'secure' hashing function.*

Micro Focus highly recommends that any certificates used in secure Orbix applications that are signed with an MD5 digest signature are regenerated to use at least a SHA-1 digest signature.

## Cipher Suite Values

The valid values that can be assigned to the IT_CIPHERSUITES and IT_ALLOWED_CIPHERSUITES configuration variables have changed.

The following existing cipher suite strings are now deprecated:

- SSLV3_RSA_WITH_RC4_128_SHA
- SSLV3_RSA_WITH_RC4_128_MD5
- SSLV3_RSA_WITH_3DES_EDE_CBC_SHA
- SSLV3_RSA_WITH_DES_CBC_SHA
- SSLV3_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSLV3_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- SSLV3_RSA_EXPORT_WITH_RC4_40_MD5

The following cipher suite strings should be used instead of the deprecated strings listed above:

- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_DES_CBC_SHA
- RSA_EXPORT_WITH_DES40_CBC_SHA
- RSA_EXPORT_WITH_RC2_CBC_40_MD5
- RSA_EXPORT_WITH_RC4_40_MD5

The currently supported cipher suite strings no longer start with “SSLV3_” to avoid the potential confusion that would arise when the IT_PROTOCOL is set to TLS_V1.

An example of setting the cipher suites in configuration:

```
IT_CIPHERSUITES =
   "RSA_WITH_AES_128_CBC_SHA,RSA_WITH_AES_256_CBC_SHA,RSA_W
   ITH_AES_128_CBC_SHA256,RSA_WITH_AES_256_CBC_SHA256";
```

# Deprecated Features

The following is a list of deprecated features in OrbixSSL C++:

| Feature | Description | Feature Removed | When Deprecated |
|---|---|---|---|
| Support for the following cipher suites:<br>• SSLV3_RSA_WITH_RC4_128_SHA<br>• SSLV3_RSA_WITH_RC4_128_MD5<br>• SSLV3_RSA_WITH_3DES_EDE_CBC_SHA<br>• SSLV3_RSA_WITH_DES_CBC_SHA<br>• SSLV3_RSA_EXPORT_WITH_DES40_CBC_SHA<br>• SSLV3_RSA_EXPORT_WITH_RC2_CBC_40_MD5<br>• SSLV3_RSA_EXPORT_WITH_RC4_40_MD5 | See “Cipher Suite Values” for replacements. | No | Orbix 3.3.13 |

# Resolved Issues

The resolved issues for OrbixSSL C++ that customers have reported are listed in this section. The numbers that follow each issue are the Reported Problem Incident number followed by the Customer Incident Numbers (in parentheses). RPIs that have numbers only (and no text) are included to confirm that the RPIs have been fixed, since no further information is required.

- The sample certificates shipped with the product have been updated with expiry dates in the year 2035.

  RPI 1094449 (2700365)

- Fixed OpenSSL 1.0.1c Heartbleed bug by disabling vulnerable heartbeats code.

  RPI 1094083 (2696838)

- A fix protects Orbix 3.3 against the POODLE vulnerability of the SSL v3 encryption protocol. See “Security Protocols” for details of the new configuration variables introduced.

  RPI 1097034 (2801728)

- Support for SHA-256 has been added to Orbix 3.3.13 for both C++ and Java.

  Support for the following cipher suites has been added:

  ```
  TLS_RSA_WITH_AES_128_CBC_SHA
  TLS_RSA_WITH_AES_256_CBC_SHA
  TLS_RSA_WITH_AES_128_CBC_SHA256
  TLS_RSA_WITH_AES_256_CBC_SHA256
  ```

  RPI 1099424 (2820682)

# OrbixSSL 3.3.13 Java

This section describes changes made specifically to OrbixSSL Java that are relevant to Orbix 3.3 SP 13.

## New Features

OrbixSSL 3.3 SP 13 Java Edition is binary compatible with OrbixSSL 3.3 Java Edition.

OrbixSSL 3.3.13 Java includes the following new features:

- Support for SHA256
- Support for TLS 1.2
- Java Security Toolkit
- KDM JNI Loading

## Support for SHA256

Support for certificates that use SHA 256 is now enabled in Orbix 3.3.13. See RPI 1099424 (2820682) for details.

## Support for TLS 1.2

Support for TLS version 1.2 is now enabled in OrbixSSL 3.3.13 Java.

## Java Security Toolkit

The Baltimore security toolkit is removed from Orbix 3.3.13. The Java security toolkit used is now the JCA/JSSE Java Security Toolkit.

By default Orbix 3.3.13 supports the following TLS protocols:

- TLS v1.0
- TLS v1.1
- TLS v1.2

See "Support for TLS 1.2" for more information, and see "Security Protocols" for an example of setting the protocol.

**Note:** Due to various security vulnerabilities, the SSLv3 protocol is disabled by default in Orbix 3.3.13. Use of the SSL protocol should be avoided in favor of TLS. It is possible, though strongly not recommended, to enable the SSLv3 protocol to interoperate with endpoints that only support the SSLv3 protocol. This can be achieved by setting the `OrbixSSL.IT_PROTOCOLS` configuration variable.

Specify the cipher suites that you wish to use, by setting the `IT_CIPHERSUITES` and `IT_ALLOWED_CIPHERSUITES` configuration variables. See "Cipher Suite Values" for a list of the cipher suites now supported.

An example of setting the cipher suites in configuration is as follows:

```
IT_CIPHERSUITES =
    "RSA_WITH_AES_128_CBC_SHA,RSA_WITH_AES_256_CBC_SHA,RSA_
    WITH_AES_128_CBC_SHA256,RSA_WITH_AES_256_CBC_SHA256";
```

### Known issues

- On HPUX 11iv3 (B.11.31) 64 bit, PKCS12 certificates generated by Netscape might not be readable by Orbix.
- If you are using either of the following cipher suites, note that your JDK must have the JCE Unlimited Strength Jurisdiction Policy Files installed:
    - `IT_SSLCipherSuite.IT_RSA_WITH_AES_256_CBC_SHA`
    - `IT_SSLCipherSuite.IT_RSA_WITH_AES_256_CBC_SHA256`

**Note:** Some normally supported cipher suites cannot be used with specific versions of Java:

- When using the IBM JDK on AIX, the following cipher suites are not permitted with TLSv1, TLSv1.1, or TLSV1.2 when using the JCE unlimited strength jurisdiction policy files:
    - `SSL_RSA_WITH_RC4_128_MD5`
    - `SSL_RSA_WITH_RC4_128_SHA`
- Java 8 may not provide support for some of the cipher suites supported by Orbix 3.3. For example, Java 8 may fail to handshake when using:
    - `SSL_RSA_EXPORT_WITH_DES40_CBC_SHA`
    - `SSL_RSA_EXPORT_WITH_RC4_40_MD5`

- If a private key is in PEM encoding and contains data similar to the following, then Orbix Java is unable to read the key:

    ```
    Proc-Type: 4,ENCRYPTED
    DEK-Info: DES-EDE3-CBC,FE4CB4E10993F9D1
    ```

    Some workarounds are:

    - Convert the private key to DER encoding.
    - Convert the private key to PKC12 encoding.
    - If the KEY must be in PEM encoding, then generate the private key so it does not contain the data above. For example, using OpenSSL use:

        ```
        openssl genrsa -out private_key.pem 2048
        ```

    Note that Orbix Java does not support PKCS8 encoded private keys.
- The Baltimore toolkit provided a means for caching sessions. The equivalent functionality is not provided by JSSE.
- The certificate verification performed by the Baltimore toolkit differs from that provided by JSSE. The exceptions thrown by certificate verification may differ from those thrown when the Baltimore toolkit was used.

## KDM JNI Loading

The JNI library `kdmjj` provides a mechanism to read a password stored in the OrbixKDM service from a Java server. In previous releases Orbix required this JNI library to be copied into the `<JREHOME>/lib/<arch>` folder.

In OrbixSSL 3.3.13 you can still copy the library into this folder, but Orbix will try to load the library via the environment variables `IONA_ROOT` or `ORBIX_HOME`. It will look in the relevant `bin/lib` sub-folder for the presence of the `kdmjj` library before calling into the Java VM to load the library. If this fails, it defaults to the old way of loading from the `jre` folder.

## Impact on APIs

The change in security toolkits changes the behavior of some of the APIs described in the ***OrbixSSL Programmer's and Administrator's Guide Java Edition***.

| Function | Description |
|---|---|
| `IE.Iona.OrbixWeb.SSL.IT_AVA.convert()` | The byte array returned to the caller is generated from the JSSE `X509Certificate` class. This array differs from the array returned when it was generated using a Baltimore class. |
| `IE.Iona.OrbixWeb.SSL.IT_X509Cert.getExtensions()` | When using JSSE, the number of extensions returned as well as the content of the extension data may differ from the Baltimore toolkit. |
| `IE.Iona.OrbixWeb.SSL.IT_X509Cert.getIssuer()` | The value in the returned `IT_AVAList` when using JSSE differs from the Baltimore toolkit. In particular, the DER value for each `IT_AVA` `i`n the I`T_AVA_LIST` will be for the entire issuer. |
| `IE.Iona.OrbixWeb.SSL.IT_X509Cert.getSubject()` | The value in the returned `IT_AVAList` when using JSSE differs from the Baltimore toolkit. In particular, the DER value for each `IT_AVA` `i`n the I`T_AVA_LIST` will be for the entire subject |
| `IE.Iona.OrbixWeb.SSL.IT_X509Cert.getVersion()` | When using the Baltimore toolkit, the version returned was the value in the certificate. For example, a version 1 certificate has a value of 0, so `0` is returned on the call.<br>With JSSE, the actual version number is returned. For a version 1 certificate, the value `1` is returned. |

| Function | Description |
|---|---|
| IE.Iona.OrbixWeb.SSL.IT_X509Cert.parseExtensions() | When using JSSE, the number of extensions returned may differ from the Baltimore toolkit. |
| IE.Iona.OrbixWeb.SSL.IT_SSL.getNegotiatedCipherSuite() | If the following cipher suites have been set with a call to IE.Iona.OrbixWeb.SSL.IT_SSL.specifyCipherSuites():<br>• IT_SSLCipherSuite.IT_RSA_WITH_AES_128_CBC_SHA<br>• IT_SSLCipherSuite.IT_RSA_WITH_AES_256_CBC_SHA<br>• IT_SSLCipherSuite.IT_RSA_WITH_AES_128_CBC_SHA256<br>• IT_SSLCipherSuite.IT_RSA_WITH_AES_256_CBC_SHA256<br>The IT_SSLCipherSuite .name() value returned by getNegotiatedCipherSuite() will be:<br>• TLS_RSA_WITH_AES_128_CBC_SHA<br>• TLS_RSA_WITH_AES_256_CBC_SHA<br>• TLS_RSA_WITH_AES_128_CBC_SHA256<br>• TLS_RSA_WITH_AES_256_CBC_SHA256<br>However, when using an IBM JDK, the values will be:<br>• SSL_RSA_WITH_AES_128_CBC_SHA<br>• SSL_RSA_WITH_AES_256_CBC_SHA<br>• SSL_RSA_WITH_AES_128_CBC_SHA256<br>• SSL_RSA_WITH_AES_256_CBC_SHA256 |

## Deprecated Features

The following is a list of features deprecated in OrbixSSL Java:

| Feature | Description | Feature Removed | When Deprecated |
|---|---|---|---|
| Support for the following cipher suites:<br>• SSLV3_RSA_WITH_RC4_128_SHA<br>• SSLV3_RSA_WITH_RC4_128_MD5<br>• SSLV3_RSA_WITH_3DES_EDE_CBC_SHA<br>• SSLV3_RSA_WITH_DES_CBC_SHA<br>• SSLV3_RSA_EXPORT_WITH_DES40_CBC_SHA<br>• SSLV3_RSA_EXPORT_WITH_RC2_CBC_40_MD5<br>• SSLV3_RSA_EXPORT_WITH_RC4_40_MD5 | See "Cipher Suite Values" for replacements. | No | Orbix 3.3.13 |

# Resolved Issues

The resolved issues for OrbixSSL Java that customers have reported are listed in this section. The numbers that follow each issue are the Reported Problem Incident number followed by the Customer Incident Numbers (in parentheses). RPIs that have numbers only (and no text) are included to confirm that the RPIs have been fixed, since no further information is required.

- The sample certificates shipped with the product have been updated with expiry dates in the year 2035.

  RPI 1094449 (2700365)

- A fix protects Orbix 3.3 against the POODLE vulnerability of the SSL v3 encryption protocol. See "Security Protocols" for details of the new configuration variables introduced.

  RPI 1097034 (2801728)

- Certificates with UTF-8 strings did not work in Orbix 3.3.12, because of an issue with the underlying Baltimore toolkit. That toolkit has been replaced in Orbix 3.3.13 with JSSE, which can handle UTF-8 strings.

  RPI 1099227 (2816136)

- Support for SHA-256 has been added to Orbix 3.3.13 for both C++ and Java.

  Support for the following cipher suites has been added:

  ```
  TLS_RSA_WITH_AES_128_CBC_SHA
  TLS_RSA_WITH_AES_256_CBC_SHA
  TLS_RSA_WITH_AES_128_CBC_SHA256
  TLS_RSA_WITH_AES_256_CBC_SHA256
  ```

  For Orbix Java 3.3.13, if using cipher suite `TLS_RSA_WITH_AES_256_CBC_SHA` or `TLS_RSA_WITH_AES_256_CBC_SHA256`, the JDK must have the JCE Unlimited Strength Jurisdiction Policy Files installed.

  RPI 1099424 (2820682)