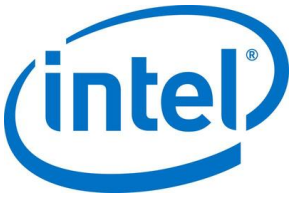

Intel® QuickAssist Technology (Intel® QAT) Software for Linux*

Release Notes

Package Version: QAT1.7.L.4.9.0-00008

March 2020

Document Number: 336211-014

Contents

Tables

Revision History

Date	Revision	Description
March 2020	014	Intel® QuickAssist Technology Software Release v4.9 changes: • Revised Table 1, package version number • Revised Table 3, package and checksum numbers • Added Table 6, Terminology Added and Revised Known Issues: QATE-50650 Resolved Issues: QATE-51676, QATE-42157, QATE-45527
February 2020	013	For software release QAT1.7.L. 4.8.0-00005 Updated package number and checksum New Open Issues: QATE-41707, QATE-42173, QATE-43713 Newly Resolved Issues: QATE-29663, QATE-38075, QATE-39220, QATE-40952, QATE-50854, QATE-51157, QATE-52111, QATE-58487
October 2019	012	For software release QAT1.7.L.4.7.0-00006 Updated package number and checksum New Open Issues: QATE-40952, QATE-41707, QATE-40173, QATE-43713 Newly Resolved Issues: QATE- 3350, QATE-38078, QATE-39129, QATE-41556
June 2019	011	For software release QAT1.7.L.4.6.0-00025 Updated package number and checksum Updated Section 1.1 Updated Table 1 Updated Section 1.2.5 Added Section 1.4, Environmental Assumptions Updated Section 4.5 Updated Chapter 4. Added FAQ 4.9 New Open Issues: QATE-29663, QATE-32074, QATE-38075, QATE-38078, QATE-38236, QATE-39129, QATE-39220 Newly Resolved Issues: QATE- 9383, QATE- 15136, QATE- 30882, QATE- 32373, QATE- 32621, QATE- 33137, QATE- 33450, QATE- 37406, QATE- 37470, QATE-38014, QATE-38119, QATE-, QATE-39082

Date	Revision	Description
March 2019	010	For software release QAT1.7.L.4.5.0-00034 Updated package number and checksum Updated Section 1.1 Updated Table 1 Updated Section 1.2.5 Updated Section 4.5 New Open Issues: QATE-32621, QATE-33137, QATE-37406 Newly Resolved Issues: QATE-7919, QATE-12516, QATE-21561, QATE-29974, QATE-31792 QATE-32022, QATE-32044, QATE-32322, QATE-37450
December 2018	009	For software release QAT1.7.L.4.4.0-00023 Updated package number and checksum Updated Section 1.1 Updated Table 1 Updated Section 1.2.5 New Open Issues: QATE-31270, QATE-31792, QATE-32022, QATE-32044, QATE-32322 Newly Resolved Issues: QATE-4051, QATE-9545, QATE-29972, QATE-30720, QATE-31201, QATE-31295, QATE-31714, QATE-31800, QATE-32336
September 2018	008	For software release QAT1.7.L.4.3.0-00033 Updated package number and checksum Updated New Features sub-section in Section 1.1 Updated Table 2 New Open Issues: QATE-29972, QATE-29974, QATE-30334, QATE-30497, QATE-30865, QATE-30880, QATE-30882, QATE-31295 Newly Resolved Issues: QATE-3982, QATE-14458, QATE-18691, QATE-20186, QATE-30340, QATE-30758, QATE-30785

Date	Revision	Description
June 2018	007	For software release QAT1.7.L.4.2.0-00012 Minor updates throughout for clarity Updated package number and checksum Updated Chapter 4. Added FAQ. New Open Issues: QATE-15136, QATE-17367, QATE-18691, QATE-20186, QATE-21561 Newly Resolved Issues: QATE-3039, QATE-3635, QATE-4051, QATE-11828, QATE-12793, QATE-14779, QATE-14870, QATE-14920, QATE-14953
April 2018	006	For software release 4.1.0-00022 Minor updates throughout for clarity Updated package number and checksum Updated Section 1.1 Updated Section 2.1 Updated Chapter 4. Added FAQ 7 New Open Issues: QATE-3350, QATE-7495, QATE-7919, QATE-12516, QATE-12793, QATE-14458, QATE-14706, QATE-14779, QATE-14870, QATE-14953, QATE-14920 Newly Resolved Issues: QATE-4111, QATE-5433, QATE-5520, QATE-5989, QATE-7393, QATE-7563, QATE-8109, QATE-8233, QATE-9234, QATE-9326, QATE-9483, QATE-10180, QATE-10780, QATE-11629, QATE-11790, QATE-12256, QATE-14171
January 2018	005	For software release 1.0.5-25
December 2017	004	For software release 1.0.5-14
August 2017	003	For software release 1.0.4-2
July 2017	002	Newly Resolved Issues: QATE-3955
July 2017	001	Initial product release

Pre-release Revision History

Date	Revision	Description
July 2017	0.97	For software release 1.0.3-42 Updated package number and checksum. New Open Issues: QATE-9953
May 2017	0.96	For software release 1.0.3 Updated package number and checksum. New Open Issues: QATE-9241, QATE-9234, QATE-9326, and QATE-8233 Newly Resolved Issues: QATE-3650, QATE-3259, and QATE-8189
May 2017	0.95	For software release 1.0.2 Updated package number and checksum. Updated generic collateral website link. New Open Issues: QATE-8361, QATE-8189, and QATE-8109 Newly Resolved Issues: QATE-7909
April 2017	0.94	For software release 1.0.1 Updated package number, checksum, and instructions for obtaining SoC BIOS
March 2017	0.93	Updated instructions for obtaining SoC BIOS
March 2017	0.92	For software release 1.0 Updated software license locations in Table 4. New Open Issues: QATE-5989 and QATE-7393 Newly Resolved Issues: QATE-3017
February 2017	0.91	Updated BIOS information for SoC Updated list of unsupported features All open and resolved issues have new reference numbers New Open Issues: QATE-4051, QATE-5433, and QATE-3017 Newly Resolved Issues: QATE-3220, QATE-3072, QATE-2985, QATE-4015 and QATE-6463

1.0 Description of Release

This document describes extensions and deviations from the release functionality described in the software Programmer's Guides for the various platforms that support Intel® QuickAssist Technology (Intel® QAT).

Changes in this software release include:

Standard Linux* installation support added

For instructions on loading and running the release software, see the *Getting Started Guide* for your platform (see Section 2.3, Related Documentation).

This software release is intended for platforms that contain:

- Intel®C62x Chipset
- Intel Atom®C3000 processor product family
- Intel Xeon® processor D family
- Intel® QuickAssist Adapter 8960/Intel® QuickAssist Adapter 8970 (formerly known as "Lewis Hill")
- Intel® Communications Chipset 8925 to 8955 Series

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

1.1 Features/Limitations

The main features available on platforms using Intel® QAT are:

- Cryptographic Services
- Data Compression Services
- Cryptographic Sample Applications
- Data Compression Sample Applications
- Intel® QAT Data Plane Cryptographic API (`cpa_cy_sym_dp.h`)
- Intel® QAT Technology Data Plane Data Compression API (`cpa_dc_dp.h`)

The following features are not currently supported:

- Dynamic instances
- Intel®Key Protection Technology (KPT)
- Batch and Pack in Compression Service
- Stateful Compression is deprecated

New Features:

- Elliptic curves related to Transport Layer Security (TLS) v1.3

Note: The software in this release has been validated with Community Enterprise Operating System* (CentOS*) (64-bit) for the following products:

- Intel® C62x Chipset
- Intel Atom® Processor C3000 Product Family
- Intel® Xeon® D Processor Family
- Intel® Communications Chipset 8925 to 8955 Series

Validated against Yocto* for this product:

Intel Atom® C3000 processor product family

Note: While the Intel® QAT Accelerator software is validated on CentOS v7.x, it is expected that the current release will work without change on other Linux distributions and Kernels.

1.1.1 Version Numbering Scheme

The version numbering scheme is:

```
name.os.major.minor.maintenance-build
```

Where:

- name is “QAT1.7”
- os is the operating system: “L” for Linux
- major is the major version of the software
- minor is the minor version of the software
- maintenance-build is the maintenance release and build number

1.1.2 Package Versions

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

Table 1. Package Versions

Chipset or SoC	Package Version
Top-Level Package	QAT1.7.L.4.9.0-00008.tar.gz

1.1.3 Licensing for Linux* Acceleration Software

The acceleration software is provided under the licenses listed in Table 5. Intel® QAT Software Specific Documentation. When using or redistributing dual-licensed components, you may do so under either license.

Table 2. Linux* Acceleration Software Licensing Files

Component	License	Directories
User Space only components	Berkeley Standard Distribution (BSD)	./quickassist/lookaside/access_layer/src/qat_direct ./quickassist/lookaside/access_layer/src/common/crypto/kpt ./quickassist/lookaside/access_layer/src/common/crypto/asym ./quickassist/utilities/osal/src/linux/user_space
Common User Space and Kernel Space Library	Dual BSD/ General Public License (GPL) v2	./quickassist/build_system ./quickassist/include ./quickassist/lookaside/ (except items in User Space only) ./quickassist/utilities/osal (except items in User Space only) ./quickassist/utilities/adf_ctl
Kernel space driver	GPL v2	./quickassist/qat/drivers
Compatibility layer for older kernel versions	GPL	./quickassist/qat/compat
User Space Direct Memory Access (DMA)-able Memory Driver	Dual BSD/ GPL v2	./quickassist/utilities/libusdm
libcrypto	OpenSSL	./quickassist/utilities/osal/src/linux/user_space/openssl
CPM Firmware	Redistribution	./quickassist/qat/fw
Calgary corpus and Canterbury corpus test files	Public domain	./quickassist/lookaside/access_layer/src/sample_code/performance/compression

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

1.1.4 Basic Input/Output System (BIOS)/Firmware Version

The term Basic Input/Output System (BIOS) refers to the pre-boot firmware that could include legacy BIOS or Extensible Firmware Interface (EFI) compliant firmware.

Note: Update your platform, so it uses the latest available version of the BIOS/firmware available for that platform.

For the Intel®C62x Chipset, update your Purley platform to use the BIOS/firmware version available in the Purley Best Known Configuration (BKC) for that platform.

1.1.5 MD5 Checksum Information

The following table gives MD5 checksum information.

Table 3. Checksum Package

	Package	Checksum
Main Package	QAT1.7.L.4.9.0-00008.tar.gz	77e123faa832bceb4b328e343e5e5534

1.2 Intel® QuickAssist Technology API Updates

The Intel® QAT API version number is different from the software package version number.

For details on any changes to the Intel® QAT APIs, refer to the Revision History pages in the following API reference manuals (refer to Table 4):

- Intel® QuickAssist Technology Cryptographic API Reference Manual
- *Intel® QuickAssist Technology Data Compression API Reference Manual*

1.3 Technical Support

Intel offers support for this software at the API level only, defined in the programmer's guides and API reference manuals listed in Table 4. If your field representative has created an account for you, submit support requests via https://premier.intel.com.

1.4 Environmental Assumptions

The following assumptions are made concerning the deployment environment:

- The driver object/executable file on the disk should be protected using the normal file protection mechanisms so that it is writable only by trusted users, for example, a privileged user or an administrator.
- The public key firmware image on the disk should be protected using normal file protection mechanisms so that it is writable only by trusted users, for example, a privileged user or an administrator.
- The Intel® QAT device should not be exposed (via Single-root Input/Output Virtualization (SR-IOV)) to untrusted guests.
- The Intel® QAT device should not be exposed (via the "user space direct" deployment model) to untrusted users.
- DRAM is considered to be inside the trust boundary. The typical memory-protection schemes provided by the Intel architecture processor and memory controller, and by the operating system, prevent unauthorized access to these memory regions.
- Persistent keys were not considered, but the storage media are considered inside the cryptographic boundary.
- The driver exposed device file should be protected using the normal file protection mechanisms so that it could be opened and read/written only by trusted users.
- If any algorithms are registered with the Linux Crypto API, all users should be trusted.

§

2.0 Where to Find Current Software

Collateral can be found on https://01.org/intel-quickassist-technology

2.1 Accessing Additional Content from My Intel

1. In a web browser, go to http://intel.com/myintel.

   Enter your login ID in the Login ID box. Check **Remember my login ID** only if you are not using a shared computer. Click **Submit**.

Note: To acquire a new My Intel Business Applications & Tools, contact your Intel Field Sales Representative.

2. Enter your password in the Password box. Click **Submit**.
3. Under the My Applications heading, click on **Design Kits**.
   a. Under the Processors, Boards, and Systems heading, click on **Processors and chipsets**.
   b. Search for the Code Name of the appropriate device:
      - For the Intel®C62x Chipset PCH, enter the text **Purley** in the text box next to the Magnifying Glass.
      - For the Intel®Atom®C3000 Processor Product Family SoC, enter the text **Denverton NS**.
   c. Click on the **View** button under the Action tab in the search results.
   d. Click on the **Technical Library** tab.

2.2 List of Files in Release

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

2.3 Related Documentation

The following table lists Intel® QAT generic documentation.

Table 4. Intel® QAT Generic Documentation

Document Name	Reference Number
Intel® QuickAssist Technology API Programmer's Guide	330684
Intel® QuickAssist Technology Cryptographic API Reference Manual	330685
Intel® QuickAssist Technology Data Compression API Reference Manual	330686

Document Name	Reference Number
Intel® QuickAssist Technology Performance Optimization Guide	330687
Using Intel® Virtualization Technology (Intel® VT) with Intel® QuickAssist Technology Application Note	330689

The following table lists Intel® QAT specific documentation.

Table 5. Intel® QAT Software Specific Documentation

Document Name	Reference Number
Intel® QuickAssist Technology Software for Linux Getting Started Guide - Hardware Version 1.7*	336212
Intel® QuickAssist Technology Software for Linux Software Programmer's Guide - Hardware Version 1.7*	336210

2.4 Terminology

Table 6. Terminology

Term	Description
API	Application Programming Interface
BIOS	Basic Input/Output System
BKC	Best Known Configuration
BSD	Berkeley Standard Distribution
CentOS*	Community Enterprise Operating System*
CY	Cryptographic
DC	Compression
DMA	Direct Memory Access
EFI	Extensible Firmware Interface
EP	Endpoint
FW	Firmware
GEN	General
GPL	General Public License
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
Intel® QAT	Intel® QuickAssist Technology

Term	Description
OS	Operating System
PERF	Performance
SR-IOV	Single-root Input/Output Virtualization
TLS	Transport Layer Security
VFs	Virtual Functions

§

3.0 Intel® QuickAssist Technology (Intel® QAT) Software - Issues

Known and resolved issues relating to the Intel® QuickAssist Technology (Intel® QAT) software are described in this section.

Note: Issue titles follow the pattern Identifier - `<Component> [Stepping]`: Description of issue where:

`<Component>` is one of the following:

- CY - Cryptographic
- DC - Compression
- EP - Endpoint
- GEN - General
- SYM DP - Symmetric Cryptography on Data Plane
- SR-IOV - Single Root I/O Virtualization
- FW - Firmware
- PERF - Performance

`[Stepping]` is an optional qualifier that identifies if the errata applies to a specific device stepping.

3.1 Known Issues

This section contains known issues related to the software for Intel® QAT Hardware Version 1.7.

3.1.1 QATE-3241 - CY - cpaCySymPerformOp, when used with parameter checking, may reveal the amount of padding

Title	CY - cpaCySymPerformOp when used with parameter checking, may reveal the amount of padding.
Reference #	QATE-3241
Description	When Performing a CBC Decryption as a chained request using `cpaCySymPerformOp` it is necessary to pass a length of the data to MAC (`messageLenToHashInBytes`). With `ICP_PARAM_CHECK` enabled, this checks the length of data to MAC is valid and, if not, it aborts the whole operation and outputs an error on `stderr`.
Implication	The length of the data to MAC is based on the amount of padding. This should remain private and not be revealed. The issue is not observed when the length is checked in constant time before passing the value to the API. This is done by OpenSSL.
Resolution	1. Build without `ICP_PARAM_CHECK`, but this opens the risk of buffer overrun. 2. Validate the length before using the API.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.2 QATE-7495 - GEN - An incorrectly formatted request to Intel® QAT can hang the entire Intel® QAT Endpoint

Title	GEN - An incorrectly formatted request to Intel® QAT can hang the entire Intel® QAT Endpoint
Reference #	QATE-7495
Description	This version of the Intel® QAT hardware does not perform request checking. It follows that a malicious application can submit requests that can bring down an entire Intel® QAT Endpoint, which can impact other Intel® QAT jobs associated with the hardware. This presents a risk to be managed by the host and guest operating systems and other system policies. The exposure can extend to other guest operating systems or applications outside of the typical access boundary of the malicious guest or application.
Implication	All guest operating systems or other applications using Intel® QAT must be trusted, and/or other steps must be taken to ensure that an untrusted application or guest cannot submit incorrectly formatted requests.
Resolution	There is no workaround available. However, system policies (including limiting certain operating system permissions) can help to mitigate this issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.3 QATE-17367 - SRIOV - PF driver might report errors if the device is reset

Title	SRIOV - PF driver might report errors if the device is reset.
Reference #	QATE-17367
Description	If a manual or automatic device reset (FLR or SBR) is triggered as a result of an error (e.g. heartbeat failure, end fatal errors, etc.) on a system with Intel® QAT VFs enabled, the PF driver might report run time errors and might not recover.
Implication	Reset of the PF driver is not supported when VFs are enabled.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.4 QATE-30334 - SRIOV – Intel® QAT API in kernel space is not supported on the host through virtual functions (VFs)

Title	SRIOV - QAT API in kernel space is not supported on the host through virtual functions (VFs).
Reference #	QATE-30334
Description	When a kernel application tries to use the Intel® QAT API through an instance associated with a VF, DMAR protection errors are reported in the system logs.
Implication	It is not possible to access the Intel® QAT API in the kernel space using VFs in the host.
Resolution	Do not use the Intel® QAT kernel API with VFs on the host. VFs on the guest is supported.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.5 QATE-30497 - GEN - Huge pages are not supported on the host when the iommu is on

Title	GEN - Huge pages are not supported on the host when the iommu is on.
Reference #	QATE-30497
Description	When an application tries to use VFs on the host with `intel_iommu`=on and huge pages enabled in USDM, DMAR protection errors are reported in the system log.
Implication	It is not possible to use huge pages with VFs on the host.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.6 QATE-30865 - DC - Decompression hardware accelerator requires a minimal destination buffer size

Title	DC - Decompression hardware accelerator requires a minimal destination buffer size.
Reference #	QATE-30865
Description	If the destination buffer size is less than 258 bytes for a decompression operation, the hardware may return overflow without processing any data. This may occur if previous decompression operations indicate the next decompression operation will produce a 258-byte match, which corresponds to the largest possible representation of the lengths symbols in the deflate standard.
Implication	No uncompressed data is produced until enough output buffer is supplied.
Resolution	For decompression operations, the minimal destination buffer size should be 258 bytes.
Affected OS	Linux
Driver/Module	CPM HW - Data Decompression

3.1.7 QATE-30880 - GEN - Partial recovery when kernel space instances are in use

Title	GEN - Partial recovery when kernel space instances are in use.
Reference #	QATE-30880
Description	If a device error (uncorrectable error or heartbeat failure) occurs while an application in kernel space is using the Intel® QAT API and if `AutoResetOnError` is set to 1 in the configuration file, the device will be stopped and reset but not restarted.
Implication	After the occurrence of an error, the device is stopped, and instances associated with that device will not be available.
Resolution	The application should stop the instances and restart the device manually with the `command./adf_ctl` restart. The application is also required to re-allocate the instances.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.8 QATE-31270 - DC - Decompression: fatal error reported instead of invalid distance

Title	DC - Decompression: fatal error reported instead of invalid distance.
Reference #	QATE-31270
Description	If a malformed deflate input is fed to the decompression engine after power-on, the API might return a status of `CPA_DC_FATALERR` (-13) instead of `CPA_DC_INVALID_DIST` (-10). To cause the problem, the input should have a bad token early in the stream that references history, which is too far back.
Implication	Input is not decompressed, and an error is reported to the application.
Resolution	If a `CPA_DC_FATALERR` is reported, the application should discard output and abort the session calling `CpaDcRemoveSession`.
Affected OS	Linux
Driver/Module	CPM IA - Data Decompression

3.1.9 QATE-32074 - SRIOV - An unprivileged user space process in the same memory context as the Intel® QAT VFs can overwrite kernel memory

Title	SRIOV - An unprivileged user space process in the same memory context as the Intel® QAT VFs can overwrite kernel memory.
Reference #	QATE-32074
Description	Using `uio`, an unprivileged user space process in the same memory context as the Intel® QAT VFs can overwrite kernel memory.
Implication	Nefarious users may be able to launch privilege escalation attacks or other attacks.
Resolution	There is no workaround available. However, system policies (including limiting specific operating system permissions) can help to mitigate this issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.10 QATE-38236 - GEN - Intel® QAT driver can report a false hang if the heartbeat is polled too frequently

Title	GEN - Intel® QAT driver can report a false hang if the heartbeat is polled too frequently
Reference #	QATE-38236
Description	In some instances, the Intel® QAT driver can report a false hang if the heartbeat is polled too frequently. The false hang can result in spurious errors or an auto-reset if the Intel® QAT driver is configured to do so. This heartbeat is triggered more than once per second.
Implication	The Intel® QAT devices can report false errors and/or be reset unnecessarily.
Resolution	Do not poll the heartbeat more frequently than once per second.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.11 QATE-41707 - CY - Incorrect digest returned when performing a plain hash operation on input data of size 4GB or larger

Title	CY - Incorrect digest returned when performing a plain hash operation on input data of size 4 GB or larger.
Reference #	QATE-41707
Description	When performing an everyday hash operation on input data size of 4 GB or larger, the incorrect digest is returned.
Implication	The incorrect digest is returned for a plain hash operation.
Resolution	Future fix
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.12 QATE-41975 - CY - Device Utilization data for Symmetric Cryptography requests less than 1K may be under-reported.

Title	CY - Device Utilization data for Symmetric Cryptography requests less than 1K may be under-reported.
Reference #	QATE-41975
Description	With symmetric cryptography requests less than 1k, the device utilization data provided may be more than reported.
Implication	The actual device utilization for symmetric cryptography may be higher than reported when packets sizes are less than 1K.
Resolution	Future fix.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.13 QATE-42173 - SRIOV - Concurrent VF bring-up may fail

Title	SRIOV - Concurrent VF bring-up may fail.
Reference #	QATE-42173
Description	If Intel® QAT VFs are started concurrently, it is possible one or more of these may not succeed.
Implication	Some interrupts may be ignored, and the VF driver's start should be retried.
Resolution	NA.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.14 QATE-43713 - CY - Advertised device capability for rate limiting and device utilization may not work for all SKUs

Title	CY - Advertised device capability for rate limiting and device utilization may not work for all SKUs.
Reference #	QATE-43713
Description	When querying the device capability, the absolute numbers of the device capability may be incorrect.
Implication	Do not rely on the absolute numbers when not running on the top SKUs.
Resolution	Future fix
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.1.15 QATE-43900 - SRIOV - Removal of Intel® QAT PF kernel modules may affect other Intel® QAT device VFs

Title	SRIOV - Removal of Intel® QAT PF kernel modules may affect other Intel® QAT device VFs.
Reference #	QATE-43900
Description	When Intel® QAT VFs are available, if Intel® QAT PF kernel modules are removed, all Intel® QAT VFs may be removed if any Intel® QAT PF kernel modules are removed.
Implication	Intel® QAT may not be available without restarting the Intel® QAT service.
Resolution	If Intel® QAT PF kernel modules must be removed, it may be necessary to remove all Intel® QAT PF kernel modules rather than a subset and then restart the Intel® QAT service
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.16 QATE-45537 - Firmware authentication may fail if PCIe* errors occur or are injected

Title	Gen - Firmware authentication may fail if PCIe* errors occur or are injected.
Reference #	QATE-45537
Description	If PCIe errors occur or are injected on a platform, the Intel® QAT firmware authentication may fail.
Implication	The system may need to be rebooted to load Intel® QAT firmware successfully.
Resolution	None
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.17 QATE-50420 - GEN - Invalid device configuration files can lead to core crashes at runtime

Title	GEN - Invalid device configuration files can lead to core crashes at runtime
Reference #	QATE-50420
Description	If a configuration file includes definitions for either crypto or compression instances when that service is not enabled, a core crash may occur at run time.
Implication	A core crash may occur if device configuration files are improperly configured.
Resolution	Ensure services are enabled in `ServicesEnabled` before defining corresponding instances of that service type. The Intel® QAT driver will be updated to handle this invalid configuration gracefully.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.18 QATE-50650 - Gen - Potential leak of file descriptors with forking use case

Title	Gen - Potential leak of file descriptors with the forking use case.
Reference #	QATE-50650
Description	While forking a process, the software may not properly close file descriptors.
Implication	This will impact a customer's trying to fork multiple processes. There could be resources leaked and multiple file descriptors for the same file repeatedly being opened.
Resolution	None
Affected OS	Linux
Driver/Module	CPM IA - Common

3.1.19 QATE-52389 - SRIOV - Huge pages may not be compatible with QAT VF usage

Title	SRIOV - Huge pages may not be compatible with QAT VF usage.
Reference #	QATE-52389
Description	When using huge pages with the Intel ®QAT VFs, the QAT PF may see fatal errors and/or DMAR errors may be reported.
Implication	Huge pages cannot be used with the Intel® QAT VFs.
Resolution	None
Affected OS	Linux
Driver/Module	CPM IA - Common

§

3.2 Resolved Issues

3.2.1 QATE-2985 - SRIOV - Failed to send the response to VF

Title	SRIOV - Failed to send the response to VF.
Reference #	QATE-2985
Description	When bringing up one or more virtual functions in a host, the driver might report in the system log an error message similar to: "*Failed to send the response to VF*." This is due to a short timeout in the `PF2VF` protocol.
Implication	Some of the virtual functions might not be available for the host.
Resolution	This is resolved with the v0.9.1 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.2 QATE-3007 - GEN - Unexpected error message when trying to bring up the driver

Title	GEN - Unexpected error message when trying to bring up the driver.
Reference #	QATE-3007
Description	The driver reports an error similar to the one below when it is brought up with `adf_ctl:` Processing `/etc/c6xx_dev0.conf` Invalid affinity configuration Kernel space instances need to be allocated on bundles lower than user space instances Please change `CoreAffinity` configuration Failed to process section `SSL_INT_0` QAT Error: Invalid configuration Failed to configure `qat_dev1`.
Implication	The driver might not be able to load valid V2 configuration files that were correctly loaded by the legacy driver.
Resolution	This is resolved with the v0.9.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.3 QATE-3017 - CY - Zero-length authentication requests affect the result of other processes using the authentication service

Title	CY - Zero-length authentication requests affect the result of other processes using the authentication service.
Reference #	QATE-3017
Description	Zero-length authentication requests affect the comparison result of other authentication requests using the same accelerator.
Implication	An authentication check can report an incorrect negative value.
Resolution	This is resolved with the v1.0.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Crypto

3.2.4 QATE-3039 - GEN - Build fails when system time is set too far in the past, relative to the package

Title	GEN - Build fails when system time is set too far in the past, relative to the package.
Reference #	QATE-3039
Description	Extract the package on a system on which the system time is not set correctly and attempt to build it. The build fails.
Implication	The build fails.
Resolution	Not a defect. Update System Time in the target platform.
Affected OS	Linux
Driver/Module	Installer

3.2.5 QATE-3072 - GEN - Stack dump after the first adf_ctl down on a VF

Title	GEN - Stack dump after the first adf_ctl down on a VF.
Reference #	QATE-3072
Description	After the first `adf_ctl` down on a VF, the kernel reports on a Syslog a call trace, which suggests a problem caused by `adf_dev_stop`.
Implication	Warning reported in Syslog. No impact to the user.
Resolution	This is resolved with the v0.9.1 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.6 QATE-3073 - GEN - Memory corruption on module verification with kernel versions greater than 4.5

Title	GEN - Memory corruption on module verification with kernel versions greater than 4.5.
Reference #	QATE-3073
Description	Verifying any Linux kernel module signature after loading the acceleration driver on any platform with a Linux kernel v4.5 and onwards will cause a memory corruption issue. This issue is due to a bug in the kernel for which a fix has been submitted.
Implication	The memory corruption will likely cause a kernel panic and make the system unusable.
Resolution	Do not load any signed kernel module after loading the acceleration driver. Load the acceleration driver at the very last.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.7 QATE-3137 - CY - AES-XTS does not support buffers sizes that are not a multiple of 16B

Title	CY - AES-XTS does not support buffers sizes that are not a multiple of 16B.
Reference #	QATE-3137
Description	A single request with a data size that is not a multiple of 16B for AES-XTS will fail in the IA Intel® QAT driver with an invalid parameter check.
Implication	The user cannot submit AES-XTS Crypto requests with buffers that are not multiples of 16B.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.8 QATE-3220 - GEN - Potential Response Data Leak

Title	GEN - Potential Response Data Leak.
Reference #	QATE-3220
Description	An internal Intel® QAT system resource is being released back to the resource pool before the PRF service has finished, and it is reused by other services.
Implication	When accelerating TLS Pseudo-Random Function (PRF) in parallel with another service (crypto or compression), portions of input data may leak between processes or virtual machines. This leak is more probable when the system is under stress. For example, when running symmetric crypto encryption in parallel with TLS PRF, portions of the input data sent for encryption might appear in the TLS PRF output buffer without encryption.
Resolution	This is resolved with the v0.9.0 release.
Affected OS	Linux
Driver/Module	CPM IA – Common

3.2.9 QATE-3259 - GEN - Package does not build on CentOS* v6.8

Title	GEN - Package does not build on CentOS* 6.8.
Reference #	QATE-3259
Description	Due to changes in the Linux kernel, the software package may fail to compile on some newer Linux distributions, including CentOS v6.8.
Implication	The software package fails to compile.
Resolution	This is resolved with v1.0.2 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.10 QATE-3350 - CY - skcipher, akcipher Intel® QAT implementations in kernel space do not support CRYPTO_TFM_REQ_MAY_BACKLOG

Title	CY - skcipher, akcipher Intel® QAT implementations in kernel space do not support CRYPTO_TFM_REQ_MAY_BACKLOG.
Reference #	QATE-3350
Description	Skcipher and akcipher implementations in the Intel® QAT driver are not capable of backlog requests.
Implication	Some kernel applications, e.g., dm-crypt, might report a kernel panic.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.11 QATE-3369 - DC - Increased minimum destination buffer size for compression

Title	DC - Increased minimum destination buffer size for compression.
Reference #	QATE-3369
Description	During the compression of a request that is a multiple of 8 bytes in length (compress a file 1024 bytes long), extra work must be done to validate that no data is lost as the end of the request.
Implication	This workaround implies that the minimum compression destination buffer size has increased from 64 bytes to 96 bytes. The new minimum destination buffer size (96B) must be used for all compression requests (static and dynamic compression, stateful, and stateless).
Resolution	This is resolved with the v0.6.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.12 QATE-3404 - GEN - The included memory driver fails during memory allocation

Title	GEN - The included memory driver fails during memory allocation.
Reference #	QATE-3404

Description	During stressful memory allocation, the included memory driver may fail with below logs and potential kernel crash:
	User-space logs:
	`------------------------------`
	`CMD NUMA fail qaeMemAllocNUMA:737`
	`mmap on memory allocated through ioctl failed`
	
	Kernel-space logs:
	`------------------------------`
	`kernel: mem_mmap:528 cannot find meminfo`
	`kernel: userMemFree:328 Could not find slab with id: xx`

Implication	Memory drivers may fail to allocate memory in stress conditions. A reboot is required to continue normal operations.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - USDM

3.2.13 QATE-3547 - GEN - Killing a Process May Lead to a Kernel Panic

Title	GEN - Killing a Process May Lead to a Kernel Panic.
Reference #	QATE-3547
Description	When a process using the driver is killed or terminates unexpectedly, the buffers associated with the bundle are flushed during the cleanup operation. Due to a race condition between releasing the memory by the included memory driver and flushing the buffers, it can sometimes happen that this causes a kernel panic.
Implication	If this occurs, the system must be rebooted.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - USDM

3.2.14 QATE-3563 - GEN - Lewisburg/Denverton: A Step: The driver can report Spurious Completion Abort Errors

Title	GEN - Lewisburg/Denverton: A Step: The driver can report Spurious Completion of Abort Errors.
Reference #	QATE-3563
Description	The driver can report Spurious PCIe Completer Abort errors when a completion returns to the driver with Completer Abort status.
Implication	The end-user may see spurious PCIe completion abort errors coming from the driver. The driver will never generate the completion of abort errors under any other circumstances.
Resolution	This is resolved with Revision B silicon.
Affected OS	Linux
Driver/Module	n/a

3.2.15 QATE-3635 - SRIOV - VFs cannot be cleanly disabled on acceleration device

Title	SRIOV - VFs cannot be cleanly disabled on the acceleration device.
Reference #	QATE-3635
Description	Writing 0 to `/sys/bus/pci/devices/<BDF>/sriov_numvfs` results in no action.
Implication	Virtual functions cannot be disabled by writing 0 to `/sys/bus/pci/devices/<BDF>/sriov_numvfs`.
Resolution	This is resolved with the v4.2.0 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.16 QATE-3650 - SRIOV - unbind of VFs to guests does not work correctly when the VF driver is loaded in the host

Title	SRIOV - The unbind of VFs to guests does not work correctly when the VF driver is loaded in the host.
Reference #	QATE-3650
Description	We observed issues when detaching VFs from the host to a guest when the VF driver is loaded in the host.
Implication	Detaching VFs from a host to a guest as well as sharing VFs between hosts and guests might not work.
Resolution	Not a defect, the test procedure has been updated.
Affected OS	Linux
Driver/Module	n/a

3.2.17 QATE-3683 - DC - Stateful Decompression Returns -13 Error with Negative Test (A step silicon only)

Title	DC - Stateful Decompression Returns -13 Error with Negative Test (A step silicon only).
Reference #	QATE-3683
Description	If incorrectly formatted data is fed to the hardware, the API may return a status of - 13 (`CPA_DC_FATALERR`). This error means that the session needs to be restarted, but the device does not need to be reset.
Implication	For stateful decompression, if the input content is invalid, both a - 10 soft error and a - 13 hard error are reported. Only the hard error is sent back to the driver as the hard error has a higher priority.
Resolution	For A step silicon: If an invalid stateful decompression request is sent to the Intel® QAT driver, and a - 13 error code is returned, the complete session should be restarted. There is no need to reset the device. This invalid request is resolved with B step silicon.
Affected OS	Linux
Driver/Module	CPM IA - Data Compression

3.2.18 QATE-3693 - SRIOV - Incorrect config file for PFs when VFs are enabled in the host

Title	SRIOV - Incorrect config file for PFs when VFs are enabled in the host.
Reference #	QATE-3693
Description	When the driver is installed in the Host with option 3 (Install SR-IOV Host Acceleration), an incorrect configuration is installed in the system. This incorrect configuration prevents the sample code from running correctly.
Implication	When trying to run the sample code in a configuration where VFs are enabled in the host, the sample code might not run properly or report an error message similar to `[error] SalCtrl_AdfServicesStartedCheck() -: Sal Ctrl failed to start in given time [error] do_userStart() -: Failed to start services main():731` Could not start `sal` for user space
Resolution	This is resolved with the v0.8.1 release.
Affected OS	Linux
Driver/Module	ADF - User Mode

3.2.19 QATE-3702 - DC - Decompression Failure, empty dynamic block reports - 7 error

Title	DC - Decompression Failure, empty dynamic block reports - 7 error.
Reference #	QATE-3702
Description	When a user submits one or more valid empty dynamic blocks, compression slice returns - 7 error code. Software implementations can decompress these block(s) successfully. An example of valid empty dynamic block: `04 c0 81 08 00 00 00 00 20 7f eb 13 00 00 ff ff.`
Implication	A - 7 soft error will be reported on a valid empty dynamic compressed block(s).
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM FW – Data Compression

3.2.20 QATE-3715 - CY - Incorrect hash generated with SHA384 and secret length > 64 bytes.

Title	CY - Incorrect hash generated with SHA384 and secret length > 64 bytes.
Reference #	QATE-3715
Description	An incorrect hash is generated when using `SHA384` with a secret length greater than 64 bytes. If the secret is length is `<= 64` bytes OR the hash algorithm is different from `SHA384`, the results are correct.
Implication	Don't use a secret length of > 64-bytes with `SHA384`.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.21 QATE-3791 - GEN - Lewisburg: Common Memory Driver incorrectly allocates memory of size between 2 MB and 4 MB

Note: This errata applies to LBG-NS only

Title	GEN - Lewisburg: Common Memory Driver incorrectly allocates memory of size between 2 MB and 4 MB.
Reference #	QATE-3791
Description	**This errata applies to LBG-NS only**. If the included memory driver (`qae_mem.ko`) is used to allocate a block of pinned memory of a size between 2 MB and 4 MB, the pointer to the allocated memory returned may be incorrect. The included memory driver does not support allocating a block of memory of 4 MB or larger.
Implication	The result of an application using a block of memory between 2 MB and 4 MB in size is indeterminate. The most likely behavior is a segmentation fault in the application using the allocated memory. Attempting to allocate memory of size 4MB or higher using the memory driver will fail.
Resolution	This is resolved with the v0.7.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.22 QATE-3955 - DC - Compression operations involving payloads above 64K while using Compress and Verify functionality may fail

Title	DC - Compression operations involving payloads above 64K while using Compress and Verify functionality may fail.
Reference #	QATE-3955
Description	Compression operations using Compress and Verify functionality may fail with `CpaDcReqStatus` of `CPA_DC_VERIFY_ERROR` or `CPA_DC_MCADECOMPERR`. The issue is observed with sessions using payload sizes above 64 K when `Storage_Enabled` = 1 in the device configuration file and the compression operations request that `CpaDcOpData.mcaDecompressCheck` = `CPA_TRUE` while calling `cpaDcCompressData2()` API.
Implication	None
Resolution	This has been confirmed as a test code issue.
Affected OS	Linux
Driver/Module	CPM IA - Sample Code

3.2.23 QATE-3971 - DC - Lewisburg/Denverton: A Step: Static Compression failure when running static and dynamic in parallel

Title	DC - Lewisburg/Denverton: A Step: Static Compression failure when running static and dynamic in parallel.
Reference #	QATE-3971
Description	While running multiple static and dynamic compression threads in parallel for a few hours, silent data loss can be seen.
Implication	When running static and dynamic compression in parallel over a long period, it is possible to lose static data silently.
Resolution	This is resolved with Revision B silicon.
Affected OS	Linux
Driver/Module	CPM IA - Data Compression

3.2.24 QATE-3978 - GEN – The Intel® QAT service must be restarted after a reboot

Title	GEN - The Intel® QAT service must be restarted after a reboot.
Reference #	QATE-3978
Description	On a fresh boot after previous Intel® QAT driver installation, an Intel® QAT application (e.g., the performance sample code) cannot immediately run.
Implication	The following error is seen: `[error] SalStatistics_GetStatEnabled() - :` Failed to get `statsGeneral` from configuration file `ADF_UIO_PROXY err: adf_user_subsystemInit: F`ailed to initialize Subservice SAL `[error] SalCtrl_ServiceEventStart() - :` Private data is NULL `ADF_UIO_PROXY err: adf_user_subsystemStart:` Failed to start Subservice SAL `[error] SalCtrl_AdfServicesStartedCheck() - :` Sal Ctrl failed to start in given time `[error] do_userStart() - : F`ailed to start services `ADF_UIO_PROXY err: icp_adf_subsystemUnregister:` Failed to shutdown subservice SAL. `main()`:710 Could not start sal for user space
Resolution	This is resolved with the v0.7.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.25 QATE-3981 - GEN - Stress test with concurrent crypto and compression may fail with a segfault

Title	GEN - Stress test with concurrent crypto and compression may fail with a segfault.
Reference #	QATE-3981
Description	When running crypto, compression, and decompression concurrently, a segmentation fault may be observed. In one case, the segmentation was observed after seven hours of running the following operations concurrently: * `AES256-CBC + SHA512 IMIX` * Stateless Deflate 50% compress and 50% decompress.
Implication	The application fails with a segmentation fault.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	Test Code

3.2.26 QATE-3982 - GEN - Child process crashes as it is accessing the Parent process's address space

Title	GEN - Child process crashes as it is accessing the Parent process's address space.
Reference #	QATE-3982
Description	Parent process calls `icp_sal_userStartMultiProcess()`, which allocates memory for all rings. When a Child process subsequently calls `icp_sal_userStartMultiProcess()`, the memory for rings is not remapped. Thus when a Child process starts a polling thread and tries to access the rings, it crashes as it is accessing the Parent process's address space.
Implication	Child process crash.
Resolution	This is resolved with the v4.3.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.27 QATE-3986 - GEN - The included memory driver impacts Traditional API sample code performance

Title	GEN - The included memory driver impacts Traditional API sample code performance.
Reference #	QATE-3986
Description	The included memory driver has a significant impact on the performance of the traditional API sample code. The impact depends on the number of instances used per device, but it has been observed to be impacted by 50% or more in most cases.
Implication	The performance of the sample code using the traditional API is lower than expected.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.28 QATE-4015 - GEN - Building the driver with LAC_HW_PRECOMPUTES is not supported in this version of the driver

Title	**GEN - Building the driver with LAC_HW_PRECOMPUTES is not supported in this version of the driver.**
Reference #	QATE-4015
Description	If the driver is built with the `LAC_HW_PRECOMPUTES` compiler option, the system may hang and/or crash.
Implication	The `LAC_HW_PRECOMPUTES` feature should not be used. Software precomputes, which are the default, must be used instead.
Resolution	Do not use the `LAC_HW_PRECOMPUTES` compiler option. This option will not be fixed.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.29 QATE-4018 - SYM DP - cpaCySymDpEnqueueOpBatch accepts only requests in a batch of the same session

Title	**SYM DP - cpaCySymDpEnqueueOpBatch accepts only requests in a batch of the same session.**
Reference #	QATE-4018
Description	When the package is built with `ICP_PARAM_CHECK`, `cpaCySymDpEnqueueOpBatch` accepts only batches of requests for the same session. When requests for different sessions are provided, this API fails to return the `CPA_STATUS_INVALID` parameter and reports the following message: "*All session contexts should be the same in the requests*."
Implication	It is not possible to use the Data Plane API to submit batches of requests that belong to different sessions using `cpaCySymDpEnqueueOpBatch`.
Resolution	This is resolved with the 0.9.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.30 QATE-4051 - GEN - Full device pass-through not available on KVM guests

Title	GEN - Full device pass-through not available on KVM guests.
Reference #	QATE-4051
Description	The new firmware authentication feature requires PF devices to be reset via function level reset (FLR) before firmware download. In KVM guests, all pass-through devices attached to a VM are reset at boot time. Any further device reset is trapped by the hypervisor and not issued. This causes firmware authentication to fail after the first firmware download. Full device pass-through might work in some conditions when using `vfio` and if the host kernel and the platform support it.
Implication	Direct mode feature not available on KVM guests for devices on full pass-through mode.
Resolution	Refer to appendix A of Using Intel® Virtualization Technology (Intel® VT) with Using Intel® Virtualization Technology (Intel® VT) with Intel® QuickAssist Technology Application Note (document number 330689-008) for instructions on how to pass through a Intel® QAT PF to a VM. Talk to your Intel representative for more information.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.31 QATE-4070 - GEN - The driver fails to send requests if the first ring put operation returns a retry or a failure when using partial symmetric crypto operations

Title	GEN - The driver fails to send requests if the first ring put operation returns a retry or a failure when using partial symmetric crypto operations.
Reference #	QATE-4070
Description	The driver can enter a deadlock state due to improper locking when using symmetric crypto operations with partial packets. A deadlock state occurs when there is heavy traffic, and the 1st request receives a retry or failure when it tries to send a message to the ring.
Implication	When using the application server and using symmetric crypto operations with partial packets, then it is possible to receive a retry when trying to send the first request, causing the `nonBlockingOpsInProgress` to be set to false. The callback function for the 1st response won't be called, causing all the requests for this session to be en-queued, and none can be de-queued and sent to the ring until the client and application server stops communicating. The application server has connection leaks when the client sends many requests at the same time. When the client stops sending requests, there are many "active connections" left in the application server.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.32 QATE-4071 - CY - cpaCySymRemoveSession fails in Data-Plane API if other active Session sharing ring

Title	CY - cpaCySymRemoveSession fails in Data-Plane API if other active Session sharing ring.
Reference #	QATE-4071
Description	If multiple sessions are sharing the same Crypto DP instance, then a call to `cpaCySymRemoveSession()` will fail if there are messages inflight from another session.
Implication	`cpaCySymRemoveSession()` may fail.
Resolution	This is resolved with the v0.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.33 QATE-4111 - DC - Engine timeout not handled correctly

Title	DC - Engine timeout not handled correctly.
Reference #	QATE-4111
Description	When an engine timeout occurs due to watchdog expiration, compression engines might lock up.
Implication	In some rare conditions, the compression engine might become unresponsive.
Resolution	This timeout is resolved with a v4.1.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.34 QATE-5433 - GEN - User space library supports only 32 devices

Title	GEN - The user space library supports only 32 devices.
Reference #	QATE-5433
Description	The user-space library enumerates only the first 32 devices in the system.
Implication	In a system with more than 32 devices, the devices indexed at and higher than 32 are unusable. Because of this, when running an application, even if there are more than 32 started, the application only uses 32 devices.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.35 QATE-5520 - DC - Stateful Dynamic compression might report a spurious CPA_DC_FATALERR

Title	DC - Dynamic Stateful compression might report a spurious CPA_DC_FATALERR.
Reference #	QATE-5520
Description	If the physical address (or I/O virtual address) of the `PrivateMetaData` of the compression context buffer has byte `0` set to `0x07` in the high part of an address, the compression operation might fail with `CPA_DC_FATALERR`.
Implication	A spurious `CPA_DC_FATALERR` might be returned by the compression engine. After this error is reported, it is not possible to continue submitting jobs using the same session.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Data compression

3.2.36 QATE-5989 - CY - AES-GCM operations with zero-length plain text results in an incorrect tag result

Title	CY - AES-GCM operations with zero-length plain text results in an incorrect tag result.
Reference #	QATE-5989
Description	Sending an AES-GCM operation with zero-length plain text using the Intel® QAT API results in an incorrect tag result.
Implication	The incorrect result when computing AES-CCM for zero-length payloads.
Resolution	This is resolved with the v4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.37 QATE-6463 - GEN - icp_sal_userStart and icp_sal_userStartMultiProcess hang if they are called more than once in the same process

Title	GEN - icp_sal_userStart and icp_sal_userStartMultiProcess hang if they are called more than once in the same process.
Reference #	QATE-6463
Description	`Icp_sal_userStart` and `icp_sal_userStartMultiProcess` hang if they are called more than once in the same process when no instances are left.
Implication	The caller to these functions can be blocked forever.
Resolution	This is resolved with the v0.9.2 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.38 QATE-7393 - CY - AES-CCM operations with zero-length plain text results in an incorrect tag result

Title	CY - AES-CCM operations with zero-length plain text results in an incorrect tag result.
Reference #	QATE-7393
Description	Sending an AES-CCM operation with zero-length plain text using the Intel® QAT API results in an incorrect tag result.
Implication	The incorrect result when computing AES-CCM for zero-length payloads.
Resolution	This is resolved with the v4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.39 QATE-7563 - SYM - Watchdog timer errors not reported to user callback

Title	SYM - Watchdog timer errors not reported to user callback.
Reference #	QATE-7563
Description	Watchdog errors are not reported to user callbacks for crypto operations.
Implication	If a watchdog timer expires, the user application is not notified.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.40 QATE-7919 - GEN - ICP_WITHOUT_THREAD not supported

Title	GEN - ICP_WITHOUT_THREAD not supported.
Reference #	QATE-7919
Description	The software package no longer supports the `ICP_WITHOUT_THREAD` build flag.
Implication	It is not possible to build a version of the software package that does not use the `pthread` library.
Resolution	This is resolved with the v4.5.0 release. A new configuration option called - **enable-icp-without-thread** has been added to the software package.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.41 QATE-8109 - GEN - Driver and firmware versions are not reported to userspace

Title	GEN - Driver and firmware versions are not reported to user space.
Reference #	QATE-8109
Description	Driver and firmware versions are not reported through the `sysfs` and cannot be queried using the `icp` API.
Implication	User applications are not able to query the software package versions.
Resolution	This is resolved with the v4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.42 QATE-8189 - CY - Key derivation function for PRF with SHA256 and 128 bytes secret causes unexpected results

Title	CY - Key derivation function for PRF with SHA256 and 128 bytes secret causes unexpected results.
Reference #	QATE-8189
Description	When performing a Key Derivation Function for TLS 1.2 for PRF, with a `SHA256` hash, the accelerator hangs and reports a fatal error if the secret used is 128 bytes.
Implication	128 bytes secrets are not supported at this time. The accelerator might hang, report a fatal error, or produce incorrect results.
Resolution	This is resolved with the v1.0.3 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.43 QATE-8233 - GEN - Installation of Intel® QAT Software on Yocto or Ubuntu image results in libraries not being placed in the default system path

Title	GEN - Installation of Intel® QAT Software on Yocto or Ubuntu image results in libraries not being placed in the default system path.
Reference #	QATE-8233
Description	The shared library `libqat_s.so` may be installed somewhere other than the default directory.
Implication	Applications may fail to link to the `libqat_s`.so at run time. This failure has been observed with Yocto images and Ubuntu v15.x and v16.x.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.44 QATE-9234 - GEN - Child process should not inherit mapping to Intel® QAT rings

Title	GEN - Child process should not inherit mapping to Intel® QAT rings.
Reference #	QATE-9234
Description	If a process forks after calling the `icp_sal_userStart`, when the child process exits, the `Syslog` will show a message "`Process <PID> <NAME>` exit with orphan rings."
Implication	None
Resolution	This is resolved with the v4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.45 QATE-9241 - GEN - Process exit with orphan rings when spawning multiple processes

Title	GEN - Process exit with orphan rings when spawning multiple processes.
Reference #	QATE-9241
Description	If multiple processes start a user space service access layer (`icp_sal_userStart`) and they all exist together, the `Syslog` may show a message "`Process <PID> <NAME>`" exit with orphan rings.
Implication	A kernel panic might happen at reboot if an application is using Intel® QAT.
Resolution	This is resolved with v1.0.5 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.46 QATE-9326 - DC - Changing StorageEnabled back to 0 doesn't reload FW

Title	DC - Changing StorageEnabled back to 0 doesn't reload FW.
Reference #	QATE-9326
Description	If the configuration file is modified to change `StorageEnabled` from 1 to 0, this does not cause the storage firmware to be replaced to the standard one.
Implication	PKE functions will not work after changing `StorageEnabled` from 1 to 0.
Resolution	This is resolved with the v4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.47 QATE-9383 - GEN - When StorageEnabled = 1, the Intel® QAT driver tries to register into the Linux Kernel Crypto framework

Title	GEN - When StorageEnabled = 1, the Intel® QAT driver tries to register into the Linux Kernel Crypto framework.
Reference #	QATE-9383
Description	When `StorageEnabled` = 1 is selected in the `config` file, the Intel® QAT driver tries to register itself into the Linux Kernel Crypto framework even if crypto operations are not available.
Implication	An error saying that `akcipher` self-test failed might be reported in the `Syslog`.
Resolution	This is resolved with the v4.6.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.48 QATE-9483 - GEN - Uncorrectable errors might lead to a kernel panic

Title	GEN - Uncorrectable errors might lead to a kernel panic.
Reference #	QATE-9483
Description	If an uncorrectable error is triggered when there are in-flight requests, the system might crash and report kernel panic.
Implication	If this error occurs, the system must be rebooted.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.49 QATE-9545 - PERF - Performance drop with Scatter Gather Lists (SGLs) composed of flat buffers of 1460B

Title	PERF - Performance drop with Scatter Gather Lists (SGLs) composed of flat buffers of 1460B.
Reference #	QATE-9545
Description	Excluding DH895X devices, a moderate performance drop might be experienced when using SGLs if the size of each collected flat buffer is not a multiple of 1024 bytes.
Implication	Applications might not perform as expected.
Resolution	This is resolved with the v4.4.0 release. However, for performant applications, it is recommended to use flat buffers or SGLs with a single flat buffer or ensure that flat buffers within an SGL are 1024B aligned.
Affected OS	Linux
Driver/Module	CPM Firmware - Crypto

3.2.50 QATE-10780 - DC - Dynamic compression capability not properly reported by cpaDcQueryCapabilities

Title	DC - Dynamic compression capability not properly reported by cpaDcQueryCapabilities.
Reference #	QATE-10780
Description	When querying the Intel® QAT driver using the function `cpaDcQueryCapabilities`, the API reports `dynamicHuffman` as `CPA_TRUE` even though dynamic compression is not supported by this release.
Implication	It is possible to discover that dynamic compression is disabled only when calling `cpaDcCompressData`, The dynamic compression being disabled, will impact the behavior of applications that query the device capabilities.
Resolution	This is resolved with the v4.0.1 release.
Affected OS	Linux
Driver/Module	CPM IA - Data compression

3.2.51 QATE-11629 - GEN - Module signature not supported by Intel® QAT installers

Title	GEN - Module signature not supported by Intel® QAT installers.
Reference #	QATE-11629
Description	The installer fails to load the Intel® QAT modules when Secure Boot is enabled on the platform. The Intel® QAT installer does not support signing kernel modules with a custom key.
Implication	Intel® QAT kernel modules should be signed manually to use UEFI Secure boot.
Resolution	This is resolved with the v4.0.1 release.
Affected OS	Linux
Driver/Module	Installer

3.2.52 QATE-11790 - CY - CPA_STATUS_FAIL reported for subsequent requests when a PKE request times out

Title	**CY - CPA_STATUS_FAIL reported for subsequent requests when a PKE request times out.**
Reference #	QATE-11790
Description	When an engine timeout is detected for the PKE service, subsequent requests might fail with the same error.
Implication	A reset is required for future PKE requests to be ensured to succeed.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.53 QATE-11828 - GEN - Kernel panic observed in Intel® QAT driver for c62x included in kernels between v4.5 and v4.8

Title	**GEN - Kernel panic observed in Intel® QAT driver for c62x included in kernels between v4.5 and v4.8**
Reference #	QATE-11828
Description	When loading the Intel® QAT driver included in a kernel distribution, the platform might report a kernel panic.
Implication	When uninstalling the Intel® QAT driver, the Intel® QAT driver present in the distribution is re-loaded, this might cause a kernel panic.
Resolution	Not a defect in the current version of the software. *Blacklist the Intel® QAT driver.* Refer to instructions in the Intel® QAT *Getting Started Guide, v1.7*.
Affected OS	Linux with kernel version between v4.5 and v4.8
Driver/Module	ADF - Kernel Mode

3.2.54 QATE-11933 - GEN - rng operation in progress while unregistering Intel® QAT AEAD implementation in the kernel

Title	GEN - rng operation in progress while unregistering Intel® QAT AEAD implementation in the kernel.
Reference #	QATE-11933
Description	A crypto operation may be in progress when the AEAD implementation in the kernel is unregistered.
Implication	With a stress test that reboots a platform continuously, a kernel panic might be observed.
Resolution	This is resolved with v1.0.5 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Module

3.2.55 QATE-12256 - VIRT - Device indices not handled correctly when a device is detached from the driver

Title	VIRT - Device indices not handled correctly when a device is detached from the driver.
Reference #	QATE-12256
Description	After detaching a device from the Intel® QAT driver, for example, in preparation for passing a VF to a VM, `qat_service` might report inconsistent indices and BDFs.
Implication	`qat_service` might report inconsistent information after a device has been detached from the Intel® QAT driver.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.56 QATE-12516 - GEN - CpaInstanceInfo2.instID reports erroneous quotes

Title	GEN - CpaInstanceInfo2.instID reports erroneous quotes.
Reference #	QATE-12516

Description	The CpaInstanceInfo2 structure returned from `cpaCyInstanceGetInfo2()` and `cpaDcInstanceGetInfo2()` shows that the field "`instID`" contains unneeded quotes. For example, using default configuration files the following strings are printed when inspecting the `CpaInstanceInfo2` runtime structures:
	`CY Instance zero shows:`
	`CpaInstanceInfo2.instID = SSL_INT_0_"SSL0"`
	`DC Instance zero shows:`
	`CpaInstanceInfo2.instID = SSL_INT_0_"Dc0"`

Implication	If the application looks at the `instID` field, the comparison might need to include these erroneous quotes.
Resolution	This is resolved with the v4.5.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.57 QATE-12793 - SYM - Algchain: chained crypto and hash requests for DES, 3DES, and Kasumi might report an incorrect output digest

Title	SYM - Algchain: chained crypto and hash requests for DES, 3DES, and Kasumi might report an incorrect output digest.
Reference #	QATE-12793
Description	When performing an algorithm chaining operation using `DES CBC, 3DES CBC`, `Kasumi` F8 as an encryption algorithm, and any hash algorithm, the resulting digest might be miscalculated.
Implication	Results digest from chained operations with `DES CBC, 3DES CBC,` and `Kasumi` F8 might not be correct.
Resolution	This is resolved with the v4.2.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.58 QATE-14171 - Run time error if the library is built with --enable-icp-dc-only

Title	Run time error if the library is built with --enable-icp-dc-only.
Reference #	QATE-14171
Description	When the driver is built with `--enable-icp-dc`-only, the `icp_sal_userStart()` API might report a run time error similar to the following: `[error] SalCtrl_GetEnabledServices()` - : Error parsing enabled services from ADF `[error] SalCtrl_ServiceEventHandler()` - : Failed to get enabled services `ADF_UIO_PROXY err: adf_user_subsystemInit`: Failed to initialize Subservice SAL
Implication	"`--enable-icp-dc-only`" was not supported until the v4.1.0 release.
Resolution	This is resolved with the v4.1.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.59 QATE-14458 - GEN - Functional sample code fails to build when the package is built in dc-only mode

Title	GEN - Functional sample code fails to build when the package is built in dc-only mode.
Reference #	QATE-14458
Description	When the Intel® QAT package is built with the option `--enable-icp-dc-only`, the functional sample codes fail to build reporting an error similar to the following: `make` `rm -vf *.o dc_stateless_sample` `cc -Wall -O1 -I/quickassist/include/ -I/quickassist/include/lac -I/quickassist/include/dc -l /quickassist/lookaside/access_layer/include -I/quickassist/lookaside/access_layer/src/sample_code/functional/include -I/quickassist/utilities/libusdm_drv// -DUSER_SPACE -DDO_CRYPTO -DWITH_UPSTREAM -DWITH_CMDRV ./../common/cpa_sample_utils.c cpa_dc_stateless_sample.c cpa_dc_sample_user.c -L/usr/Lib -L/build /build/libqat_s.so /quickassist/utilities/libusdm_drv//linux/build/linux_2.6/user_space/libusdm_drv.a -lpthread -lcrypto -ludev -o dc_stateless_sample` `/tmp/ccnX80N8.o: In function `sal_polling':` `cpa_sample_utils.c:(.text+0xb5): undefined reference to `icp_sal_CyPollInstance'` `/tmp/ccnX80N8.o: In function `sampleCyGetInstance':` `cpa_sample_utils.c:(.text+0x14e): undefined reference to `cpaCyGetNumInstances'` `cpa_sample_utils.c:(.text+0x169): undefined reference to `cpaCyGetInstances'` `/tmp/ccnX80N8.o: In function `sampleCyStartPolling':` `cpa_sample_utils.c:(.text+0x209): undefined reference to `cpaCyInstanceGetInfo2'` `collect2: error: ld returned 1 exit status` `/quickassist/lookaside/access_layer/src/sample_code/functional/dc/stateless_sample/./../common.mk:130: recipe for target 'default' failed` `make: *** [default] Error 1`
Implication	It is not possible to build the functional sample codes when the package is built in dc-only mode.
Resolution	This is resolved with the v4.3.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Sample code

3.2.60 QATE-14779 - CY - On SKUs with PKE service-disabled, self-test fails when driver loads and watchdog timer errors might be reported

Title	**CY - On SKUs with PKE service-disabled, self-test fails when driver loads and watchdog timer errors might be reported.**
Reference #	QATE-14779

Description	On SKUs with PKE disabled, the self-test provided by the Linux kernel might fail with an error similar to the following
	`[ +1.167496] alg: akcipher: encrypt test failed. err -22`
	`[ +0.001260] alg: akcipher: test 1 failed for qat-rsa, err=-22`
	`[ +0.001478] alg: dh: generate public key test failed. err -22`
	`[ +0.001245] alg: dh: test failed on vector 1, err=-22`
	When running the `cpa_sample_code`, the PKE might fail with the following message: [error] `LacPke_MsgCallback()–`: The slice hang error is detected on the MMP slice.

Implication	No functional impact.
Resolution	The error can be ignored. Talk with your Intel representative for more information.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.61 QATE-14870 - GEN - Library built with --enable-lac-hw-precomputes might report run time errors

Title	**GEN - Library built with --enable-lac-hw-precomputes might report run time errors.**
Reference #	QATE-14870
Description	The user-space library might report run time errors (e.g., segmentation faults) if built with `enable-lac-hw-precomputes`.
Implication	`lac-hw-precomputes` configuration option is not supported in this release.
Resolution	This option has been removed since release v4.2.0.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.62 QATE-14920 - GEN - Library built with --enable-icp-trace might report run time errors

Title	GEN - Library built with --enable-icp-trace might report run time errors.
Reference #	QATE-14920
Description	The user-space library might report run time errors (e.g., segmentation faults) if built with `enable-icp-trace`.
Implication	the `enable-icp-trace` configuration option is not supported in this release.
Resolution	This has been confirmed to be a test issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.63 QATE-14953 - SRIOV - VF driver might report errors if the device is reset

Title	SRIOV - VF driver might report errors if the device is reset.
Reference #	QATE-14953
Description	If a manual or automatic device reset (FLR or SBR) is triggered as a result of an error (e.g., heartbeat failure, end fatal errors, etc.) on a system with Intel® QAT VFs enabled, the VF driver might report run time errors and might not recover.
Implication	The reset of the PF driver is not supported when VFs are enabled.
Resolution	This is resolved with the v4.2.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.64 QATE-15136 - GEN - Hang of asymmetric crypto engines might not be detected by heartbeat

Title	GEN - Hang of asymmetric crypto engines might not be detected by heartbeat.
Reference #	QATE-15136
Description	Heartbeat might not detect a hang of an asymmetric crypto engine.
Implication	The device might be reported as responsive even if one of the engines is hung.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.65 QATE-18691 - DC - Incorrect consumed bytes reported during decompression

Title	DC - Incorrect consumed bytes reported during decompression.
Reference #	QATE-18691
Description	In some circumstances, the calculation of residue bits at the end of the decompression stream may be inaccurate.
Implication	For decompression requests where the last `bfinal` bit is 1, the number of bytes reported consumed may be incorrect. Also, for decompression requests where the last `bfinal` bit is 0, an extra byte of output may be emitted. This is not applicable to data compressed using the Intel® Communications Chipset 8925 to 8955 Series with `bfinal`=0 and `bfinal`=1. T This is not applicable to data compressed by other accelerators covered by release 4.2.0 and prior with `bfinal`=1.
Resolution	This is resolved with the v4.3.0 release.
Affected OS	All
Driver/Module	CPM HW - Data Decompression

3.2.66 QATE-20186 - DC - endOfLastBlock not set in CpaDcRqResults during Stateful decompression with an overflow of the last chunk

Title	DC - endOfLastBlock not set in CpaDcRqResults during Stateful decompression with the overflow of the last chunk.
Reference #	QATE-20186
Description	When performing decompression operations in Stateful sessions, the application will not see the `endOfLastBlock` property set in `CpaDcRqResults` if the last request of the stream is zero bytes long. This scenario may happen when the flush flag is set to `CPA_DC_FLUSH_FINAL`, and overflow happens on the last packet of data to be decompressed.
Implication	The `endOfLastBlock` property is not set in the `CpaDcRqResults` structure. Consumed and produced fields in the `CpaDcRqResults` structure remain correct when the issue happens.
Resolution	This is resolved with the v4.3.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.67 QATE-21561 - CY - PkeServiceDisabled = 1 in the user configuration file might cause a failure during driver initialization

Title	CY - PkeServiceDisabled = 1 in the user configuration file might cause a failure during driver initialization.
Reference #	QATE-21561
Description	When `PkeServiceDisabled` is set to 1 in the configuration file, the software (1) incorrectly registers PKE services with the Linux Kernel crypto infrastructure, and (2) sets an incorrect mask for the asymmetric crypto capabilities.
Implication	The driver may fail to initialize, a software crash may occur, or failure will occur in PKE operations. Asym crypto capabilities are incorrectly reported to the user-space driver.
Resolution	This is resolved with the v4.5.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.68 QATE-29663 - GEN - Device index may be off with rmmod after adf_ctl up or qat_service start

Title	GEN - Device index may be off with rmmod after adf_ctl up or qat_service start
Reference #	QATE-29663
Description	When using multiple types of devices represented by different modules (e.g., `qat_dh895xcc.ko` and `qat_c62x.ko`), and when removing a subset of modules after `adf_ctl` up or `qat_service` start, the indices of the devices may be off.
Implication	Device references may not be sequential, and some devices may not be available for use.
Resolution	Restart `adf_ctl` or `qat_service` after removing any subset of Intel® QAT modules.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.69 QATE-29972 - Gen - Compilation with Intel C Complier (ICC) not supported

Title	Gen - Compilation with Intel C Compiler (ICC) not supported.
Reference #	QATE-29972
Description	When compiling the software package with the Intel® Compiler (ICC), the compilation will fail.
Implication	Build with the ICC compiler was not supported before the v4.4.0 release.
Resolution	This is resolved with the v4.4.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.70 QATE-29974 - GEN - Compilation on RHEL v6.9 may not be supported

Title	GEN - Compilation on RHEL v6.9 may not be supported.
Reference #	QATE-29974
Description	When compiling the software package on RHEL v6.9 with `kernel 2.6.32-696.18.7.el6.x86_64`, the compilation might fail.
Implication	Build on RHEL v6.9 may not be supported by this release.
Resolution	This has been confirmed to be a test issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.71 QATE-30340 - GEN - Kernel panic during device power-off

Title	GEN - Kernel panic during device power-off.
Reference #	QATE-30340
Description	It is not possible to remove a Intel® QAT device driver with `rmmod` if there is a user space process using the device (attached to the driver). There is a reference counter preventing this from happening. However, If, for any reason, the kernel driver of an Intel® QAT device is removed while a user space process is running, the Kernel will crash. The user-space library will send IOCTL to the Kernel space driver that will not be dealt with because the Kernel driver is no longer available. This issue has been observed during a change of power mode state.
Implication	`Dmesg` will report a Kernel Oops. The user application may report a `segfault`, and a reboot is required.
Resolution	This is resolved with the v4.3.0 release
Affected OS	Linux
Driver/Module	ADF - Kernel Mode

3.2.72 QATE-30720 - GEN - Library, and driver do not support devices enumerated in a PCI domain different than 0

Title	GEN - Library and driver do not support devices enumerated in a PCI domain different than 0.
Reference #	QATE-30720
Description	The user space driver and the Intel® QAT library cannot handle devices enumerated in a domain different than 0.
Implication	It is not possible to use the software in systems where the device is enumerated with a PCI domain different than 0.
Resolution	This is resolved with the v4.4.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.73 QATE-30758 - USDM - Suspected vulnerability in-memory driver

Title	USDM - Suspected vulnerability in-memory driver.
Reference #	QATE-30758
Description	The memory driver included in the software package can enable privilege escalation.
Implication	An unprivileged user process may be able to gain root privileges with a specialized kernel memory allocation attack.
Resolution	This is resolved with the v4.3.0 release.
Affected OS	Linux
Driver/Module	CPM IA - USDM

3.2.74 QATE-30785 - SYM - Request cookie not released in case of error

Title	SYM - Request cookie not released in case of error.
Reference #	QATE-30785
Description	If an error is encountered while processing a symmetric crypto request, the request cookie is not freed back to the cookie pool.
Resolution	This is resolved with the v4.3.0 release
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.75 QATE-30882 - GEN – Intel® API in kernel space not validated on 32bit OSes

Title	GEN - Intel® API in kernel space not validated on 32bit OSes.
Reference #	QATE-30882
Description	The Intel® QAT API in kernel space is not validated on 32 bit OSes.
Implication	When running the `cpa` sample code in kernel space on 32 bit systems, the test might report errors while allocating memory.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.76 QATE-31201 - DC - Payloads compressed using DH895XCC may not be marked as complete

Title	DC - Payloads compressed using DH895XCC may not be marked as complete.
Reference #	QATE-31201
Description	Sporadically, while compressing data with static or dynamic stateless compression, `BFINAL` might not be set.
Implication	The deflate stream produced might not be complete. A decompress operation might flag an error while trying to decompress it.
Resolution	This is resolved with the v4.4.0 release.
Affected OS	Linux
Driver/Module	CPM FW - Data Compression

3.2.77 QATE-31295 - GEN - Internal Intel® QAT Memory can be exposed

Title	GEN - Internal Intel® QAT Memory can be exposed.
Reference #	QATE-31295
Description	While performing penetration tests on Intel® QAT, the ability to read internal device memory was observed. This required root access on the platform. Processes running in virtual functions are not able to exploit this vulnerability.
Implication	Internal data structures may be visible to unauthorized users.
Resolution	This is resolved with the v4.4.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.78 QATE-31714 - SRIOV: VF driver incorrectly exposes some debugs entries

Title	SRIOV: VF driver incorrectly exposes some debugs entries.
Reference #	QATE-31714
Description	The VF driver incorrectly exposes through debugs the following entries: heartbeat, version, `fw_counters, cnv_errors`.
Implication	The system may crash if any of those entries are read.
Resolution	This is resolved with the v4.4.0 release. Debugs entries have been removed from the VF drivers.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.79 QATE-31792 - GEN - Cleanup sequence might fail if the process using Intel® QAT is traced

Title	GEN - Cleanup sequence might fail if the process using Intel® QAT is traced.
Reference #	QATE-31792
Description	If a process using Intel® QAT is traced (e.g., via `cat/proc/<pid>/smaps`) while it gets killed, the cleanup sequence might fail to report in the system log a message similar to the following in Intel® QAT: Bundle `0`, rings `0x0001` already reserved.
Implication	The cleanup sequence might not be executed, and the Intel® QAT driver might leak instances.
Resolution	This is resolved with the v4.5.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.80 QATE-31800 - DC: Stateful decompression may not succeed

Title	DC: Stateful decompression may not succeed.
Reference #	QATE-31800
Description	When performing stateful decompression, intermediate requests with odd-length payloads under 2048 bytes are not handled correctly. This mishandling may occasionally cause the operation to fail.
Implication	To decompress the stream, the application increases the size of the output buffer to a value greater than 2048.
Resolution	This is resolved with the v4.4.0 release.
Affected OS	Linux
Driver/Module	CPM IA - FW

3.2.81 QATE-32022 - SYM - AES-XTS: parameter check does not report an error if the request is smaller than the size of the block

Title	SYM - AES-XTS: parameter check does not report an error if the request is smaller than the size of the block.
Reference #	QATE-32022
Description	Currently the Intel® QAT library reports an invalid parameter error when `pOpData->messageLenToCipherInBytes < ICP_QAT_HW_AES_BLK_SZ and packetType == CPA_CY_SYM_PACKET_TYPE_LAST_PARTIAL but not for packetType == CPA_CY_SYM_PACKET_TYPE_FULL.`
Implication	An `AES-XTS` request of type `CPA_CY_SYM_PACKET_TYPE_FULL` smaller than 16 bytes, might report an incorrect output.
Resolution	This is resolved with the v4.5.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.82 QATE-32044 - GEN - Polling banks APIs in kernel space are not supported

Title	GEN - Polling banks APIs in kernel space are not supported.
Reference #	QATE-32044
Description	The polling APIs `icp_sal_pollBank` and `icp_sal_pollAllBanks` are not supported by the Intel® QAT API in kernel space.
Implication	An application using `icp_sal_pollBank` and `icp_sal_pollAllBanks` APIs in kernel space might incur in a deadlock.
Resolution	This has been confirmed to be a test issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.83 QATE-32322 - GEN - Interrupt coalescing not supported

Title	GEN - Interrupt coalescing not supported.
Reference #	QATE-32322
Description	Setting `InterruptCoalescingEnabled` or `InterruptCoalescingTimerNs` in the `config` file does not have any effect.
Implication	Interrupt coalescing is not supported in this release.
Resolution	This is resolved with the v4.5.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.84 QATE-32336 - GEN: Incorrect Frequency Calculation

Title	GEN: Incorrect Frequency Calculation.
Reference #	QATE-32336
Description	In C3538, C3558, C3758, C3308, C3508, C3708, the device frequency might be miscalculated, and the driver might report in the system logs a message similar to this: `c3xxx 0000:01:00.0`: Slow clock 320000000 MHz measured, assuming 533000000.
Implication	Some frequency-dependent features such as heartbeat, Interrupt coalescing, or completion timeout might not behave as expected.
Resolution	This is resolved with the v4.4.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.85 QATE-32373 - GEN - Error observed when multiple processes die or are killed

Title	GEN - Error observed when multiple processes die or are killed
Reference #	QATE-32373
Description	When multiple processes die or are killed, the end-user can observe an error message in the kernel log.
Implication	The following error is observed: Intel® QAT: failed to receive response message in 5000
Resolution	This is resolved with the v4.6.0 release.
Affected OS	Linux
Driver/Module	CPM IA

3.2.86 QATE-32621 - GEN - qat_service not enabled by default in SUSE Linux*

Title	GEN - qat_service not enabled by default in SUSE Linux*.
Reference #	QATE-32621
Description	The `qat_service` script is not enabled by default in some versions of SUSE Linux after the installation finishes.
Implication	After a restart, the Intel® QAT driver might not be loaded with the correct configuration.
Resolution	Please refer to Frequently Asked Questions at the end of this document.
Affected OS	SUSE Linux
Driver/Module	CPM IA - Common

3.2.87 QATE-33137 - USDM - virt2phy fails on allocated huge pages

Title	USDM - virt2phy fails on allocated huge pages.
Reference #	QATE-33137
Description	When using huge pages allocated from the USDM memory driver, an error similar to the following is reported: `hugepage_alloc_slab:226 virt2phy` on huge page memory allocation failed.
Implication	In systems with a kernel version greater than or equal to v4.0, an unprivileged user cannot use huge pages allocated by the memory driver (USDM).
Resolution	Do not use huge pages. Ask your Intel representative for more information.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.88 QATE-33450 - GEN - Hang of asymmetric crypto engines might not be detected by heartbeat

Title	GEN - Hang of asymmetric crypto engines might not be detected by heartbeat.
Reference #	QATE-33450
Description	Heartbeat might not detect a hang of an asymmetric crypto engine.
Implication	The device might be reported as responsive even if one of the engines is hung.
Resolution	None.
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.89 QATE-37406 - GEN - Hash + Compression chaining performance sample code might hang

Title	GEN - Hash + Compression chaining performance sample code might hang.
Reference #	QATE-37406
Description	When using different types of devices with one type supporting hash + compression chaining and one not, the `cpa_sample_code` application hangs.
Implication	The hash + compression chaining performance sample code does not run to completion.
Resolution	When testing hash + compression chaining, bring down unsupported devices first.
Affected OS	Linux

3.2.90 QATE-37450 - CY - Memory corruption in GCM and CCM in case of failure

Title	CY - Memory corruption in GCM and CCM in case of failure.
Reference #	QATE-37450
Description	When a GCM or CCM requests fail the internal callback when cleaning sensitive data, it might write into a wrong address. This failure is more likely if the destination buffer is composed of multiple flat buffers, and the cipher offset is different than 0.
Implication	When a GCM or CCM request fails, the behavior of the application using the software package is indeterminate. The most likely behavior is a segmentation fault.
Resolution	This is resolved with the v4.5.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.91 QATE-37470 – SR-IOV VF driver is not reporting RESTARTING event to the application

Title	SR-IOV VF driver is not reporting RESTARTING event to the application
Reference #	QATE-37470
Description	SR-IOV VF driver is not reporting the RESTARTING event to the application. When the device hangs 'Restarting' event is posted to all VF's through PF-VF message communication. Once the VF driver receives restarting message with message type 'ADF_PF2VF_MSGTYPE_RESTARTING', the VF driver should notify the 'ADF_EVENT_RESTARTING' event to registered application. There is a bug in the current driver wherein the VF driver receives 'ADF_PF2VF_MSGTYPE_RESTARTING' message from PF, but it doesn't notify the event to the application.
Implication	An application may not be able to quiesce correctly, and requests and responses may be lost.
Resolution	This is resolved with the v4.6.0 release
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.92 QATE-38014 - CY - Destination buffer is overrun in a Digest Verify + Decrypt that does not reserve output space for the digest

Title	CY - Destination buffer is overrun in a Digest Verify + Decrypt that does not reserve output space for the digest
Reference #	QATE-38014
Description	It has been noticed when the field verifyDigest in CpaCySymSessionSetupData is set to CPA_TRUE; the digest is written back to the destination buffer even if there is not allocated space in the destination buffer for it.
Implication	Unallocated memory may be overwritten
Resolution	This is resolved with the v4.6.0 release
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.93 QATE-38075 - CY - Initialization vector is not returned when using skcipher API

Title	CY - Initialization vector is not returned when using skcipher API
Reference #	QATE-38075
Description	When doing encryption or decryption of a buffer, the `skcipher` API expects the IV to be returned to the user. The Intel® QAT implementation is not returning it.
Implication	IV is not returned to the user
Resolution	This issue is resolved with v4.8.0 release
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.94 QATE-38078 - GEN - APIs called with CPA_INSTANCE_HANDLE_SINGLE may fail

Title	GEN - APIs called with CPA_INSTANCE_HANDLE_SINGLE may fail
Reference #	QATE-38078

Description	APIs called with `CPA_INSTANCE_HANDLE_SINGLE` may fail to get the first instance handle when only `sym/asym` services are enabled. The following APIs are included:
	`cpaCyStopInstance`
	`cpaCyInstanceGetInfo`
	`cpaCyInstanceGetInfo2`
	`cpaCyQueryCapabilities`
	`cpaCySetAddressTranslation`
	`icp_sal_CyPollInstance`
	`cpaCyStartInstance`
	`cpaCySymQueryCapabilities`

Implication	Crypto instances and, therefore, APIs won't work when called `CPA_INSTANCE_HANDLE_SINGLE`.
Resolution	Use the multiple instance discovery functions.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.95 QATE-38119 - DC - Extended use of dynamic compression may result in Intel® QAT HW reporting watchdog timeout

Title	DC - Extended use of dynamic compression may result in Intel® QAT HW reporting watchdog timeout
Reference #	QATE-38119
Description	An oversight in the handling of dynamic compression requests has the potential to induce watchdog timeout events. The conditions necessary to trigger this scenario generally only arise when the device has been in continual operation for several days, at which point a minimal failure rate will come into effect.
Implication	Affected requests return `CPA_DC_WDOG_TIMER_ERR` and require resubmission by the application.
Resolution	This issue is resolved with the v4.6.0 release.
Affected OS	Linux
Driver/Module	CPM FW

3.2.96 QATE-39082 - GEN - Access to /dev/qat_adf_ctl allows a limited-trust user to reconfigure or reset the Intel® QAT Endpoint

Title	GEN - Access to /dev/qat_adf_ctl allows a limited-trust user to reconfigure or reset the Intel® QAT Endpoint.
Reference #	QATE-39082
Description	The device `/dev/qat_adf_ctl` provides several ioctls. Some ioctls are used by regular users of Intel® QAT for ring reservation and querying the configuration values. Others are used to reconfigure or reset the device. With the current implementation, any user that can use Intel® QAT for crypto or compression service can also reconfigure, bring down, or reset the device. These admin capabilities should be limited to admin users.
Implication	A user with access to `/dev/qat_adf_ctl` can reconfigure, bring down, or reset the device.
Resolution	This is resolved with the v4.6.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.97 QATE-39129 - GEN – Intel® QAT driver may report uncorrectable error messages after a power-cycle reboot or a hard reset

Title	GEN - Intel® QAT driver may report uncorrectable error messages after a power-cycle reboot or a hard reset
Reference #	QATE-39129
Description	The Intel® QAT driver may report uncorrectable error messages after a power-cycle reboot on some platforms during the driver load but not on subsequent reloads of the driver. This error message has been seen on Broadwell-based platforms.
Implication	There is no known functional impact, provided that subsequent reloads of the driver are done.
Resolution	Restart the device using `adf_ctl` or `qat_service`.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.98 QATE-39220 - GEN - Intel® QAT API submissions with bad addresses that trigger DMA to invalid or unmapped addresses can cause a platform hang

Title	GEN - Intel® QAT API submissions with bad addresses that trigger DMA to invalid or unmapped addresses can cause a platform hang
Reference #	QATE-39220
Description	This version of the Intel® QAT hardware does not perform request checking. It follows that a malicious application can submit requests that can bring down an entire Intel® QAT endpoint, which can impact other Intel® QAT jobs associated with the hardware. Furthermore, if any Intel® QAT API submission has bad addresses that would trigger DMA to invalid or unmapped addresses, these can induce a platform hang. This presents a risk to be managed by the host and guest operating systems and other system policies. The exposure can extend to other guest operating systems or applications outside of the typical access boundary of the malicious guest or application.
Implication	All guest operating systems or other applications using Intel® QAT must be trusted, and/or other steps must be taken to ensure that an untrusted application or guest cannot submit incorrectly formatted requests.
Resolution	There is no workaround available. However, system policies (including limiting specific operating system permissions) can help to mitigate this issue.
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.99 QATE-40952 - CY - Kernel > 5.0 LKCF self-test errors

Title	CY - Kernel > 5.0 LKCF self-test errors.
Reference #	QATE-40952
Description	`LKCF` tests are failing when the Intel® QAT driver is loaded. For some algorithms output results are different from the expected, for others the destination buffer overflow is detected
Implication	`LKCF` for the kernel >v5.0 is not fully supported.
Resolution	This is resolved with v4.8.0 release
Affected OS	Linux.

3.2.100 QATE-41556 - CY - Input data is copied from source buffer to destination buffer when doing an everyday hash operation

Title	CY - Input data is copied from source buffer to destination buffer when doing an everyday hash operation
Reference #	QATE-41556
Description	When performing an everyday hash operation, where the digest result (`pDigestResult`) is placed in a buffer unrelated to the source buffer, the input data from the source buffer gets copied to the destination buffer as part of the operation.
Implication	Additional PCIe cycles consumed for the transfer of the input data from the source buffer to the destination buffer.
Resolution	Future fix
Affected OS	Linux
Driver/Module	CPM IA - Crypto

3.2.101 QATE-42157 - CY - System reboot may be triggered with nginx* restart when huge pages are used (ADDED)

Title	CY - System reboot may be triggered with nginx* restart when huge pages are used.
Reference #	QATE-42157
Description	When Nginx* is restarted using the command: kill -hup [`nginx PID`] and the memory driver is configured to use huge pages with more than 16 huge pages per process defined, a system reboot may be triggered.
Resolution	This is resolved with the v4.7.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Crypto
Reference #	QATE-41556

3.2.102 QATE-45527 - GEN - Device utilization and rate limiting is exposed for all Intel® QAT services is available to users regardless of the individual service being enabled

Title	GEN - Device utilization and rate limiting is exposed for all Intel® QAT services is available to users regardless of the individual service being enabled
Reference #	QATE-45527
Description	There are no checks to verify given service is enabled for device utilization and rate limiting. As such requests to create Service Level Agreements or query device utilization for services are allowed even if the corresponding service was not enabled.
Implication	Device utilization and rate limiting requests for services not enabled are allowed. These requests should gracefully fail.
Resolution	This is resolved with the v4.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Common
Reference #	QATE-41556

3.2.103 QATE-50854 - CY - Incorrect cipher sizes passed via the Linux Crypto API may disrupt Intel® QAT crypto services

Title	CY - Incorrect cipher sizes passed via the Linux Crypto API may disrupt Intel® QAT crypto services.
Reference #	QATE-50854
Description	For Intel® QAT crypto operations exposed via the Linux Crypto API, the Intel® QAT driver may not be checking that the cipher sizes are correct.
Implication	Current crypto operations may be disrupted. For DH895X devices, the device may need to be reset.
Resolution	This is resolved with v4.8.0 release
Affected OS	Linux.

3.2.104 QATE-51157 - GEN - Makefile sets unsafe file permissions for some non-Intel® QAT files

Title	GEN - Makefile sets unsafe file permissions for some non- Intel® QAT files.
Reference #	QATE-51157
Description	The Makefile incorrectly reduces file permissions on some non-QAT files within the QAT user group.
Implication	This could allow unauthorized access to devices, and it could prevent some system services from working correctly.
Resolution	This is resolved in the v4.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - GEN

3.2.105 QATE-52111 - DC - Incorrectly formatted payload during decompression job can hang the Intel® QAT Endpoint

Title	DC - Incorrectly formatted payload during decompression job can hang the Intel® QAT Endpoint.
Reference #	QATE-52111
Description	Specific files that are not correctly formatted compressed files can hang the Intel® QAT Endpoint when decompression is attempted on these.
Implication	The Intel® QAT Endpoint can hang.
Resolution	This is fixed with the v4.8.0 release.
Affected OS	Linux
Driver/Module	CPM IA - Compression

3.2.106 QATE-58487 - DC - Compressed data fails to decompress

Title	DC - Compressed data fails to decompress.
Reference #	QATE-58487
Description	If the Compress and Verify feature is explicitly disabled (which is not a supported configuration) when performing a compression operation with Intel® QAT , with specific input data of greater than 64KB, the compressed data cannot be decompressed.
Implication	An error may be encountered during the decompression of the compressed data.
Resolution	This is resolved with Intel® QAT Software Release v4.8.0. Compression operations with input data greater than 64 kB will no longer be supported if the Compress and Verify feature is explicitly disabled.
Affected OS	Linux
Driver/Module	CPM HW – Data Compression

3.2.107 QATE-51676 - Gen - PF/VF comms can increase attack surface

Title	Gen - PF/VF comms can increase attack surface
Reference #	QATE-51676
Description	`adf_pfvf_crc` can read extra data, including one or more relevant function pointers.
Implication	Combined with one or more other exploits, this can improve an attack against Kernel Address Space Randomization.
Resolution	This issue is fixed in v4.9.0
Affected OS	Linux
Driver/Module	CPM IA - Common

3.2.108 QATE-52049 - CY - Input to Intel® QAT algorithms registered to Linux Crypto API has limited parameter checking

Title	GEN - Makefile sets unsafe file permissions for some non- Intel® QAT files.
Reference #	QATE-52049
Description	The Intel® QAT software and firmware stack does not validate all inputs. As such, typically Intel® QAT services are only provided to privileged accounts on a system, where the account has explicitly been provided access. Intel® QAT also registers algorithms with the Linux Crypto API, which can be used by unprivileged accounts. It follows that unprivileged users can inadvertently or intentionally provide invalid parameters to the Intel® QAT API, resulting in an impact to Intel® QAT service availability for other users, or other undefined platform behavior.
Implication	Intel® QAT services may not be available without restarting the QAT service or rebooting the system.
Resolution	As of the v4.8 release, the software will no longer register with the Linux Crypto API by default. In addition, parameter checks have been added to validate input.
Affected OS	Linux.

§

4.0 Frequently Asked Questions

4.1 I have an application called XYZ with the intent to use two cryptography instances from each of the two chipset (PCH) devices in the system (a total of four instances). What would the configuration files look like?

In this case, the `NumberCyInstances` parameter should be set to **2** in the configuration file for each PCH device.

4.2 Should the Cy<n>Name parameter use unique values for <n> in each configuration file?

The `Cy<n>Name` parameter can be used in different configuration files without issue. In addition, the same `Cy<n>Name` name can be used in different domains within the same configuration file. The same rules apply to the `Dc<n>Name` parameter.

4.3 The firmware does not load. How can I fix this?

If the firmware does not load, verify that `udev` is available and running. On older systems (such as CentOS v6.5), verify that the kernel was built with `CONFIG_FW_LOADER=y`. On more recent systems (such as CentOS v7), `udev` is part of `systemd`, and it is installed by default as part of the `systemd-udevd` service.

4.4 When I try to start the driver, I see errors (including kernel messages) that appear to be related to memory allocation. What can I do to avoid this?

When many instances are declared in the configuration file, it is possible to see these errors. The errors can typically be avoided by using the recommendations found in the "Reducing Asymmetric Service Memory Usage" section of the *Intel® QuickAssist Technology Performance Optimization Guide*, by reducing the `NumConcurrentSymRequests` parameters in the configuration file, or by reducing the number of instances declared in the configuration file (see the "*Acceleration Driver Configuration File*" chapter in the chipset Programmer's Guide). Refer to Table 4 for a copy of these guides.

Another approach is to modify Linux* such that the value in `/proc/sys/vm/max_map_count` is increased (for example, to double the value). That value can be increased by modifying `/etc/sysctl.conf` to include the following line:

```
vm.max_map_count = <large_number_here>
```

Then reboot, and run cat `/proc/sys/vm/max_map_count` to verify that the value has been increased.

4.5 When trying to start the Intel® QuickAssist Technology driver, I see errors similar to one or more of the following:

- Failed to send admin msg to accelerator `dh895xcc 0000:b1:00.0`: Failed to send init message
- Error -14 with the "make install" dh895xcc: probe of 0000:b1:00.0 failed with error -14

Note: The above may be seen in `/var/log.messages.`

- Fewer qat acceleration devices than you expect when starting Intel® QAT .

Note: For example, you may see all the c6xx type devices but not the dh895x device.

On systems that support PCIe* ECRC (PCIe transaction layer end-to-end CRC checking), the root cause may be that ECRC is enabled in BIOS for the PCIe root ports. A proper fix will be for the BIOS to avoid enabling ECRC when devices are present that do not support ECRC or to disable ECRC by default in BIOS.

If a BIOS update is not practical, or for a temporary workaround, the following instructions may work:

1. On a fresh boot, before insertion of the Intel® QAT kernel module software and before the driver is brought up, enter the command:

   ```
   # setpci -s <bb:dd.f> 160.w=0
   ```

   where <`bb:dd.f`> are the values for the root port that your Intel® QAT device(s) is behind.

   You can find these values by entering the lspci command. The root port data could appear as follows:

   ```
   00:03.2 PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
   v4/Xeon D PCI Express Root Port 3 (rev 01)
   ```

2. After entering the setpci command, you can insert the Intel® QAT modules and bring up the driver.

4.6 When loading the package modules, I see kernel log warnings related to the signing of the modules. What do I need to do?

If certain kernel configuration flags are set (as some background, see CONFIG_MODULE_SIG and CONFIG_MODULE_SIG_ALL), these messages may be returned. To avoid these warnings, consult the documentation for the applicable kernel configuration flags.

4.7 Why does Intel® QAT performance drop around buffer/packet sizes of 2kB?

Depending on the specifics of the particular algorithm and Intel® QAT API parameters, a relatively small decrease in performance may be observed for submission requests around a buffer/packet size of 2 kB to 4 kB. This decrease is expected due to optimizations in the Intel® QAT software that can apply for requests of a specific size.

4.8 I am receiving failures or hangs when sending perform requests to the Intel® QAT API after a fresh boot or after hotplug events. How can these be resolved?

For the proper initialization, adf_ctl must be brought down and then back up (execute adf_ctl down followed by adf_ctl up) after a fresh boot. Various errors or hangs can occur if this is not done. qat_service, if used, handles this. For hotplug, events, remove the Intel® QAT modules and reinsert them before executing adf_ctl down and adf_ctl up.

4.9 How do I get the Intel® QAT driver to automatically start in SUSE Linux?

Run “systemd-sysv-install enable qat_service” to enable the Intel® QAT driver to start in SUSE Linux automatically.

§