Intel® QuickAssist for Windows*

Release Notes

Package Version: QAT1.1.0-29

March 2019

Revision 002US

Document Number: 337758-002US

Contents

Figures

Tables

Revision History

Revision Number	Description	Revision Date
002	Intel QuickAssist Software release v1.1.0-29 • 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 v1.1.0-29. This document also describes extensions and deviations from the release functionality described in Table 2, *Intel® QuickAssist Technology Software for Linux* Software Programmer's Guide* for the various platforms that support Intel® QAT.

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)

1.2 Supported Operating Systems

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

- Windows* Server 2016

1.3 Features

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

Includes the following compression/decompression `QATZIP` APIs:

- `qzInit`
- `qzSetupSession`
- `qzCompress`
- `qzDecompress`
- `qzTeardownSession`
- `qzClose`
- `qzGetStatus`
- `qzSetDefaults`

- `qzGetDefaults`
- `qzMalloc`
- `qzFree`

This software package also provides the following cryptography services:

- 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 2.

- An Intel® QAT CNG provider that 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

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

1.4 Customer Support

Intel offers support for this software at the Application Program Interface (API) level, defined in Table 1 and Table 2 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.

1.5 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.

1.6 Reference Documents

Table 1 lists Intel® QuickAssist Technology generic documentation.

Table 2 lists Intel® QuickAssist Technology specific documentation.

Table 1. Intel® QuickAssist Technology Generic Documentation

Document	Document No./Location
Intel® QuickAssist Technology API Programmer's Guide	330684

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

Table 2. Intel® QuickAssist Technology Software Specific Documentation

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

1.7 Terminology

Table 3. Terminology

Term	Description
API	Application Program Interface
BOM	Bill of Materials
OS	Operating System
Intel® QAT	Intel® QuickAssist Technology
PKE	Public Key Encryption
HLK*	Windows* Hardware Lab Kit

§

2.0 Limitations and Known Issue

2.1 Limitations

This release does not support the following:

- Static Deflate Stateful compression/decompression
- Dynamic Deflate Stateful compression/decompression
- Symmetric (bulk) cryptography algorithms (AES)

2.2 Known Issues

Title	Cannot disable driver while parcomp (compression) is running
Reference #	QATE-36847
Description	When running parcomp stress tests, you cannot disable all 37c8 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 QAT Micro server 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 QAT devices only after the compression operations have completed.
Affected OS	Windows* Server 2016
Driver/Module	QAT 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 Since curve25519 is not supported by QAT, cryptography operations will fail when using cipher suites with ECDHE. However, the NistP256 and Nist384 curves are supported by 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: Launch the Group Policy Editor: *gpedit.msc* Open Computer Configuration -> Administrative Template -> Network -> SSL Configuration Settings Double-click ECC Curve Order (in the right pane) Click Enabled Edit the ECC Curve Order in the priority order described above. Click 'Apply' and exit the application
Affected OS	Windows* Server 2016
Driver/Module	QAT IA – Compression

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 C628 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 crash. 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

§

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
```

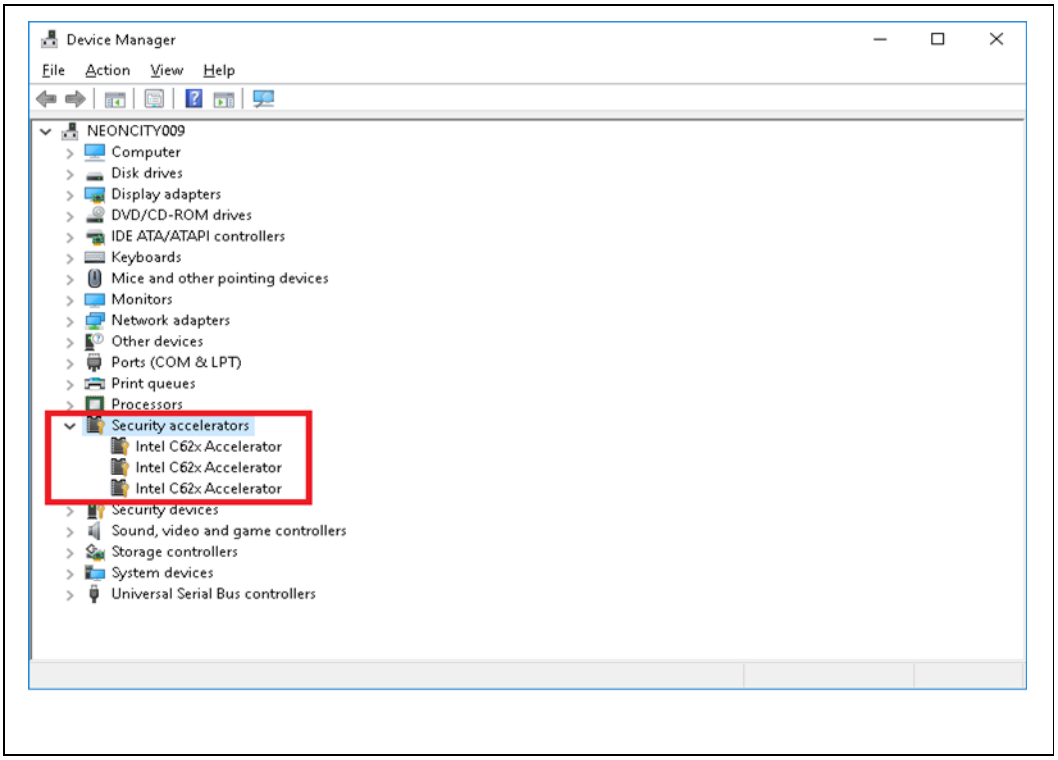
Upon completion of the installation, the README. The text file can also be found in the following folder:

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

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

Note: To make sure the software installation completed successfully and the Intel® QAT devices run as expected, Refer to Figure 1, Device Manager which lists three “Intel C62x Accelerator ”Intel® QAT devices under the “Security accelerators” folder Neoncity/security accelerators.

Figure 1. Device Manager



§

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, 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
```

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
```

§