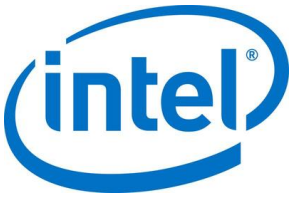


Intel® QuickAssist for Windows*

Release Notes

Package Version: QAT1.3.0-0009

April 2020

Revision 003US

Document Number: 337758-003US

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, Xeon, and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © Intel Corporation.

Contents

Figures

Tables

Revision History

Revision Number	Description	Revision Date
003	Intel® QuickAssist Software release 1.3.0-0009 • Updated Windows* Software Release version v1.3.0-0009 • Added new sections 1.3.1 What's New and 1.3.2 Software Release History • Updated Features Paragraph 13, compression/decompression features • Updated Section 3.0 removing Neoncity security accelerators • Added Known Issues: QATE 38968, 40170 • Added Resolved Issue: QATE-37219	April 2020
002	Intel QuickAssist Software release v1.1.0-29 • Removed Support for Windows Server 2012 • Added known issues QATE-37219 and QATE-36847 • Resolved QATE-15336, Parcomp/FVL25 Driver Compatibility Issue Server 2012 R2 Update 1 • Section 1.1 Supported Platforms updated	March 2019
001	Initial release.	June 2018

§

1.0 Description of Release

This document contains information on the accompanying Intel® QuickAssist Technology (Intel® QAT) Windows* Software release v1.3.0-0009. This document also describes extensions and deviations from the release functionality described in Table 3, *Intel® QuickAssist Technology Software for Linux* Software Programmer's Guide* for the various platforms that support Intel® QAT.

Note: These release notes may include known issues with third-party or reference platform components that affect the operation of the software.

1.1 Supported Hardware Platforms

The software in this release has been validated against the following devices:

- Intel® QuickAssist Adapter 8960 and 8970
- Intel® Xeon® Scalable Platform with Intel® C62x Chipset (with Intel® QAT)
- Intel® Xeon® D Platform with Intel® C62x Chipset (with Intel® QAT)

Note: Intel® QAT supports Intel® Xeon® Scalable first and second generations.

1.2 Supported Operating Systems

The software in this release has been validated against the following Operating Systems (OS):

- Windows* Server 2019
- Windows* Server 2016

1.3 What's New

New features added for this release include the following:

- Software fallback in the event of hardware failure for cryptography and compression services
- Improved error handling with the Intel® QuickAssist cryptography and compression services

1.4 Intel® QAT Software Release Feature History

Table 1. Intel® QAT Software Release Feature History

Release History	New Features
Release 1.2.0-0018	• Intel® Intelligent Storage Acceleration Library (ISA-L) integration with Intel® QuickAssist compression and decompression services.

Release History	New Features
	• Compression fallback support with ISA-L. • Improved error handling with the Intel® QuickAssist compression services
Release 1.1.0-0029	• Add support for PKE cryptography services
Release 1.0.0-0022	• Initial release that supports Intel® QAT compression and decompression.

1.5 Data Compression Services

This software package provides the following Data Compression services:

- Static Deflate Stateless compression/decompression
- Dynamic Deflate Stateless compression/decompression
- Includes sample code application for compression services – parcomp

For ISA-L integration, the source code and information to build the DLL can be found in Table 3, *Intel® Intelligent Storage Application Library GitHub*. The minimum required version is 2.26.0. The DLL should be placed in the Windows* system32 directory.

The QATZip file includes the following compression/decompression functions:

- `qzInit`
- `qzSetupSession`
- `qzCompress`
- `qzDecompress`
- `qzTeardownSession`
- `qzClose`
- `qzMalloc`
- `qzFree`

1.6 Cryptography Services

This software package also provides the following cryptography services.

Support for PKE cryptography services include:

- Cryptography API: Next-Generation (CNG) support, sometimes referred to as the “BCrypt API.” Refer to Cryptography API: Next-Generation, Table 3.
- An Intel® QuickAssist CNG provider is registered to support the following PKE algorithms:

  -RSA

  -DSA

- ECDSA (P256, P384, P521)
- DH
- ECDH (P256, P384, P521)

- CNG API support in both user mode and kernel mode

  This software release has passed the Windows Hardware Lab Kit (HLK) Certification and contains certified device drivers.

- Public Key Encryption (PKE) services
- Support for PKE cryptography services include:
- Cryptography API: Next-Generation (CNG) support, sometimes referred to as the "`BCrypt API`."

  Refer to *Cryptography API: Next-Generation*, Table 3.

- An Intel® QAT CNG provider that is registered to support the following PKE algorithms:
- Rivest-Shamir-Adleman (RSA)
- Digital Signature Algorithm (DSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA) (P256, P384, P521)
- Diffie–Hellman (DH)
- Elliptic-curve Diffie–Hellman ECDH (P256, P384, P521)
- CNG API support in both user mode and kernel mode

Note: This software release has passed the Windows* Hardware Lab Kit (HLK*) Certification and contains certified device drivers.

1.7 Customer Support

Intel offers support for this software at the Application Program Interface (API) level, defined in Table 2 and Table 3 of the Programmer Guides and API reference manuals. If the field representative has created an account for you, submit support requests via the Online Service Center, https://supporttickets.intel.com/?lang=en-US.

1.8 List of Files in this Release

The Bill of Materials (BOM) is included as a text file in the released software package. This text file is labeled "`filelist`" and located at the top directory level for each release package.

1.9 Reference Documents

Table 2 lists Intel® QuickAssist Technology's generic documentation.

Table 3 lists Intel® QuickAssist Technology specific documentation.

Table 2 lists Intel® QuickAssist Technology Generic Documentation.

Document	Document No./Location
Intel® QuickAssist Technology API Programmer's Guide	330684
Intel® QuickAssist Technology Performance Optimization Guide	330687
Cryptography API: Next-Generation	https://docs.microsoft.com/en-us/windows/desktop/SecCNG/cng-portal

Table 3. Intel® QuickAssist Technology Software Specific Documentation

Document	Document No./Location
Intel® QuickAssist Technology Software for Linux Software Programmer's Guide*	336210

1.10 Terminology

Table 4. Terminology

Term	Description
API	Application Program Interface
AES	Advanced Encryption Standard
BOM	Bill of Materials
CNG	Cryptography API: Next Generation
DH	Diffie–Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic-curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
WHLK*	Windows* Hardware Lab Kit
Intel® QAT	Intel® QuickAssist Technology
OS	Operating System
PKE	Public Key Encryption
RSA	Rivest-Shamir-Adleman

§

2.0 Limitations and Known Issue

This section provides the all known limitations and known issues for windows software release v1.3.0-00009.

2.1 Limitations

This release does not support the following:

- Static Deflate Stateful compression/decompression
- Dynamic Deflate Stateful compression/decompression
- Symmetric (bulk) cryptography algorithms like Advanced Encryption Standard (AES)
- Fallback for Cryptography services
- Virtualization with Microsoft® Hyper-V using SR-IOV

2.2 Known Issues

Table 5 lists the known issues with this software Release.

Table 5. Known Issues with this Release

Title	Cannot disable driver while parcomp (compression) is running
Reference #	QATE-36847
® Description	When running `parcomp` stress tests, you cannot disable all `37c8` Intel® QAT devices. Doing so may cause the driver to disable to spin until the `parcomp` process is stopped. The issue has been observed mostly on Skylake-D systems. Environment: Supermicro* X11 Intel® QAT Microserver with 2x 37C8 devices Windows* Server 2016 W.1.1.0-0029 drivers Steps: 1. Run a `parcomp` stress test. Automation runs with the following parameters: `.\parcomp.exe -i C:\\CompressionFiles\silesia -o C:\\CompressionFiles\compress -p qat -Q -t 6 -k 4096 -j 60 -x 2 -n 200` 2. Disable `37c8` devices, one at a time until no more left (sometimes may occur on the first `37c8` disable). 3. Last, disable should keep spinning until `parcomp` thread is stopped.
Resolution	Disable the Intel® QAT devices only after the compression operations have been completed.
Affected OS	Windows* Server 2019/2016

Title	Cannot disable driver while parcomp (compression) is running
Driver/Module	QAT IA – Compression

Title	Windows Setup /passive install has crypto failures
Reference #	QATE-38404
Description	When you use the '/passive' option for installation, it seems that Crypto will fail after a few iterations.
Resolution	Please use normal GUI installation or when installing using '/passive, use the `/qn'` option.
Affected OS	Windows* Server 2019/2016

Title	WCAT workload has ECDHE curve25519 failure
Reference #	QATE-38965
Description	The `ECDHE` curve "`curve25519`" is the default curve for `ECDHE` in Windows*. The WCAT workload on IIS fails to authenticate when using Intel® QAT to run `ECDHE` and RSA, using the default curve preference order.
Resolution	Two possible resolutions: 1) Change the default `ECDH` curve in Windows to be a curve that is supported by Intel® QAT. The result is that ECDH is executed on Intel® QAT (but not using `curve25519`). 2) Use the `CPMCNGInstaller` tool to unregister ECDH provider for QAT. The result is that `ECDH` is executed on the CPU using the default `curve25519`.
Affected OS	Windows* Server 2019/2016

Title	Parcomp unable to read > 1GB file for compression
Reference #	QATE-40170
Description	Parcomp is unable to read large files (test file was 2.2 GB) for compression. Thus compression would fail.
Resolution	When writing an application with QATZIP, chunk the file into at most 1GB increments.
Affected OS	Windows* Server 2019/2016

Title	`cngtest` does not validate fallback operations are working correctly
Reference #	QATE-38968

Title	`cngtest` does not validate fallback operations are working correctly
Description	Currently, the `cngtest` does not include tests to validate the fallback to the Microsoft* provider works for unsupported algorithms and curves. Environment: Supermicro* X11 Intel® QAT Microserver with 2x 37C8 devices Windows* Server 2016 The `cngtest` cannot validate fallback operations. If encryption is performed by SW, it needs to ensure that decryption can be performed by the Intel® QAT HW or vice-versa.
Resolution	There is currently no workaround for this, and It may be added in a future release.
Affected OS	Windows* Server 2019/2016
Driver/Module	QAT IA – Crypto

2.3 Resolved Issues

Title	Parcomp/FVL25 Driver Compatibility Issue Server 2012 R2 Update 1
Reference #	QATE-15336
Description	During `parcomp` parameter testing (running through hundreds of possible `parcomp` combinations), the `parcomp` executable may stop responding at random times. The issue has only been observed on Windows* Server 2012 R2 Update 1. Environment: Platform: S2600WFQ (Wolf-Pass with Intel® C628 Chipset OS: Windows Server 2016 RS1 Intel® QAT: Driver: QAT1.7.W.1.0.0-1 Steps: Run through hundreds of different `parcomp` combinations. Observe executable crashes. The system is okay if force was killing `parcomp` PID.
Resolution	Windows* Server 2012 is not supported for this release.
Affected OS	Windows* Server 2012
Driver/Module	CPM IA – Compression

Title	Default curve order for elliptic curves not supported by QAT
Reference #	QATE-37219

Description	The default curve order on Windows when using cipher suites with `ECDHE` is as follows:
	`curve25519`
	`NistP256`
	`NistP384`

Title	Default curve order for elliptic curves not supported by QAT

	Since `curve25519` is not supported by Intel® QAT, cryptography operations will fail when using cipher suites with `ECDHE`.
	However, the `NistP256` and `Nist384` curves are supported by Intel® QAT, so if the curve priority order is changed as shown below, cryptography operations when using cipher suites with `ECDHE` will succeed:
	`NistP256`
	`NistP384`
	`curve25519`

Resolution	Modify the default ECC Curve Order as below: 1. Launch the Group Policy Editor: `gpedit.msc` 2. Open Computer `Configuration/Administrative Template/Network/ SSL Configuration Settings` 3. Double-click ECC Curve Order (in the right pane) 4. Click **Enabled** 5. Edit the ECC Curve Order in the priority order described above. 6. Click '**Apply**' and exit the application
Affected OS	Windows* Server 2019/2016
Driver/Module	QAT IA – Crypto

§

3.0 Software Installation

The release package includes the Setup.exe installation application. Use this application to install the package on the targeted OS. For more information on how to install the package, refer to the Readme file included in the package:

```
.\quickassist\README.txt
```

Upon completion of the installation, the `README` text file can also be found in the following folder:

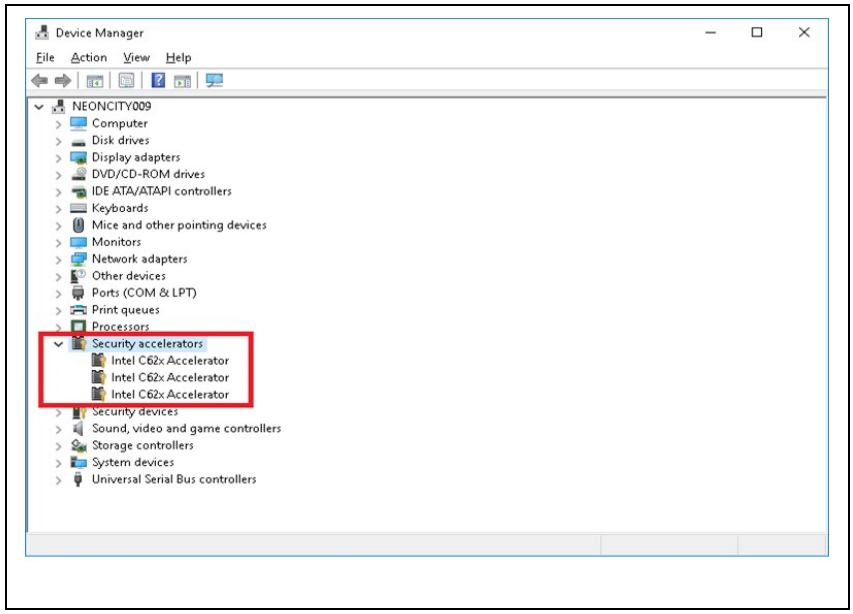
```
<Program Files>\Intel\Intel(R) QuickAssist Technology
```

Note: For those customers that had already have installed the previous version of the Intel® QAT software package, uninstall it and reboot before installing this new production package.

To ensure software installation completed successfully and that Intel® QAT devices are functional, refer to Figure 1. The screenshot lists three “Intel C62x Accelerator” devices under the “Security accelerators” PNP Classification.

Figure 1, Device Manager with Intel® QuickAssist driver installed in Microsoft® Windows

Figure 1. Device Manager with Intel® QuickAssist driver installed in Microsoft® Windows



§

4.0 Test Applications

4.1 Compression Test Application

A compression test application, parcomp, is included in this package. For more information on how to use the parcomp application, refer to the Readme file included in the package. You can find the README file in the following folder upon completion of the installation:

```
<Program Files>\Intel\Intel(R) QuickAssist Technology
```

4.2 Cryptography (PKE) Test Application

A cryptography test application for PKE operations, cngtest, is included in this package. For more information on how to use the cngtest application, please refer to the Readme file included in the package. You can find the README file in the following folder upon completion of the installation:

```
<Program Files>\Intel\Intel(R) QuickAssist Technology
```

§