

RTI TLS Support

Release Notes

Version 6.1.0



© 2021 Real-Time Innovations, Inc.
All rights reserved.
Printed in U.S.A. First printing.
April 2021.

Trademarks

RTI, Real-Time Innovations, Connex, NDDS, the RTI logo, 1RTI 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/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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	1
Chapter 2 Compatibility	3
Chapter 3 What's New in 6.1.0	
3.1 Added Platforms	4
3.2 Removed Platforms	4
3.3 Updated OpenSSL Version	5
3.4 Target OpenSSL Bundles Distributed as .rtipkg Files	5
3.5 Changes to OpenSSL Static Library Names	5
Chapter 4 What's Fixed in 6.1.0	
4.1 Still reachable memory leaks	6
4.2 No way to configure TLS 1.3 ciphers	6
Chapter 5 Known Issues	
5.1 Possible Valgrind still-reachable leaks when loading dynamic libraries	7

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 Connex DDS Core Libraries Platform Notes*.

Note: POSIX®-compliant architectures that end with "FACE_GP" are not supported.

Table 1.1 Supported Platforms

Operating System	Version
Android® <i>Available on demand</i>	All Android 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 SUSE® Linux Enterprise Server.
macOS®	All macOS 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	CPU	RTI Architecture Abbreviation
Linux	RedHawk™ Linux 6.5	x86	i86RedHawk6.5gcc4.9.2
		x64	x64RedHawk6.5gcc4.9.2
	Wind River® Linux 8	Arm v7	armv7aWRLinux8gcc5.2.0
	Yocto Project® 2.5	Arm v8	armv8Linux4gcc7.3.0
QNX	QNX Neutrino 6.6	Arm v7	armv7aQNX6.6.0qcc_cpp4.7.3
		x86	i86QNX6.6qcc_cpp4.7.3
	QNX Neutrino 7.0.4	Arm v7	armv7QNX7.0.0qcc_cxx5.4.0 ^a

^aarmv7QNX7.0.0qcc_cxx5.4.0 was tested with QNX Neutrino 7.0.0 kernel.

Chapter 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 6.1.0 is API-compatible with OpenSSL® versions 1.1.0a through 1.1.1k. It is not API-compatible with versions earlier than OpenSSL 1.1.0a. Note that *TLS Support* 6.1.0 has only been tested by RTI using OpenSSL 1.1.1k. If you need *TLS Support* 6.1.0 to run against older versions of OpenSSL, please contact support@rti.com.

TLS Support 6.1.0 uses TLS 1.3. When communicating with *TLS Support* 6.0.0 or below, *TLS Support* 6.1.0 uses TLS 1.1.

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

Chapter 3 What's New in 6.1.0

3.1 Added Platforms

This release adds support for these platforms:

- macOS 10.15 (x64) (x64Darwin17clang9.0)
- QNX Neutrino 7.0.4 (Arm v8) (armv8QNX7.0.0qcc_gpp5.4.0, armv8QNX7.0.0qcc_cxx5.4.0)
- QNX Neutrino 7.0.4 (x64) (x64QNX7.0.0qcc_gpp5.4.0, x64QNX7.0.0qcc_cxx5.4.0)
- QNX Neutrino 7.0.4 (Arm v7) (custom supported platform armv7QNX7.0.0qcc_cxx5.4.0)
- Red Hat® Enterprise Linux 7.6 (x64) (x64Linux3gcc4.8.2)
- Ubuntu® 18.04 LTS (Arm v7) (armv7Linux4gcc7.5.0)
- Ubuntu 18.04 LTS (Arm v8) (armv8Linux4gcc7.3.0)
- Ubuntu 20.04 LTS (x64) (x64Linux4gcc7.3.0)
- Yocto Project 2.5 (Arm v8) (custom supported platform armv8Linux4gcc7.3.0)

3.2 Removed Platforms

These platforms are no longer supported:

- Android™ 5.0, 5.1
- Debian 7 (custom supported platform)
- iOS®
- macOS 10.12
- Ubuntu 12.04 LTS
- Wind River Linux 7

3.3 Updated OpenSSL Version

This release uses OpenSSL® 1.1.1k (instead of 1.1.1d).

3.4 Target OpenSSL Bundles Distributed as .rtipkg Files

Target OpenSSL bundles are now distributed as **.rtipkg** files. Once installed, the OpenSSL files are available in `<installation_folder>/third_party`.

3.5 Changes to OpenSSL Static Library Names

The OpenSSL static library names no longer have a "z" suffix. **libcryptoz** has been renamed to **libcrypto**, and **libsslz** has been renamed to **libssl**. When including the static libraries in a makefile, we recommend including the whole path to the OpenSSL static libraries in order to avoid confusion with the dynamic libraries. Here is an example:

```
gcc -o myApp myApp.o -L$NDDSHOME/lib/$ARCH -lndstransporttcpz -lndstlsz -lndscz -lndscorez  
$RTI_OPENSSLHOME/$ARCH/release/lib/libssl.a $RTI_OPENSSLHOME/$ARCH/release/lib/libcrypto.a
```

In addition, the Android static library **librtisslsupportz** has been removed. You may use **libcrypto** and **libssl** instead.

Chapter 4 What's Fixed in 6.1.0

This section describes bugs fixed in 6.1.0. These fixes have been made since 6.0.1 was released.

4.1 Still reachable memory leaks

After shutting down an application using (D)TLS, memory profilers, such as ValgrindTM, may have reported memory leaks categorized as still reachable memory leaks. These leaks were harmless and could not lead to unbounded memory growth. This problem has been fixed.

[RTI Issue ID COREPLG-510]

4.2 No way to configure TLS 1.3 ciphers

The property **tls.cipher.cipher_list** applies only to TLS 1.2 communication, which occurs when either *DomainParticipant* is using a *Connex DDS* version older than 6.0.1. When both *DomainParticipants* are using *Connex DDS* 6.0.1 or later, they use TLS 1.3 communication, and the **tls.cipher.cipher_list** property does not apply. There was no way to configure the list of ciphers to be used when using TLS 1.3. This problem has been fixed by introducing a new property, **tls.cipher.ciphersuites**. See the OpenSSL manual page for `SSL_CTX_set_ciphersuites` for more information on the format of this string.

[RTI Issue ID COREPLG-534]

Chapter 5 Known Issues

5.1 Possible Valgrind still-reachable leaks when loading dynamic libraries

If you load any dynamic libraries, you may see "still reachable" memory leaks in "dlopen" and "dlclose". These leaks are a result of a bug in Valgrind (<https://bug-s.launchpad.net/ubuntu/+source/valgrind/+bug/1160352>).

This issue affects the *Core Libraries*, *Security Plugins*, *Secure WAN*, and *TLS Support*.

[RTI Issue IDs CORE-9941, SEC-1026, and COREPLG-510]