

RTI TLS Support

Release Notes

Version 6.0.0



© 2019 Real-Time Innovations, Inc.
All rights reserved.
Printed in U.S.A. First printing.
February 2019.

Trademarks

Real-Time Innovations, RTI, NDDS, RTI Data Distribution Service, 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.

This is an independent publication and is neither affiliated with, nor authorized, sponsored, or approved by, Microsoft Corporation.

The security features of this product include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

Technical Support

Real-Time Innovations, Inc.

232 E. Java Drive

Sunnyvale, CA 94089

Phone: (408) 990-7444

Email: support@rti.com

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

Contents

1 Supported Platforms	1
2 Compatibility	2
3 What's New in 6.0.0	
3.1 New Platforms	3
3.2 Updated OpenSSL Version	3
4 Third-Party Licenses	4

1 Supported Platforms

This release of *RTI® TLS Support* is supported on the platforms in [Table 1.1 Supported Platforms](#).

Table 1.1 Supported Platforms

Operating System	Version
Android®	All Android platforms listed in the <i>RTI Connex® DDS Core Libraries Release Notes</i> for the same version number.
iOS®	All iOS platforms listed in the <i>RTI Connex DDS Core Libraries Release Notes</i> for the same version number.
Linux®	All Linux platforms in the <i>RTI Connex DDS Core Libraries Release Notes</i> for the same version number, except not supported on SUSE® Linux Enterprise Server.
OS X®	All OS X platforms listed in the <i>RTI Connex DDS Core Libraries Release Notes</i> for the same version number.
QNX®	All QNX Neutrino® 6.5 and higher platforms listed in the <i>RTI Connex DDS Core Libraries Release Notes</i> for the same version number.
Windows®	All Windows platforms listed in the <i>RTI Connex DDS Core Libraries Release Notes</i> for the same version number.

TLS Support is also supported on the platforms in [Table 1.2 Custom Supported Platforms](#); these are target platforms for which RTI offers custom support. If you are interested in these platforms, please contact your local RTI representative or email sales@rti.com.

Table 1.2 Custom Supported Platforms

Operating System	Version
Linux	RedHawk™ Linux 6.5 Wind River® Linux 8
QNX	QNX Neutrino 6.6 on x86 and ARMv7 CPUs

2 Compatibility

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 Connex DDS Core Libraries Platform Notes*).

TLS Support 6.0.0 is API-compatible with OpenSSL® versions 1.0.1c through 1.0.2o. It is not API-compatible with OpenSSL® 1.1.0a or above. Note that *TLS Support* 6.0.0 has only been tested by RTI using OpenSSL 1.0.2o.

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.

For backward compatibility information between 6.0.0 and previous releases, see the *Migration Guide* on the RTI Community Portal (<https://community.rti.com/documentation>).

3 What's New in 6.0.0

3.1 New Platforms

This release adds support for the following platforms.

Operating System	CPU	Compiler	RTI Architecture Abbreviation
Ubuntu 18.04 LTS	x64	gcc 7.3.0	x64Linux4gcc7.3.0
Wind River Linux 8	ARMv7	gcc 5.2.0	armv7aWRLinux8gcc5.2.0 (custom target platform)

See the *RTI Connex DDS Core Libraries Platform Notes* for details.

3.2 Updated OpenSSL Version

This release uses OpenSSL 1.0.2o (instead of 1.0.2n).

4 Third-Party Licenses

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

Copyright (c) 1998-2015 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.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. 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/>)

4. 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.
5. 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.
6. 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 (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).