

# **RTI TLS Support**

**Release Notes**

**Version 5.3.1**



© 2018 Real-Time Innovations, Inc.  
All rights reserved.  
Printed in U.S.A. First printing.  
March 2018.

## Trademarks

Real-Time Innovations, RTI, NDDS, RTI Data Distribution Service, DataBus, Connex, Micro DDS, the RTI logo, IRTI and the phrase, “Your Systems. Working as one,” are registered trademarks, trademarks or service marks of Real-Time Innovations, Inc. All other trademarks belong to their respective owners.

## Copy and Use Restrictions

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form (including electronic, mechanical, photocopy, and facsimile) without the prior written permission of Real-Time Innovations, Inc. The software described in this document is furnished under and subject to the RTI software license agreement. The software may be used or copied only under the terms of the license agreement.

## Third-Party Copyright Notices

Note: In this section, "the Software" refers to third-party software, portions of which are used in Connex DDS; "the Software" does not refer to Connex DDS.

This product implements the DCPS layer of the Data Distribution Service (DDS) specification version 1.4 and the DDS Interoperability Wire Protocol specification version 2.2, both of which are owned by the Object Management, Inc. Copyright 2015 Object Management Group, Inc. The publication of these specifications can be found at the Catalog of OMG Data Distribution Service (DDS) Specifications. This documentation uses material from the OMG specification for the Data Distribution Service, section 2.

Reprinted with permission. Object Management, Inc. © OMG. 2013.

Portions of this product were developed using ANTLR ([www.ANTLR.org](http://www.ANTLR.org)). This product includes software developed by the University of California, Berkeley and its contributors.

Portions of this product were developed using AspectJ, which is distributed per the CPL license. AspectJ source code may be obtained from Eclipse. This product includes software developed by the University of California, Berkeley and its contributors.

Portions of this product were developed using MD5 from Aladdin Enterprises.

Portions of this product include software derived from Fmatch, (c) 1989, 1993, 1994 The Regents of the University of California. All rights reserved. The Regents and contributors provide this software "as is" without warranty.

Portions of this product were developed using EXPAT from Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Expat maintainers. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

Copyright © 1994–2013 Lua.org, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### **Technical Support**

Real-Time Innovations, Inc.

232 E. Java Drive

Sunnyvale, CA 94089

Phone: (408) 990-7444

Email: [support@rti.com](mailto:support@rti.com)

Website: <https://support.rti.com/>

# Contents

---

## **TLS Support Release Notes**

1 Supported Platforms .....	1
2 Compatibility with Current Software .....	1
3 Backward Compatibility .....	2
4 What's New in 5.3.1 .....	2
5 What's New in 5.3.0 .....	2
5.1 New Platforms .....	2
5.2 Platforms on Legacy Operating Systems .....	3
5.3 Removed Platforms .....	3
6 Third-Party Licenses .....	4

# TLS Support Release Notes

## 1 Supported Platforms

TLS Support is available for the platforms in the following table.

**Table 1.1 Supported Platforms**

Operating System	Version
Android™	All platforms in the <i>RTI® Connex® DDS Platform Notes</i> for the same version number, except not supported on SUSE® 11. Among custom target platforms, only RedHawk™ Linux 6.5 is supported.
iOS®	
Linux®	
OS X®	
QNX®	All QNX Neutrino® 6.5 and higher platforms in the <i>RTI Connex DDS Core Libraries Platform Notes</i> for the same version number.
Windows®	All platforms in the <i>RTI Connex DDS Platform Notes</i> for the same version number.

For details on these platforms, see the *RTI Connex DDS Platform Notes*:

## 2 Compatibility with Current Software

RTI TLS Support is designed for use with the TCP transport that is included with RTI Connex DDS. If you choose to use TLS Support, it must be installed on top of an existing TLS Support installation with the same version number. It can only be used on architectures that support the TCP transport (see the *RTI Core Libraries Platform Notes*).

RTI TLS Support 5.3.1 is compatible with OpenSSL 1.0.2n.

## 3 Backward Compatibility

If you are upgrading from OpenSSL 1.0.1 to OpenSSL 1.0.2 or above: The number of bits of any Diffie-Hellman (DH) parameters must now be at least 1024 (see <https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/>). Therefore, if you are using the property `tls-cipher.dh_param_files` and there is a DH parameter file that has fewer than 1024 bits, you must regenerate the file with at least 1024 bits.

## 4 What's New in 5.3.1

This release adds support for the following platforms:

Operating System	CPU	Compiler	RTI Architecture Abbreviation
OS X 10.13	x64	clang 9.0	x64Darwin17clang9.0
QNX Neutrino 7.0	ARMv8	qcc 7.0.0 with LLVM default libraries	armv8QNX7.0.0qcc_cxx5.4.0
		qcc 7.0.0 with GNU C++ libraries	armv8QNX7.0.0qcc_gpp5.4.0
	x64	qcc 7.0.0 with LLVM default libraries	x64QNX7.0.0qcc_cxx5.4.0
		qcc 7.0.0 with GNU C++ libraries	x64QNX7.0.0qcc_gpp5.4.0
RedHawk™ Linux 6.5 (Available through custom support)	i86	gcc 4.9.2	i86RedHawk6.5gcc4.9.2
	x64	gcc 4.9.2	x64RedHawk6.5gcc4.9.2
Ubuntu® 16.04 LTS	ARMv8 (AArch64)	gcc 5.4.0	armv8Linux4.4gcc5.4.0
Wind River® Linux 7	x64	gcc 4.9.1	x64WRLinux7gcc4.9.1
Windows 10	x86	Visual Studio 2017 Update 2	i86Win32VS2017
Windows Server 2008 R2	x64	Visual Studio 2017 Update 2	x64Win64VS2017
Windows Server 2016			

For details on these platforms, see the *RTI Connex DDS Platform Notes*.

## 5 What's New in 5.3.0

### 5.1 New Platforms

This release adds support for platforms on the following operating systems:

- OS X 10.12
- Red Hat Enterprise Linux 6.8
- Ubuntu 16.04 LTS
- Windows Server 2016

For details on these platforms, see the *RTI Connex DDS Platform Notes*.

### 5.2 Platforms on Legacy Operating Systems

The following legacy operating systems have reached end-of-life from their corresponding vendors. Please contact RTI support or your account manager if you require version 5.3 to run on these platforms:

- CentOS 5.x
- Red Hat Enterprise Linux 5.x

### 5.3 Removed Platforms

Platforms on the following operating systems are no longer supported:

- OS X 10.8
- Red Hat Enterprise Linux 4
- Windows Vista, Windows XP Pro, Windows 2003

## 6 Third-Party Licenses

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR



OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).