



Release Notes - VMware*

Intel® QuickAssist Technology Hardware Version 1.X

February 2023

Performance varies by use, configuration and other factors. Learn more on the Intel's [Performance Index site](#).

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

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

Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

See Intel's [Legal Notices and Disclaimers](#).

© Intel Corporation. Intel, the Intel logo, Atom, Xeon, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Contents

1	Description of Release	1
1.1	Features	1
1.2	Feature Addition and Enhancements	2
1.3	Limitations	2
1.4	Package Information	3
1.5	List of Files in Release	3
1.6	Supported Guest Drivers	3
1.7	Technical Support	4
1.8	Environmental Assumptions	4
1.9	Related Documentation	5
2	Release Updates	6
2.1	Known Issues	6
2.1.1	Issues Relating to Violation of Trust Model	6
2.1.2	QATE-7495 - An Incorrectly formatted requests to Intel® QAT can render the Intel® QAT endpoint unresponsive	7
2.1.3	QATE-30251 - Turning off Bus Master Enable may cause PF hang	8
2.1.4	QATE-64395 - Usage of DC Session Update API can render the application unresponsive	8
2.1.5	VQQ-122 – Intel® QAT HW doesn't support "Number of VFs" SR-IOV configuration	9
2.1.6	Intel® QAT HW (c6xx and 200xx QAT) doesn't support VF reset functionality	9
2.1.7	Intel® QAT HW requires masking some errors in AER register due to HW limitations	9
2.1.8	VMware ESXi may require to manually toggle passthrough for Intel® QAT VFs	10
2.1.9	VQQ-1604 - HKDF is not currently supported by some Intel® QAT HW (c6xx and 200xx QAT)	10
2.2	Resolved Issues	11
2.2.1	VQQ-1553 Incompatibility between legacy 1.7 and 2.0 drivers	11
3	Revision History	12

1 Description of Release

This document contains information on the accompanying Intel® QuickAssist Technology (Intel® QAT) Hardware Version 1.X Driver for VMware ESXi*.

This software enables single root I/O virtualization (SR-IOV) for the Intel QAT driver on VMware ESXi*. SR-IOV enables the creation of Virtual Functions (VF) from a single Intel QAT device to support acceleration for multiple virtual machines.

There are 2 components available for this release - one with **7.0.0** in name for VMware ESXi 7.0 and with **8.0.0** for VMware ESXi 8.0. Right package should be chosen based on the version of VMware ESXi installed on the target host. Hence installation commands from **README.txt** may require adjustments and pointing to a particular device component with compatible version.

For instructions on loading and running the release software, refer to the **README.txt** file in the released software package. For instructions on how to install the driver in the Guest Operating System (OS) refer to corresponding guest driver's collaterals listed in the [Related Documentation](#) section.

Refer to the [Revision History](#) to check the changes of this document.

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

1.1 Features

- Sym/Asym Crypto.
- Data Compression.

1.2 Feature Addition and Enhancements

Feature	Description
New HW support	Support for QAT on next platforms is added: <ul style="list-style-type: none">▪ Intel® Atom® P5300 processor product family (c4xxx QAT)▪ Intel® Atom® P5700 processor product family (c4xxx QAT)▪ Intel® Atom® C5000 processor product family (200xx QAT)▪ Intel® Xeon® D2700 processor product family (c4xxx QAT)▪ Intel® Xeon® D1700 processor product family (200xx QAT)
Service configuration	User can change default service configuration per QAT endpoint
Support for VMware ESXi 8.0	Package for VMware ESXi 8.0 is added to the package

1.3 Limitations

- HKDF is not currently supported on all devices.
- Intel® Key Protection Technology (KPT) is not supported.
- Ratelimiting is not supported.
- Due to HW limitations, only all (maximum number) VFs could be enabled, arbitrary number of VFs is not supported.
- The Intel® QAT device should not be exposed (via SR-IOV) to untrusted guests.
- ESXi limitation: number of PCI passthrough devices per VM is limited, so please check this [KB article](#) for exact limits. ESXi will not allow to power on VM if such limit is exceeded.

1.4 Package Information

Package Name	qat-l.x_ext_rel_bin_1.5.0.47.tar.gz
Release Date	02/13/2023
Supported Hardware	<ul style="list-style-type: none"> ▪ Intel® C62x Chipset (c6xx QAT) ▪ Intel® QuickAssist Adapter 8960/8970 (c6xx QAT) ▪ Intel® Atom® P5300 processor product family (c4xxx QAT) ▪ Intel® Atom® P5700 processor product family (c4xxx QAT) ▪ Intel® Atom® C5000 processor product family (200xx QAT) ▪ Intel® Xeon® D2700 processor product family (c4xxx QAT) ▪ Intel® Xeon® D1700 processor product family (200xx QAT)
Supported ESXi Version(s)	VMware ESXi 7.0 and 8.0
Driver Version	1.5.0.47
Package Checksum	SHA256: 47ad7615b9b44b2ec786547d10d8fea928dc411fec2fed405af757fd-fce3alaa

1.5 List of Files in Release

File	Description
icp-qat-pf-drv_1.5.0.47-10EM.700.1.0.15843807_21250985.zip	Driver component for 7.0
icp-qat-pf-drv_1.5.0.47-10EM.800.1.0.20613240_21262822.zip	Driver component for 8.0
LICENSE.txt	License information
README.txt	Basic driver installation and configuration information

1.6 Supported Guest Drivers

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

- **Linux*:** Intel QAT driver QAT.L.4.19.0-*
- **Windows*:** Intel QAT driver QAT1.7.w.1.8.0-*

Actual list of supported guest OS depends on the guest driver compatibility. Refer to the corresponding documentation for more information.

1.7 Technical Support

Intel offers support for this software at the API level only, defined in the Programmer's Guide and API reference manuals listed in the [Related Documentation](#) section.

For technical support, including answers to questions not addressed in this document, visit the technical support forum, FAQs, and other support information at [Intel Support](#).

VMware forwards all issues they suspect to be related to Intel QAT to Intel to help triage and resolve with the customer directly.

1.8 Environmental Assumptions

The following assumptions are made about the deployment environment:

- The driver object/executable file on disk should be protected using the normal file protection mechanisms, so it is writable by only 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 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 (SRIOV)) to untrusted guests.
- The Intel QAT device should not be exposed (through the *user space direct* deployment model) to untrusted users.
- The Dynamic Random-Access Memory (DRAM) is considered to be inside the trust boundary. The traditional memory-protection schemes provided by the Intel architecture processor and memory controller, and by the OS, is to prevent unauthorized access to these memory regions.
- Persistent keys were not considered, but the storage media are also 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.

1.9 Related Documentation

Title	Number
Intel QuickAssist Technology for Linux* - Getting Started Guide (HW 1.7)	336212
Intel QuickAssist Technology for Linux* - Release Notes (HW 1.7)	336211
Intel QuickAssist Technology for VMware* - Release Notes (HW 1.X)	768798
Intel QuickAssist Technology - Programmer's Guide (HW 1.7)	336210
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

2 Release Updates

2.1 Known Issues

2.1.1 Issues Relating to Violation of Trust Model

The second generation of Intel® QAT was designed with performance as the primary objective. To attain the best possible performance, applications are exposed directly to the hardware with no bounds checking. This approach implies a trusted programming model, wherein an application is expected to supply correctly formatted addresses and arguments at the Application Programming Interface (API).

An application failing to follow the programming conventions runs the risk of negatively impacting the platform.

2.1.2 QATE-7495 - An Incorrectly formatted requests to Intel® QAT can render the Intel® QAT endpoint unresponsive

Title	An Incorrectly formatted request to Intel® QAT can render the Intel® QAT endpoint unresponsive
Reference	QATE-7495
Description	<p>This version of the Intel® QAT hardware does not perform exhaustive request address and parameter checking. It follows that a malicious application could submit requests that can bring down an entire Intel® QAT endpoint or platform itself, which can impact other Intel® QAT jobs associated with the hardware. This presents a risk that must 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.</p> <p>Conditions like invalid address, address range that crosses the SecureRAM boundaries, and invalid request can cause HW to hang or system reset.</p>
Implication	All guest operating systems and applications using 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.
Related issues	<p>QATE-14706 - Partial descriptor submission may cause hang</p> <p>QATE-14287 - IOMMU page fault provokes device hang</p> <p>QATE-15430 - Malformed NULL descriptor may cause hang</p> <p>QATE-30895 - Crossing SecureRAM boundaries may cause device hang</p> <p>QATE-39377 - Continuous submitting malformed requests in VM may cause the platform to hang or reboot</p> <p>Root Cause Analysis:</p> <p>When a non-posted transaction is initiated to an invalid target (bad memory address), a UR is returned. Later, a Completion Time Out happens. A tag is issued to the non-posted transaction, and a tag is returned by the UR and a tag is returned by the CTO. This means that for every one tag issued, two are returned. This causes unexpected overflows in counters, too many outstanding transactions, and eventually leads to system instability and a crash.</p>

2.1.3 QATE-30251 - Turning off Bus Master Enable may cause PF hang

Title	Turning off Bus Master Enable may cause PF hang
Reference	QATE-30251
Description	Specific guest's operations to rings with disabled BME bit may cause PF to hang.
Implication	-
Resolution	If PF hangs, the system administrator should shut down all the VMs and manually reload the driver or restart the whole system.

2.1.4 QATE-64395 - Usage of DC Session Update API can render the application unresponsive

Title	Usage of DC Session Update API can render the application unresponsive
Reference	QATE-64395
Description	In case of using Linux driver 4.10 with DC Session Update API user may get a time-out and fatal errors in Guest OS dmesg: <code>c6xxvf 0000:ff:00.0: Fatal error received from PF 0x6ac20013</code>
Implication	The application which is using the mentioned API may get a timeout-related error or stuck on waiting for a response from HW
Resolution	Use smaller chunks for submission or increase timeout values in the application that is using Intel® QAT. Also, possible to increase a Heartbeat and Quiesce timeouts for PF driver itself via the next steps: <ol style="list-style-type: none"> 1. Power off all VMs that is using Intel® QAT hardware 2. Unload driver: <pre>> esxcfg-module -u icp_qat_pf</pre> 3. Load driver module via next command where hb_interval is ranged from 500 to 5000 ms and quiesce_timeout is from 350 to 20000 ms: <pre>> esxcli system module parameters set -m icp_qat_pf -p "hb_ ↪ interval=5000 quiesce_timeout=20000"</pre> 4. Reset device manager: <pre>> kill -HUP \$(cat /var/run/vmware/vmkdevmgr.pid)</pre> <p>To reset <code>hb_interval</code> and <code>quiesce_timeout</code>, just repeat all steps omitting setting time values on step 3</p>

2.1.5 VQQ-122 – Intel® QAT HW doesn't support "Number of VFs" SR-IOV configuration

Title	Intel® QAT HW doesn't support "Number of VFs" SR-IOV configuration
Reference	VQQ-122
Description	If the system administrator configures the number of VFs less than the total number of VFs supported by PF, the driver will fail to attach the device.
Implication	The system administrator can't configure the VF number less than the total VFs.
Resolution	Enable all VFs per endpoint. If previously smaller number was configured and no VFs are available, reconfigure SR-IOV with maximum number of VFs.

2.1.6 Intel® QAT HW (c6xx and 200xx QAT) doesn't support VF reset functionality

Title	Intel® QAT HW (c6xx and 200xx QAT) doesn't support VF reset functionality
Reference	-
Description	The Intel® QAT HW (c6xx and 200xx QAT) doesn't implement the SR-IOV specification section, which requires VFs to support Function Level Reset (FLR)
Implication	-
Resolution	ESXi PF SR-IOV driver emulates VFRLR for HW which doesn't support it.

2.1.7 Intel® QAT HW requires masking some errors in AER register due to HW limitations

Title	Intel® QAT HW requires masking some errors in AER register due to HW limitations
Reference	-
Description	QAT HW does not process Completion Timeout, Unsupported Request, and Uncorrectable Internal Errors correctly, and the associated bits should be masked in the AER mask register to prevent NMI failures which may lead to platform crash.
Implication	-
Resolution	ESXi PF SR-IOV driver masking appropriate errors to mitigate platform crashes.

2.1.8 VMware ESXi may require to manually toggle passthrough for Intel® QAT VFs

Title	VMware ESXi may require to manually toggle passthrough for Intel® QAT VFs
Reference	
Description	Due to limitations in VMware ESXi 7.0 Intel® QAT VFs could be not marked for passthrough and require to enable passthrough for VFs in vSphere UI manually.
Implication	System administrator need to manually toggle passthrough for VFs before assigning to VMs
Resolution	Update to 7.0 Update 1 or newer release of ESXi or follow next instruction to toggle passthrough manually: <ol style="list-style-type: none">1. Connect to the target ESXi host via Web User Interface (UI)2. In the left pane, click on Manage.3. Choose Hardware tab.4. Using checkboxes select Intel® Co-processor devices that have Disabled passthrough state.5. Click on Toggle passthrough button to enable passthrough for disabled devices.

2.1.9 VQQ-1604 - HKDF is not currently supported by some Intel® QAT HW (c6xx and 200xx QAT)

Title	HKDF is not currently supported by some Intel® QAT HW (c6xx and 200xx QAT)
Reference	VQQ-1604
Description	Intel® QAT driver for VMware ESXi is using DEFAULT <code>ServicesProfile</code> and doesn't allow user to change it. Hence some of the device capabilities like HKDF support could be not available on c6xx and 200xx QAT HW.
Implication	HKDF is not currently supported.
Resolution	No workaround is available.

2.2 Resolved Issues

2.2.1 VQQ-1553 Incompatibility between legacy 1.7 and 2.0 drivers

Title	Incompatibility between legacy 1.X and 2.0 drivers
Reference	VQQ-1553
Description	1.7 driver (version 1.1.0.7) couldn't be installed on the same system with 2.0 driver. They are using same namespaces and will conflict, so one of the drivers will fail initialization.
Implication	Only one of the driver could be installed on the system.
Resolution	Use updated 1.X driver, starting from version 1.5.0.41 it's compatible with 2.0 driver.

3 Revision History

Version	Description	Date
2.0	For software release 1.5.0	February 2023
1.0	Initial Release	August 2020