RTI TLS Support

Release Notes

Version 6.0.1

Printed in U.S.A. First printing.
November 2019.

Trademarks

Copy and Use Restrictions

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

Chapter 1 Supported Platforms

This release of *RTI® TLS Support* is supported on the platforms in Table 1.1 Supported Platforms.

For details on these platforms, see the *RTI Connext DDS Core Libraries Platform Notes*.

Table 1.1 Supported Platforms

Operating System	Version
Android®	All Android platforms listed in the *RTI Connext® DDS Core Libraries Release Notes* for the same version number.
iOS®	All iOS platforms listed in the *RTI Connext DDS Core Libraries Release Notes* for the same version number.
Linux®	All Linux platforms in the *RTI Connext DDS Core Libraries Release Notes* for the same version number, except SUSE® Linux Enterprise Server 11 and 12.
macOS®	All macOS platforms listed in the *RTI Connext DDS Core Libraries Release Notes* for the same version number.
QNX®	All QNX Neutrino® 6.5 and higher platforms listed in the *RTI Connext DDS Core Libraries Release Notes* for the same version number.
Windows®	All Windows platforms listed in the *RTI Connext DDS Core Libraries Release Notes* 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	Debian® 7 (Arm v7) RedHawk™ Linux 6.5 (x86 and x64) Wind River® Linux 8 (PPC e6500 and Arm v7) Yocto Project® 2.5 (Arm v7)
QNX	QNX Neutrino 6.6 (x86 and Arm v7)

Chapter 2 Compatibility

TLS Support is designed for use with the TCP transport that is included with *RTI Connext 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 Connext DDS Core Libraries Platform Notes*).

TLS Support 6.0.1 is API-compatible with OpenSSL® versions 1.1.0a through 1.1.1d. It is not API-compatible with previous versions to OpenSSL® 1.1.0a. Note that *TLS Support* 6.0.1 has only been tested by RTI using OpenSSL 1.1.1d. If you need *TLS Support* 6.0.1 to run against older versions of OpenSSL®, please contact support@rti.com.

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 6.0.1 and previous releases, see the *Migration Guide* on the RTI Community Portal (https://community.rti.com/documentation).

Chapter 3 What's New in 6.0.1

3.1 Added platforms

This release adds support for these platforms:

- Android 9 (Arm v7, Arm v8 64-bit)
- macOS 10.14 (x64)
- Red Hat Enterprise Linux 8 (x64)
- Wind River Linux 8 (PPC e6500) (Custom-supported target platform. Contact your RTI sales representative or sales@rti.com for more information.)
- Windows 10 (x86, x64) with Visual Studio® 2019
- Windows Server 2016 (x86, x64) with Visual Studio 2019
- Yocto Project 2.5 (Arm v7) (Custom-supported target platform. Contact your RTI sales representative or sales@rti.com for more information.)

3.2 Removed platforms

These platforms are no longer supported:

- macOS 10.11
- Windows 7
- Windows Server 2008 R2

3.3 Updated OpenSSL Version

This release uses OpenSSL 1.1.1d (instead of 1.0.2o).

Chapter 4 Previous Release

4.1 What's New in 6.0.0

4.1.1 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	Arm v7	gcc 5.2.0	armv7aWRLinux8gcc5.2.0 (custom target platform)

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

4.1.2 Updated OpenSSL Version

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

Chapter 5 Third-Party Licenses

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

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