



# Intel® QuickAssist Technology Software for FreeBSD\*

Package Version: QAT.B.3.0.5-00017.tar.gz  
Release Notes

---

November 2017  
**Intel Confidential**



You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein. No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

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

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.

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

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at <http://www.intel.com/> or from the OEM or retailer.

No computer system can be absolutely secure.

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

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

Copyright © 2017, Intel Corporation. . All rights reserved



## Release Overview

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.

For instructions on loading and running the release software, see the Getting Started Guide for your platform.

This software release is intended for platforms that contain:

- 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.

The QAT R3.0.5 FreeBSD package is provided as production quality release and is therefore intended to be used in a production environment only for the dh895xcc device.

The QAT R3.0.5 FreeBSD release is provided to enable the use of the QAT driver on FreeBSD 11.0

## Features/Limitations

The main features of the software package are:

- Cryptographic Services
- Data Compression Services
- Cryptographic Sample Applications
- Data Compression Sample Applications
- Intel® QuickAssist Technology Data Plane Cryptographic API (cpa\_cy\_sym\_dp.h)
- Intel® QuickAssist Technology Data Plane Data Compression API (cpa\_dc\_dp.h)
- SR-IOV functionality with FreeBSD 11.0 guest

The following features are not currently supported:

- Heartbeat
- Dynamic instances
- Dynamic compression
- SR-IOV functionality FBSD as a host
- Any other version on FBSD than 11.0

There are known issues with the production release of the driver as described in [Known Issues for Intel® Communications Chipset 8925 to 8955 Series](#)



## MD5 Checksum Information

The table below gives MD5 checksum information.

	<b>Package</b>	<b>Checksum</b>
QAT Package	QAT.B.3.0.5-00017.tar.gz	0fb3bd48bce7ea392258cb548fe5f77e

## Licensing for FBSD\* Acceleration Software

The acceleration software is provided under the following license as listed in the table below.

When using or redistributing dual-licensed components, you may do so under either license.

<b>Component</b>	<b>Licence</b>	<b>Directories</b>
User Space Library	BSD	./quickassist/build_system ./quickassist/include ./quickassist/lookaside ./quickassist/utilities/osal
Kernel space driver	Dual BSD/GPL v2	./quickassist/qat/drivers ./quickassist/utilities/adf_ctl
Compatibility layer for older kernel versions	GPL	./quickassist/qat/compat
User Space 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



# QuickAssist Driver Package Installation on FreeBSD Environment

## Environmental Assumptions

The following assumptions are made with regard to the deployment environment

- The driver object/executable file on 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 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 QAT device should not be exposed (via SR-IOV) to untrusted guests.
- The 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 normal 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 also considered inside the cryptographic boundary.

Users must have root privileges to perform the following.

### 1) Compiling the Driver

Step 1: Copy package onto the system

Step 2: Extract package.

```
# cd /root/  
# mkdir QAT  
# cd QAT  
# tar -xzf <path_to>/QAT.B.3.0.5-00017.tar.gz
```

Step 3: Set network proxy (if required) and install gmake.

```
# setenv http_proxy http://<proxy\_server>:<proxy\_port>
```

Step 4: Install build dependencies:

1. gmake:

```
# cd /usr/ports/devel/gmake  
# make config-recursive  
# make install
```
2. Boost

```
# pkg install boost-all
```
3. Automake & autoconf

```
# pkg install automake  
# pkg install autoconf
```
4. Bash

```
# pkg install bash
```
5. pkg-config

```
# cd /usr/ports/devel/pkgconf/  
# make  
# make install
```



Step 5: Setup the environment to build driver.

```
# /root/QAT/  
# ./configure
```

Step 6: Build and install driver

```
# gmake  
# gmake install
```

## 2) Compiling and execute performance sample code

Step 1: Build application

```
# cd /root/QAT/  
# gmake samples-install
```

Step 2: Run application

```
# cd ./build  
# ./cpa_sample_code signOfLife=1 <- sign of life tests  
# ./cpa_sample_code <- full application run
```

## 3) Uninstalling the driver

Step 1: Bring down the driver

```
# ./adf_ctl down
```

Step 2: Uninstall driver

```
# cd /root/QAT/  
# gmake uninstall
```

## 4) Driver Persistence

Step 1: in /etc/rc.conf

```
qat_enable="YES"
```



## Known Issues for Intel® Communications Chipset 8925 to 8955 Series

The known issue additions or updates since the last release of the software for the platform are listed below.

### Summary of Known Issues for Intel® Communications Chipset 8925 to 8955 Series

<b>QATE-5092</b>	CY: AES-XTS does not support buffers sizes that are not a multiple of 16B
<b>QATE-7325</b>	CY: AES-GCM operation with zero length plain text results in an incorrect tag result
<b>QATE-10019</b>	Gen: The mmapped CSR region in user space is not unmapped at the end
<b>QATE-10386</b>	Gen: cp_sal_reset command to a device influences behaviour of other devices

<b>Title</b>	<b>CY: AES-XTS does not support buffers sizes that are not a multiple of 16B</b>
<b>Reference #</b>	<b>QATE-5092</b>
<b>Description</b>	A single request with a data size that is not a multiple of 16B for AES-XTS will fail with an invalid param check.
<b>Implication</b>	The user cannot submit AES-XTS Crypto requests with buffers that are not multiples of 16B.
<b>Resolution</b>	No Workaround Available
<b>Affected OS</b>	FreeBSD 11.0
<b>Driver/Module</b>	CPM IA – Crypto

<b>Title</b>	<b>CY: AES-GCM operation with zero length plain text results in an incorrect tag result</b>
<b>Reference #</b>	<b>QATE-7325</b>
<b>Description</b>	Sending an AES-GCM operation with zero length plain text may generate an incorrect tag result
<b>Implication</b>	Potentially bad record errors and failing connections
<b>Resolution</b>	There is no workaround available
<b>Affected OS</b>	FreeBSD 11.0
<b>Driver/Module</b>	Feature - Acceleration Driver

<b>Title</b>	<b>Gen: The mmapped CSR region in user space is not unmapped at the end</b>
<b>Reference #</b>	<b>QATE-10019</b>
<b>Description</b>	If creating (or forking a process) and mapping rings into process, the process can crash. This happens mostly when high process creation / disposal rate is made.
<b>Implication</b>	The process can crash
<b>Resolution</b>	Do not create processes dynamically
<b>Affected OS</b>	FreeBSD 11.0
<b>Driver/Module</b>	Feature - Acceleration Driver



<b>Title</b>	<b>Gen: cp_sal_reset command to a device influences behaviour of other devices</b>
<b>Reference #</b>	<b>QATE-10386</b>
<b>Description</b>	A device can become unresponsive after reset on a system with more than one QAT device.
<b>Implication</b>	Device becomes unresponsive
<b>Resolution</b>	To prevent that this procedure has to be followed: 1. detach (exit) all the processes which use the device to reset 2. run adf_ctl down qatX where X is the number of the device 3. run adf_ctl up qatX where X is the number of the device 4. restart the processes detached in (1)
<b>Affected OS</b>	FreeBSD 11.0
<b>Driver/Module</b>	Feature - Acceleration Driver