



# **Windows Release Notes**

---

**Intel® QuickAssist Technology**

**Hardware Version 2.0**

***Production Release***

February 2023

# CONTENTS

<b>1</b>	<b>Release Description</b>	<b>3</b>
1.1	Supported Hardware Platforms	3
1.2	Supported Operating Systems	4
1.3	Package Version	4
1.4	What's New	5
1.5	Data Compression Services	5
1.6	Cryptography Services	6
1.7	List of Files in this Release	7
1.8	Reference Documents	7
1.9	Terminology	7
<b>2</b>	<b>Limitations, Known Issues and Resolved Issues</b>	<b>12</b>
2.1	Limitations	12
2.2	Known Issues	12
2.2.1	Cngtest does not validate fallback operations are working correctly	12
2.2.2	Parcomp unable to read > 1GB file for compression	13
2.2.3	Repeatedly referencing invalid memory in Guest may lead to instability	13
2.2.4	Not all devices recover from heartbeat failure in Linux VF SW fallback in 1vm64vf configuration	13
2.2.5	Linux VF remove/add stress fails in 1vm64vf configuration	14
2.2.6	QATzip Single Offload behaves inconsistently	14
2.2.7	Single offload compression with 512K request fails on silesia	14
2.2.8	CpmBCryptSample.sys may cause DRIVER_UNLOADED error	15
2.2.9	Changing Crypto ServicesNeeded requires cpmprov/cpmprovuser restart	15
2.2.10	Xeon® 4th-Generation in 4-Socket and above configurations, QAT devices may not load initially	15
2.2.11	Changing ServicesNeeded may cause Linux Guest kernel panic when using adf_ctl to change config	16
2.3	Resolved Issues	16
2.3.1	The isa-l.dll is not being installed for Windows Server Core editions	16
2.3.2	Cpmprov service is not running by default	16
2.3.3	Performing driver upgrade may sometimes see DRIVER_VERIFIER_DMA_VIOLATION	17
2.3.4	Changing ServicesNeeded to 'asym;sym' may cause KER- NEL_SECURITY_CHECK_FAILURE	17
2.3.5	PKE does not work when ServicesEnabled set to 'asym;sym' mode	17
2.3.6	AES-XTS does not work with 64-256 byte buffer sizes	17
2.3.7	Error in Cngtest doing AES-GCM stress	18
2.3.8	System instability when doing AES-CCM stress via Cngtest	18
2.3.9	DRIVER_VERIFIER_DMA_VIOLATION (e6) when running stressful AES-XTS/GCM via cngtest	18
2.3.10	Decompression error counters observed	18
2.3.11	QAT counters not loaded by default in WS2019 Guest	19

2.3.12	Cngtest displays -1 number of devices in Windows Guest . . . . .	19
2.3.13	Windows Guest AES-XTS may result in MEMORY_MANAGEMENT check . . . . .	19
2.3.14	Crypto example file Perf_User.bat has deprecated algorithms . . . . .	19
2.3.15	Cngtest Negative Ops output observed on certain params . . . . .	20
2.3.16	HyperVMode is possible with QatGen4m . . . . .	20
2.3.17	QatGen4m PKE performance under expectations . . . . .	20
<b>3</b>	<b>Software Installation</b>	<b>21</b>
<b>4</b>	<b>Test Applications</b>	<b>22</b>
4.1	Compression Test Application . . . . .	22
4.2	Cryptography (PKE) Test Application . . . . .	22

## Intel® QuickAssist for Windows\* Release Notes

### Package Version: W.2.0.4-0004

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.

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

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](https://www.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.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

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

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

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Copyright © 2022, Intel Corporation. All rights reserved.

Table 1:: Revision History

Document Number	Revision Number	Description	Revision Date
758459	005	Intel® QuickAssist Software release W.2.0.4-0004 <ul style="list-style-type: none"><li>• Updated Limitations Section</li><li>• Updated Known and Resolved Issues</li></ul>	February 2023
758459	004	Intel® QuickAssist Software release W.2.0.3-0004 <ul style="list-style-type: none"><li>• Added What's New</li><li>• Updated Data Compression services</li><li>• Updated Limitations Section</li><li>• Updated Known and Resolved Issues</li></ul>	January 2023
758459	003	Intel® QuickAssist Software release W.2.0.1-0016 Initial Production Release	November 2022
N/A	002	Production Candidate Release	September 2022
N/A	001	Initial EAR Release	July 2022

## RELEASE DESCRIPTION

This document contains information on the accompanying Intel® QuickAssist Technology (Intel® QAT) Windows\* Software Engineering Early Access Release W.2.0.4-0004. This document also describes extensions and deviations from the release functionality described in [Reference Documents](#), 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.

---

For more detailed technical information about the Windows\* QAT driver package, please see the “Intel® QuickAssist Technology Software for Windows\* - Technical Guide” in [Reference Documents](#).

---

**Note:** The “Intel® QuickAssist Technology Software for Windows\* - Technical Guide” is updated in the weeks following a public Windows\* QAT driver release.

---

### 1.1 Supported Hardware Platforms

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

- Intel® Xeon® 4th-Generation Scalable Processor with Intel® QAT Gen4 in 1-Socket and 2-Socket configurations.

---

**Note:** Intel® Xeon® 4th-Generation Scalable Processor with Intel® QAT Gen4 in configurations above 4-Socket are not validated.

---

- Intel® Xeon® 4th-Generation Scalable Processor with Intel® QAT Gen4m in 1-Socket and 2-Socket configurations.

---

**Note:** Intel® Xeon® 4th-Generation Scalable Processor with Intel® QAT Gen4m in configurations for 4-Socket and above are not validated.

---

## 1.2 Supported Operating Systems

Below are the currently validated Bare-Metal/Host Operating Systems supported for this release.

Table 1.1:: Validated Host Operating Systems

Host Operating System	Intel® 4xxx Accelerator	Intel® 401xx Accelerator
Windows* Server 2016	No	No
Windows* Server 2019	No	No
Windows* Server 2022	Yes	Yes

Below are the currently validated Guest Operating Systems supported with this release for SR-IOV using the Accelerator Virtual Function(s).

Table 1.2:: Validated Guest Operating Systems

Guest Operating System	Intel® 4xxx Accelerator	Intel® 401xx Accelerator
Windows* Server 2016	No	No
Windows* Server 2019	Full QAT HW/SW Support	Full QAT HW/SW Support
Windows* Server 2022	Full QAT HW/SW Support	Full QAT HW/SW Support
Windows* 10 Enterprise 21H2	SW ISA-L / MS SQL Restore only	SW ISA-L / MS SQL Restore only
Windows* 11 Enterprise 21H2	SW ISA-L / MS SQL Restore only	SW ISA-L / MS SQL Restore only
Ubuntu* 18.04 LTS, Kernel 4.15	Full QAT HW/SW Support	Full QAT HW/SW Support
Ubuntu* 20.04 LTS, Kernel 5.4	Full QAT HW/SW Support	Full QAT HW/SW Support

**Note:** The Linux VF driver was validated using Intel® QAT Linux driver package QAT20.L.1.0.2-00004.

**Note:** Windows 10 and Windows 11 Enterprise has only been validated for software ISA-L support specifically for Microsoft\* SQL software restore from QAT hardware or ISA-L software backup.

**Important:** Other Host/Guest Operating System combinations may work but has not been validated by Intel®.

## 1.3 Package Version

The following table shows the OS-specific package versions for each platform supported in this release.

Table 1.3:: Package Version

Chipset or SoC	Package Version	SHA256 Checksum
Top-Level Package	QAT.2.0. W.2.0.4-0004.zip	27B5103135117F02AEF0BEC1FAFC183E 828227798E9447A350E647031225AE9C

**Important:** Please verify the SHA256 checksum of the driver package to prevent use of repackaged Intel® drivers.

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

## 1.4 What's New

- Added support for Intel® Xeon® 4th-Generation Scalable Processor with Intel® QAT QatGen4m for Bare-Metal and virtualization using SR-IOV.
- Minor defect fixes.

Table 1.4:: Intel® Software Release Feature History

Release History	New Features
Release W.2.0.3-0004	<ul style="list-style-type: none"> <li>• Added support for Intel® Xeon® Scalable Processor with Intel® QAT QatGen4m for Bare-Metal</li> <li>• Added LZ4 metadata support via QATzip API with qzCompressWithMetadataExt</li> <li>• Installer security hardening</li> </ul>
Release W.2.0.1-0016	<ul style="list-style-type: none"> <li>• Initial production release that supports Intel® QAT Gen4</li> </ul>

## 1.5 Data Compression Services

This software package provides the following Data Compression services:

- Static and Dynamic Deflate Stateless compression/decompression
- Stateless LZ4 compression with separate metadata
- 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 6*, Intel® Intelligent Storage Application Library GitHub. However, Intel recommends only using the ISA-L DLL included in the Windows QAT driver package.

The QATzip file includes (and may not be limited to) the following compression and decompression functions. For more information, see the Windows\* QAT Technical Guide.

- qzAllocateMetadata
- qzClose
- qzCompress
- qzCompressCrc64
- qzCompressCrc64Ext
- qzCompressExt
- qzCompressWithMetadataExt



- qzDecompress
- qzDecompressCrc64
- qzDecompressCrc64Ext
- qzDecompressExt
- qzFree
- qzFreeMetadata
- qzGetDefaults
- qzGetSessionCrc64Config
- qzGetSoftwareComponentCount
- qzGetSoftwareComponentVersionList
- qzGetStatus
- qzInit
- qzMalloc
- qzMaxCompressedLength
- qzMetadataBlockRead
- qzMetadataBlockWrite
- qzSetDefault
- qzSetSessionCrc64Config
- qzSetupSession
- qzTeardownSession

## 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, in [Reference Documents](#).
- An Intel® QuickAssist CNG provider is registered to support the following PKE algorithms in user mode:
  - Rivest-Shamir-Adleman (RSA) with key lengths (2048, 3072, 4096, 8192 bit)
  - Elliptic Curve Digital Signature Algorithm (ECDSA) (nistP256/P384/P521)
  - Elliptic-curve Diffie-Hellman ECDH (nistP256/P384/P521 and Curve25519)
- An Intel® QuickAssist CNG provider is registered to support the following symmetric crypto algorithms in kernel mode:
  - AES (CBC, CCM, GCM, XTS with 256 bit key length)

## 1.7 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.

## 1.8 Reference Documents

[Async Mode for Nginx](#)

[GZIP File Format Specifications RFC1952](#)

[Intel® Intelligent Storage Acceleration Library](#)

[Intel® QuickAssist Technology API Programmer's Guide](#)

[Intel® QuickAssist Technology OpenSSL\\* Engine](#)

[Intel® QuickAssist Technology QATzip](#)

[Intel® QuickAssist Technology Software for Linux\\* Drivers \(Hardware Version 1.7\)](#)

[Intel® QuickAssist Technology Software for Linux\\* Getting Started Guide \(Hardware Version 1.7\)](#)

[Intel® QuickAssist Technology Software for Linux\\* Release Notes \(Hardware Version 1.7\)](#)

[Intel® QuickAssist Technology Software for Windows\\* - Technical Guide](#)

[Microsoft\\* Cryptography API Next Generation](#)

[Microsoft\\* DevCon GitHub](#)

[Microsoft\\* PowerShell GitHub](#)

[OpenSSL Cryptography and SSL/TLS Toolkit](#)

## 1.9 Terminology

### **ADF**

Acceleration Driver Framework.

### **AEAD**

Authenticated Encryption With Associated Data.

### **AES**

Advanced Encryption Standard.

### **API**

Application Programming Interface.

### **ASIC**

Application Specific Integrated Circuit.

### **BDF**

Bus Device Function.

### **BIOS**

Basic Input/Output System.

### **BOM**

Bill of Materials.

**BSD**

Berkeley Software Distribution.

**CBC**

Cipher Block Chaining mode.

**CCM**

Counter with CBC-MAC mode.

**CLI**

Command Line Interface.

**CnV**

Compress and Verify.

**CnVnR**

Compress and Verify and Recover.

**C-States**

C-States are advanced CPU current lowering technologies.

**CY**

Cryptography.

**DC**

Data Compression.

**DID**

Device ID.

**DMA**

Direct Memory Access.

**DRAM**

Dynamic Random Access Memory.

**DSA**

Digital Signature Algorithm.

**DTLS**

Datagram Transport Layer Security.

**ECC**

Elliptic Curve Cryptography.

**ECDH**

Elliptic Curve Diffie-Hellman.

**FLR**

Function Level Reset.

**FW**

Firmware.

**GCM**

Galois/Counter Mode.

**GPL**

General Public License.

**GUI**

Graphical User Interface.

**HMAC**

Hash-based Message Authentication Mode.

**IA**

Intel® Architecture.

**IEEE**

Institute of Electrical and Electronics Engineers.

**IKE**

Internet Key Exchange.

**Intel® ISA-L**

Intel® Intelligent Storage Acceleration Library. This includes an optimized library for fast software Deflate compression and decompression.

**Intel® QAT**

Intel® QuickAssist Technology.

**Intel® SpeedStep® Technology**

Advanced means of enabling very high performance while also meeting the power-conservation needs of mobile systems.

**Intel® VT**

Intel® Virtualization Technology.

**IOCTL**

Input Output Control function.

**IOMMU**

Input-Output Memory Management Unit.

**LAC**

LookAside Crypto.

**Latency**

The time between the submission of an operation via the QuickAssist API and the completion of that operation.

**MSI**

Message Signaled Interrupts.

**NUMA**

Non-uniform Memory Access.

**Offload Cost**

This refers to the cost, in CPU cycles, of driving the hardware accelerator. This cost includes the cost of submitting an operation via the Intel® QuickAssist API and the cost of processing responses from the hardware.

**OS**

Operating System.

**PCH**

Platform Controller Hub. In this manual, a Platform Controller Hub device includes standard interfaces and Intel® QAT Endpoint and I/O interfaces.

**PCI**

Peripheral Component Interconnect.

**PF**

Physical Function.

**PKE**

Public Key Encryption.

**PowerShell**

Cross-platform command-line shell and scripting language using the .NET Common Runtime.

**RAS**

Reliability, Availability, Serviceability.

**RSA**

Rivest-Shamir-Adleman.

**SAL**

Service Access Layer.

**SGL**

Scatter-Gather List.

**SHA**

Secure Hash Algorithm.

**sIOV**

Intel® Scalable I/O Virtualization

**SoC**

System-on-a-Chip.

**SR-IOV**

Single-Root Input/Output Virtualization.

**SSL**

Secure Sockets Layer.

**SYM**

Symmetric Crypto.

**TCG**

Trusted Computing Group.

**Throughput**

The accelerator throughput usually expressed in terms of either requests per second or bytes per second.

**TLS**

Transport Layer Security.

**TPM**

Trusted Platform Module.

**UDP**

User Datagram Protocol.

**USDM**

User Space DMA-able Memory.

**VF**

Virtual Function.

**VHD**

Virtual Hard Disk, VHD(x) is the successor file format.

**VM**

Virtual Machine.

**WDK**

Windows\* Driver Kit

## **WPP**

Windows\* Software Trace Pre-processor

## **LIMITATIONS, KNOWN ISSUES AND RESOLVED ISSUES**

This section provides the all known limitations and known issues for this Windows\* software release. For detailed information on features/limitations, please refer to the README.txt file inside the software package (./QuickAssist/README.txt).

### **2.1 Limitations**

This release does not support the following:

- Public Key Encryption in kernel mode; symmetric cryptography in user mode.
- CRC64 support in hardware or with user selected polynomials.
- LZ4 compression support is restricted to qzCompressWithMetadataExt in QATzip API.
- LZ4 decompression with metadata.
- LZ4 software fallback and failover.
- Compression and hash/cryptography chaining functionality.
- Software Fallback for PKE in SR-IOV mode.
- Dynamic and static Deflate Stateful compression/decompression

### **2.2 Known Issues**

The known issues and resolved issues with this software release are listed below:

#### **2.2.1 Cngtest does not validate fallback operations are working correctly**

Title	Cngtest does not validate fallback operations are working correctly
Reference	QATE-38968
Description	Currently, Cngtest does not include tests to validate the fallback to the Microsoft* provider works for unsupported algorithms and curves. 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 2022
Driver/Module	QAT IA - Crypto

### 2.2.2 Parcomp unable to read > 1GB file for compression

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 2022
Driver/Module	QAT IA - Compression

### 2.2.3 Repeatedly referencing invalid memory in Guest may lead to instability

Title	Repeatedly referencing invalid memory in SR-IOV enabled Guest may lead to Guest instability.
Reference	QATE-81175
Description	When repeatedly referencing invalid memory in a stressful manner for hours in a guest with Intel® QAT VF's, it may lead to system instability and a guest OS crash.
Resolution	Updating the Hyper-V host and Windows* guest to the latest cumulative updates greatly reduces the risk of this happening to negligible levels.
Affected OS	Windows* Server 2022 with Hyper-V using Windows* Guests
Driver/Module	QAT IA - Compression

### 2.2.4 Not all devices recover from heartbeat failure in Linux VF SW fallback in 1vm64vf configuration

Title	Not all devices recover from heartbeat failure in Linux VF SW fallback heartbeat test in 1vm64vf configuration.
Reference	QAT20-20783
Description	<p>After running Linux VF software fallback heartbeat test in 1vm 64vm configuration, observed least one device not resetting.</p> <p>In the Nginx logs in /opt, the RESTARTING/RESTARTED messages are mismatched, where there are always 128 RESTARTING messages but less than 128 RESTARTED messages.</p> <p>In Dmesg, among the “Function level reset, resetting device” messages after a heartbeat failure, at least one “Device is still in use, can’t be stopped” message is seen.</p>
Resolution	Reboot the Guest.
Affected OS	Windows* Server 2022 with Hyper-V using Ubuntu Guests
Driver/Module	QAT IA - Base Driver



### 2.2.5 Linux VF remove/add stress fails in 1vm64vf configuration

Title	Linux VF remove/add stress fails in 1vm64vf configuration, some VFs left in bad state
Reference	QAT20-21454
Description	When repeatedly executing remove/add on Linux VM with 64 VFs assigned will sometimes fail with some VFs in a bad state. These VFs do not appear in lspci in the VM but they ARE listed as an assigned device from the Windows host perspective.
Resolution	Reboot the Guest
Affected OS	Windows* Server 2022 with Hyper-V using Ubuntu Guests
Driver/Module	QAT IA - Base Driver

### 2.2.6 QATzip Single Offload behaves inconsistently

Title	QATzip Single Offload behaves inconsistently
Reference	QAT20-22944
Description	When attempting to use single offload compression with Windows QATzip (e.g., using a request and chunk size greater than 1016KB), the operation may fail. This is a current QAT limitation using default page sizes that limits the contiguous memory allocation for a single request. In Windows* Server 2022, it is approximately 8MB; on older Windows* Server, it is limited to approximately 1016KB.
Resolution	Limit the request size when doing single offload.
Affected OS	Windows* Server 2022 and Windows* Server 2022 with Hyper-V using Windows* Guests
Driver/Module	QAT IA - Compression

### 2.2.7 Single offload compression with 512K request fails on silesia

Title	Single offload compression with 512K request fails on silesia
Reference	QAT20-24514
Description	When using attempting single offload compression on silesia corpus file with 512K request, user may observe a return code of QZ_FAIL. This happens only with QZ_STATIC_HDR (static) mode.
Resolution	<ol style="list-style-type: none"><li>1. Use QZ_DYNAMIC_HDR (dynamic) mode.</li><li>2. Use chunking or increase the request size.</li></ol>
Affected OS	Windows* Server 2022 and Windows* Hyper-V 2022 using Windows* Guests
Driver/Module	QAT IA - Crypto

### 2.2.8 CpmBCryptSample.sys may cause DRIVER\_UNLOADED error

Title	CpmBCryptSample.sys may cause DRIVER_UNLOADED error
Reference	QAT20-25736
Description	When using multiple stressful AES-XTS sessions with cngtest sample application, we may observe a DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS on very rare occasions.
Resolution	Reduce application thread count.
Affected OS	Windows* Server 2022 and Windows* Hyper-V 2022 using Windows* Guests
Driver/Module	QAT IA - Crypto

### 2.2.9 Changing Crypto ServicesNeeded requires cpmprov/cpmprovuser restart

Title	Changing Crypto ServicesNeeded requires cpmprov and/or cpmprovuser restart.
Reference	QAT20-25739
Description	When changing the ServicesNeeded registry key, the new ServicesNeeded value may not be fully set until the cpmprov and/or cpmprovuser services have been restarted. This may cause system instability, especially in PnP scenarios. This does not apply to the QAT VF device, as the ServicesNeeded is only affected at the QAT PF level.
Resolution	After changing ServicesNeeded, restart the affected QAT devices, and then restart the cpmprov and/or cpmprovuser services.
Affected OS	Windows* Server 2022 and Windows* Hyper-V 2022 using Windows* Guests
Driver/Module	QAT IA - Crypto

### 2.2.10 Xeon® 4th-Generation in 4-Socket and above configurations, QAT devices may not load initially

Title	Xeon® 4th-Generation in 4-Socket and above configurations, QAT devices may not load initially
Reference	QAT20-26576
Description	When installing QAT driver package on Xeon® 4th- Generation in 4-socket and above configurations, there may be a chance that some QAT devices may not initially load correctly. This may be accompanied by a system reboot required message from device manager.
Resolution	Restart the system and QAT devices will load correctly.
Affected OS	Windows* Server 2022 and Windows* Hyper-V 2022 using Windows* Guests
Driver/Module	QAT IA - Base Driver

### 2.2.11 Changing ServicesNeeded may cause Linux Guest kernel panic when using adf\_ctl to change config

Title	Changing ServicesNeeded may cause Linux Guest kernel panic when using adf_ctl to change config
Reference	QAT20-26664
Description	Linux guest kernel panic may be seen after changing the Windows host PF ServicesNeeded and then changing Linux Guest VF config file with adf_ctl in short succession.
Resolution	After changing the ServicesNeeded registry key, restart the system if the intended use case is to use QAT VF's in SR-IOV mode.
Affected OS	Windows* Server 2022 with Hyper-V using Ubuntu Guests
Driver/Module	QAT IA - Base Driver

## 2.3 Resolved Issues

### 2.3.1 The isa-l.dll is not being installed for Windows Server Core editions

Title	The isa-l.dll is not being installed for Windows Server Core editions.
Reference	QATE-84471
Description	When installing the Windows QAT driver package on Windows Server Core editions, the isa-l.dll is not installed. The QAT installation summary erroneously attributes this to the lack of the NuGet binary.
Resolution	User can manually unpack and copy the isa-l.dll into the Windows system32 directory.Reboot the Guest.
Affected OS	Windows* Server 2016/2019/2022 Core Edition
Driver/Module	QAT IA - Installer

### 2.3.2 Cpmprov service is not running by default

Title	Cpmprov service is not running by default
Reference	QAT20-21152
Description	After installing the QAT20 driver package, the cpmprov service is configured or running by default.
Resolution	Use sc.exe to create and start the cpmprov service.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Installer

### 2.3.3 Performing driver upgrade may sometimes see DRIVER\_VERIFIER\_DMA\_VIOLATION

Title	Performing driver upgrade may sometimes see DRIVER_VERIFIER_DMA_VIOLATION
Reference	QAT20-21314
Description	When doing a PF driver upgrade with stressful multi-threaded compression in the Windows Guest, we sometimes see a DRIVER_VERIFIER_DMA_VIOLATION.
Resolution	Restart the system.
Affected OS	Windows* Server 2022 with Hyper-V with Windows Guest
Driver/Module	QAT IA - Base Driver

### 2.3.4 Changing ServicesNeeded to 'asym;sym' may cause KERNEL\_SECURITY\_CHECK\_FAILURE

Title	Changing ServicesNeeded to 'asym;sym' may cause KERNEL_SECURITY_CHECK_FAILURE
Reference	QAT20-21396
Description	When repeatedly setting ServicesNeeded to asym;sym and start/stopping cpmprov service (or some combination thereof), we observe KERNEL_SECURITY_CHECK_FAILURE.
Resolution	Do not set 'Asym;sym' mode.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Base Driver

### 2.3.5 PKE does not work when ServicesEnabled set to 'asym;sym' mode

Title	PKE does not work when ServicesEnabled set to 'asym;sym' mode
Reference	QAT20-21416
Description	When setting ServicesNeeded on all qat20dev to asym;sym, PKE operations no longer work in HW.
Resolution	Do not set 'Asym;sym' mode.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Base Driver

### 2.3.6 AES-XTS does not work with 64-256 byte buffer sizes

Title	AES-XTS does not work with 64-256 byte buffer sizes
Reference	QAT20-21417
Description	Cngtest AES-XTS does not work with 64Byte - 256Byte buffer sizes. Expected to work; AES-GCM and CCM works.
Resolution	Use software for small payload AES-XTS.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Crypto

### 2.3.7 Error in Cngtest doing AES-GCM stress

Title	Error in Cngtest doing AES-GCM stress
Reference	QAT20-21452
Description	When doing AES-GCM stress via Cngtest, we sometimes see error message “Error in CNG multi-thread sample : 31”
Resolution	None.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Crypto

### 2.3.8 System instability when doing AES-CCM stress via Cngtest

Title	System instability when doing AES-CCM stress via Cngtest
Reference	QAT20-21453
Description	When doing AES-CCM stress via Cngtest, we usually see system instability after <10 minutes. System is slower and slower and then no response.
Resolution	None.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Crypto

### 2.3.9 DRIVER\_VERIFIER\_DMA\_VIOLATION (e6) when running stressful AES-XTS/GCM via cngtest

Title	DRIVER_VERIFIER_DMA_VIOLATION (e6) when running stressful AES-XTS/GCM via cngtest
Reference	QAT20-21563
Description	Observed that sometimes there is a DRIVER_VERIFIER_DMA_VIOLATION e6 when running multiple multi-threaded AES tests back to back via Cngtest using the AES-GCM or AES-XTS algorithms.
Resolution	None.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Crypto

### 2.3.10 Decompression error counters observed

Title	Decompression error counters observed
Reference	QAT20-21564
Description	Observing decompression error counters increment when doing decompression. Note decompress completes successfully and the checksum matches against the original file.
Resolution	None.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Compression

### 2.3.11 QAT counters not loaded by default in WS2019 Guest

Title	QAT counters not loaded by default in WS2019 Guest
Reference	QAT20-22862
Description	When using command line or GUI for the target platform's first QAT driver install, the QAT counters are not loaded by default.
Resolution	Manually add the counters
Affected OS	Windows* Server 2022 with Hyper-V using Windows* Server 2019 Guests
Driver/Module	QAT IA - Base Driver

### 2.3.12 Cngtest displays -1 number of devices in Windows Guest

Title	Cngtest displays -1 number of devices in Windows Guest
Reference	QAT20-22976
Description	When attempting to use cngtest, the output for the number of [QAT] Devices is -1, which is inaccurate
Resolution	Do not use the Device count number in this situation.
Affected OS	Windows* Server 2022 with Hyper-V using Windows* Guests
Driver/Module	QAT IA - Crypto

### 2.3.13 Windows Guest AES-XTS may result in MEMORY\_MANAGEMENT check

Title	Windows Guest AES-XTS may result in MEMORY_MANAGEMENT check
Reference	QAT20-24560
Description	When running AES-XTS workload on Windows Guest, we may occasionally see a MEMORY_MANAGEMENT (1a) check. Note that there are no QAT components on stack trace.
Resolution	Avoid highly threaded AES-XTS workloads.
Affected OS	Windows* Hyper-V 2022 using Windows* Guests
Driver/Module	QAT IA - Crypto

### 2.3.14 Crypto example file Perf\_User.bat has deprecated algorithms

Title	Crypto example file Perf_User.bat has deprecated algorithms
Reference	QAT20-24572
Description	The Perf_User.bat located in ..\Crypto\Samples\bin has deprecated algos as part of the examples.
Resolution	Remove the DH and DSA entries.
Affected OS Title	Windows* Server 2022 and Windows* Hyper-V 2022 using Windows Guest
Driver/Module	QAT IA - Crypto

### 2.3.15 Cngtest Negative Ops output observed on certain params

Title	Cngtest Negative Ops output observed on certain params
Reference	QAT20-24585
Description	When using certain crypto algorithms in cngtest (e.g., RSA 8192 key length decrypt), sometimes negative Operations/sec (Ops) may be observed. This occurs with high iteration (numIter) counts.
Resolution	Use shorter iteration count.
Affected OS	Windows* Server 2022 and Windows* Hyper-V 2022 using Windows* Guests
Driver/Module	QAT IA - Crypto

### 2.3.16 HyperVMode is possible with QatGen4m

Title	HyperVMode is possible with QatGen4m
Reference	QAT20-25912
Description	For the QAT Windows installer, QatSetup.exe, the QatGen4m has the ability to install with HyperVMode. However, QatGen4m does not support virtualization.
Resolution	Reinstall the driver in Standalone mode as QatGen4m has no functionality in HyperVMode.
Affected OS	Windows* Server 2022 and Windows* Hyper-V 2022
Driver/Module	QAT IA - Installer

### 2.3.17 QatGen4m PKE performance under expectations

Title	QatGen4m PKE performance under expectations
Reference	QAT20-25914
Description	The QatGen4m PKE performance e.g., RSA with key size of 2048 bits, may be lower than the equivalent when compared to the Linux* QAT driver.
Resolution	No mitigation until next release.
Affected OS	Windows* Server 2022
Driver/Module	QAT IA - Crypto

## 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 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 four “Intel® 4xxx Accelerator” devices under the “Security accelerators” PNP Classification.

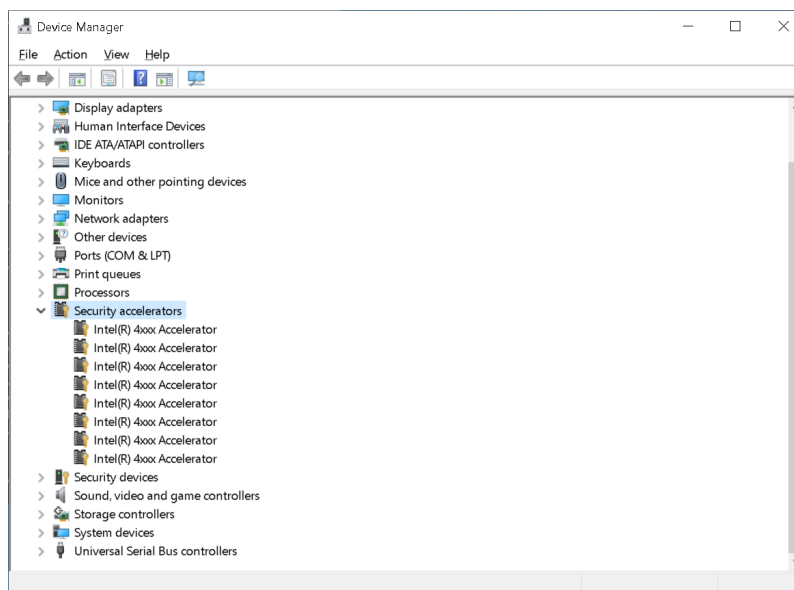


Figure 3.1:: Device Manager with Intel® QuickAssist Driver Installed in Microsoft® Windows\*



## 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
```