



TIBCO Rendezvous®

Release Notes

Version 8.7.0 | October 2023

Contents

New Features	3
Deprecated and Removed Features	4
Deprecated Features	4
Removed Features	4
Removed Platforms	5
Migration and Compatibility	6
OpenSSL V1.1.1 to 3.0 Migration	6
Changes in OpenSSL 3.0	7
Closed Issues	9
Known Issues	11
Special Note for IBM i	13
TIBCO Documentation and Support Services	14
Legal and Third-Party Notices	17

New Features

The following features have been added in this release of TIBCO Rendezvous®:

Prometheus Endpoints

TIBCO Rendezvous daemons (rvd, rvrd, rvsd, rvsrd) now provide two Prometheus HTTP/S endpoints: /metrics and /metrics/subscriptions. The /metrics endpoint provides basic metrics, for example client counts, subscription counts, inbound messages, outbound messages, for services supported by the daemon. The /metrics/subscriptions endpoint provides a list of every user subject and the number of subscribers on that subject for services supported by the daemon.

For more information, see the [Prometheus Endpoints](#) section of the Administration Guide.

Secure Upgrade

TIBCO Rendezvous client applications can be upgraded to use the Rendezvous Secure Daemon client library (TLS and client authorization) using environment variables and without code changes.

Using the Secure Daemon client library requires the use of Rendezvous Secure Daemons (rvsd or rvsrd) or the TIBCO Rendezvous Network Service (TRNS).

For more information, see the [Secure Daemon](#) section of the Concepts Guide.

OpenSSL Support

TIBCO Rendezvous® now supports OpenSSL 3.0.9. For more information, see [OpenSSL V1.1.1 to 3.0 Migration](#) section of TIBCO Rendezvous® Release Notes.

.NET Support

TIBCO Rendezvous® now supports .NET 6.

Deprecated and Removed Features

The following features have been deprecated or removed as of this release of TIBCO Rendezvous®.

Deprecated Features

Affected Component	Description	Deprecated Release
macOS 64-bit x86-64	Support for the macOS 64-bit x86-64 platform is deprecated. It is going to be removed in a future release. macOS on 64-bit arm64 is going to be supported instead.	8.7.0

Removed Features

Affected Component	Description	Deprecated Release	Removed Release
IPM	IPM on Windows is removed.	8.6.0	8.7.0
Relay Agent (rvrad)	The Relay Agent (rvrad) is removed.	8.6.0	8.7.0

Removed Platforms

Affected Component	Description	Deprecated Release	Removed Release
32-Bit Windows	Support for the 32-Bit Windows platform is removed.	8.6.1	8.7.0

For information on currently supported platforms, see the Rendezvous [Readme](#) file for Release 8.7.0.

Migration and Compatibility

The following information provides migration procedures for this release of TIBCO Rendezvous®.

PKCS12 certificates created with OpenSSL versions prior to 3.0 must be updated. The default PKCS12 settings used by OpenSSL versions prior to 3.0 are considered insecure and not supported by default.

OpenSSL V1.1.1 to 3.0 Migration

Industry security guidelines are now recommending that certificates, ciphers and keys originally created using older protocols be upgraded to newer, stronger implementations as soon as possible to prevent unauthorized access to applications and systems. It is important for TIBCO Messaging customers to review and update current security configurations as soon as possible.

In upcoming releases, TIBCO Enterprise Message Service, TIBCO FTL/eFTL, and TIBCO Rendezvous will require strengthening ciphers and certificates, and removing older, exploitable protocols. Upcoming releases are introducing a new set of minimum requirements that will affect the backwards compatibility of older certificates, ciphers and keys. Customers should review their current configurations and begin updating as soon as possible for a smooth transition to the new messaging product releases. The “openssl” command line utility, version 1.1.1 and later, can be used to update existing installations before this transition.

TIBCO Rendezvous - RVRD secure neighbor connections or RVSD/RVSRD client connections may be affected.

- Certificates, whether specified in PKCS#12 files or copied into the daemon configurations or elsewhere, may need to be updated as indicated below.
- PKCS#12 files specified in RVRD configurations or used in RVSD/RVSRD connections may need to be converted as specified below.

Changes in OpenSSL 3.0

As part of this strengthening of security, TIBCO is transitioning from OpenSSL 1.1.1 to OpenSSL 3.0. The new version attempts to simplify such things as cipher suite selection and key length choices using a security level setting (SECLEVEL) from 0 to 5. The default SECLEVEL is 1, and includes the following restrictions, as documented on the OpenSSL site:

- RSA, DSA and DH keys shorter than 1024 bits and ECC keys shorter than 160 bits are prohibited.
- All export cipher suites are prohibited.
- SSL version 2 is prohibited.
- Any cipher suite using MD5 for the MAC is also prohibited.
- Signatures using SHA1 and MD5 are also forbidden.

TIBCO products impose additional restrictions beyond these:

- SSL version 3 is disabled.
- TLS versions 1.0 and 1.1 are disabled.

Additional restrictions may be applied in the future as best practices evolve. Because of these restrictions, many of the cipher suites available in OpenSSL 1.1.1 are, by default, disabled. Certificates and keys that do not meet these criteria will fail.

The first consequence of this that may be noticed is that PKCS#12 files encrypted with older ciphers will no longer be readable. This is because, by default, older utilities produced files that use RC2 encryption to protect the private key. RC2 is considered a legacy algorithm in OpenSSL 3.0. Not only does it not meet the criteria of SECLEVEL 1, it is not actually compiled into the main library. See below for instructions on converting older PKCS#12 files to a format acceptable to OpenSSL 3.0.

Converting the PKCS#12 file to newer ciphers will, of course, introduce the requirement that all consumers of the file must support the new ciphers. Because TIBCO Rendezvous Java clients use OpenSSL, the Java version is not relevant to compatibility.

Even after the file is converted, if the key algorithm or key size are not acceptable by modern standards, OpenSSL will reject any certificate based on that key. Customers or users need to replace existing certificates with new ones that meet the requirements of SECLEVEL 1.

There are other reasons that OpenSSL 3.0 may reject a customer generated certificate. OpenSSL 3.0 generally enforces the rules specified in the applicable RFCs much more strictly. For instance, the following errors may come up:

- Path length given without key usage
- Missing Authority Key Identifier
- Missing Subject Key Identifier
- Basic Constraints of CA cert not marked critical
- CA cert does not include key usage extension

This is not an exhaustive list, but represents a few of the errors we have seen in practice.

The restrictions on actual TLS cipher suite selection should be benign, since virtually all clients support at least one cipher mode that meets the criteria.

Converting PKCS#12 Files

To convert a legacy PKCS#12 file to newer algorithms using **OpenSSL 1.1**, use the following commands:

```
openssl pkcs12 -in sample.p12 -passin pass:password -nodes > tmp.txt
```

```
openssl pkcs12 -in tmp.txt -out fixed_sample.p12 -macalg SHA256 -keypbe AES-256-CBC -certpbe AES-256-CBC -export -passout pass:password
```

The corresponding commands for **OpenSSL 3.0**:

```
openssl pkcs12 -in sample.p12 -passin pass:password -noenc -legacy > tmp.txt
```

```
openssl pkcs12 -in tmp.txt -out fixed_sample.p12 -export -passout pass:password
```

The result can be verified with the following command:

```
openssl pkcs12 -in fixed_sample.p12 -info -noenc -noout -passin pass:password
```

If the output contains “RC2” in any of the text, then the p12 file is incompatible with OpenSSL 3.0.

Closed Issues

The following issues have been fixed in this release of TIBCO Rendezvous®:

Closed Issues

Key	Summary
RV-4001	The CM client library review-ledger API no longer truncates CM sequence numbers if they exceed 32 bits.
RV-3982	The platform target set in the dotnet samples project files is now x64.
RV-3980	The self-signed certificate generated automatically by Rendezvous daemons matches the security level requested using the <code>-tls-ciphers</code> option.
RV-3978	You can create secure neighbor connections using the <code>tibrvcfg</code> tool.
RV-3964	Rendezvous daemons using the <code>-reuse-port</code> option no longer exits unexpectedly if the process supports file descriptors greater than 1024 bytes.
RV-3948	The RPATH of TIBCO Rendezvous CM, CMQ, and FT libraries decorated with "64" now references decorated libraries.
RV-3929	RVDA now supports the URL semantics for the latest TIBCO FTL servers.
RV-3894	The neighbor hostname limit for routers is now 253 bytes.
RV-3550, RV-3922	The <code>TibrvDispatcher</code> from <code>tibrvnative.jar</code> no longer exits unexpectedly after handling

Key	Summary
	internal protocol messages.
RV-3282	Long CM subject names no longer prevents the CM confirmation from completing. This could happen if the length of the CM subject name in addition to the CM advisory preamble exceeded the maximum subject length.
RV-2923	To accommodate long alias lists and comments, the maximum supported network service entry size (getservbyname_r) is now 4 KB.

Known Issues

The following issues exist in this release of TIBCO Rendezvous®:

Key	Summary
RV-3694	<p>Summary: Message Access after Java Dispose</p> <p>After calling <code>TibrvMsg.dispose</code> to release a message, the Java methods <code>TibrvMsg.getSendSubject()</code> and <code>TibrvMsg.getReplySubject()</code> retrieve null rather than throwing an exception.</p> <p>Workaround: None.</p>
RV-3806	<p>Summary: On macOS, installing the package may result in a system prompt stating the package cannot be installed because the developer cannot be verified. This happens when the installation package was downloaded through a Web browser and consequently labeled as quarantined by the operating system.</p> <p>Workaround: This will be addressed in a future release. In the meantime, a workaround consists of removing the quarantine flag from the package prior to unzipping it. For example: <code>xattr -d com.apple.quarantine TIB_rv_8.6.0_macosx_x86_64.zip</code></p>
RV-3863	<p>Summary: If you install TIBCO Rendezvous® version 8.6.1 or later on a machine where TIBCO Rendezvous® V8.6.0 was installed using 'rpm -ivh', a conflict of files error message is generated.</p>

Key	Summary
	Workaround: Use ' rpm -ivh TIB_rv_8.6.1_linux_x86_64.rpm -U' to upgrade to TIBCO Rendezvous® version 8.6.1.

Special Note for IBM i

TIBCO Rendezvous® software does not support the following features on IBM i (formerly i5 and AS/400) platforms:

- Secure daemons (rvsd and rvsrd)
- Secure daemon API calls

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the [Product Documentation website](#), mainly in HTML and PDF formats.

The [Product Documentation website](#) is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The following documentation for this product is available on the [TIBCO Rendezvous® Product Documentation](#) page:

- *TIBCO Rendezvous® Concepts* - Read this book first. It contains basic information about Rendezvous components, principles of operation, programming constructs and techniques, advisory messages, and a glossary. All other books in the documentation set refer to concepts explained in this book.
- *TIBCO Rendezvous® Administration* - Begins with a checklist of action items for system and network administrators. This book describes the mechanics of TIBCO Rendezvous® licensing, network details, plus a chapter for each component of the TIBCO Rendezvous® software suite. Readers should have TIBCO Rendezvous Concepts at hand for reference.
- *TIBCO Rendezvous® Installation* - Includes step-by-step instructions for installing TIBCO Rendezvous® software on various operating system platforms.
- *TIBCO Rendezvous® C Reference* - Detailed descriptions of each data type and function in the TIBCO Rendezvous® C API. Readers should already be familiar with the C programming language, as well as the material in TIBCO Rendezvous Concepts.
- *TIBCO Rendezvous® C++ Reference* - Detailed descriptions of each class and method in the TIBCO Rendezvous® C++ API. The C++ API uses some data types and functions from the C API, so we recommend the TIBCO Rendezvous C Reference as an

additional resource. Readers should already be familiar with the C++ programming language, as well as the material in TIBCO Rendezvous Concepts.

- *TIBCO Rendezvous® .NET Reference* - Detailed descriptions of each class and method in the TIBCO Rendezvous® .NET interface. Readers should already be familiar with either C# or Visual Basic .NET, as well as the material in TIBCO Rendezvous Concepts.
- *TIBCO Rendezvous® Java Reference* - Detailed descriptions of each class and method in the TIBCO Rendezvous® Java language interface. Readers should already be familiar with the Java programming language, as well as the material in TIBCO Rendezvous Concepts.
- *TIBCO Rendezvous® Configuration Tools* - Detailed descriptions of each Java class and method in the TIBCO Rendezvous® configuration API, plus a command line tool that can generate and apply XML documents representing component configurations. Readers should already be familiar with the Java programming language, as well as the material in TIBCO Rendezvous Administration.
- *TIBCO Rendezvous® z/OS Installation and Configuration* - Information about TIBCO Rendezvous® for IBM z/OS systems regarding installation and maintenance. Some information may be also useful for application programmers.
- *TIBCO Rendezvous® Release Notes* - Lists new features, changes in functionality, deprecated features, migration and compatibility information, closed issues and known issues.

To directly access documentation for this product, double-click the following file:

`TIBCO_HOME/release_notes/TIB_rv_8.7.0_docinfo.html`

where `TIBCO_HOME` is the top-level directory in which TIBCO products are installed.

- On Windows, the default `TIBCO_HOME` is `C:\tibco`.
- On UNIX systems, the default `TIBCO_HOME` is `/opt/tibco`.

How to Contact Support for TIBCO Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our [product Support website](#).
- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the our [product Support website](#). If you do not have a username, you can

request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the [TIBCO Ideas Portal](#). For a free registration, go to [TIBCO Community](#).

Legal and Third-Party Notices

SOME CLOUD SOFTWARE GROUP, INC. (“CLOUD SG”) SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, “INCLUDED SOFTWARE”). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

USE OF CLOUD SG SOFTWARE AND CLOUD SERVICES IS SUBJECT TO THE TERMS AND CONDITIONS OF AN AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER AGREEMENT WHICH IS DISPLAYED WHEN ACCESSING, DOWNLOADING, OR INSTALLING THE SOFTWARE OR CLOUD SERVICES (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH LICENSE AGREEMENT OR CLICKWRAP END USER AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE SAME TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, TIB, Information Bus, FTL, eFTL, Rendezvous, and LogLogic are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG’s Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

Cloud SG software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the “readme” file

for the availability of a specific version of Cloud SG software on a specific operating system platform.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. CLOUD SG MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), THE PROGRAM(S), AND/OR THE SERVICES DESCRIBED IN THIS DOCUMENT AT ANY TIME WITHOUT NOTICE.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "README" FILES.

This and other products of Cloud SG may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.tibco.com/patents>.

Copyright © 1997-2023. Cloud Software Group, Inc. All Rights Reserved.