Intel® Advanced Encryption Standard New Instructions (AES-NI) Ecosystem March 2013 Update

This document doesn't include all software products that support Intel® AES-NI. Please contact the software vendor directly for support information. The listed software versions indicate the initial Intel AES-NI support. The subsequent versions of the same software should support AES-NI as well.

Intel® AES-NI Usage Model	Application with Intel® AES-NI	**Status**
Secure Transactions (TLS/SSL)	Microsoft* Windows Server* 2008 R2	Available now
	OpenSSL* 1.0.1	Available now
	GnuTLS*	Available now
	CyaSSL* 1.5.4	Available now
	Red Hat Enterprise Linux* 6	Available now
	SUSE Linux Enterprise Linux* 11 SP1	Available now
	Solaris* 10	Available now
	Fedora* Linux 13	Available now
	Ubuntu* 11.10	Available now
	Intel® Expressway Service Gateway R3.4	Available now
	Intel® Expressway Tokenization Broker R3.4	Available now

Full Disk Encryption Software	Checkpoint* Endpoint Security R73 FDE 7.4 HFA1	Available now
	McAfee Endpoint Encryption* 6.0 with ePolicy Orchestrator* 4.5	Available now
	Microsoft BitLocker* WS2008R2	Available now
	Symantec* PGP Universal 10.1	Available now
	WinMagic* SecureDoc* 5.2	Available now
	Dell* Data Protection for windows system	Available now
	FileVault* Version 2 (Mac OS X Lion)	Available now
	TrueCrypt* 7.0	Available now
	Sophos* SafeGuard Easy 6.0/SafeGuard Device Encryption 6.0	Available now
Enterprise Applications	Oracle* Berkeley* DB 11.2.5.0.26	Available now
	Oracle* Database* 11.2.0.2	Available now
	IBM* InfoSphere* Guardium Data Encryption for DB2*	Available now
	IBM* WebSphere* Application Server	Available now
	IBM* J9 Java 7 SR3	Available now
	SAP* Netweaver*, HANA*, and Business ByDesign* (software as a service) products	Available now

	Red Hat* JBoss* Enterprise Application Platform (v5/v6)	Available now
	VMware* ESX 4.0 U1 (supports AES-NI usage in the guest OS)	Available now
	VMware* vSphere* 5.1 (supports AES-NI natively in IPSec)	Available now
	Microsoft* Hyper-V* Server 2012 (supports AES-NI usage in the guest OS)	Available now
	Citrix* XenServer 5.6 (supports AES-NI usage in the guest OS)	Available now
	Citrix* XenClient 1.0	Available now
	Oracle* VM 3.0 (supports AES-NI usage in the guest OS)	Available now
	Xen 4.0.1 (supports AES-NI usage in the guest OS)	Available now
	KVM* (supports AES-NI usage in guest OS)	Available now
	Hitachi* Virtualization Manager (HVM, also known as Virtage*) (supports AES-NI usage in the guest OS)	Available now
	InterSystems* Caché* 2012.2	Available now
	Vormetric* Encryption 5	Available now
	Intel® Distribution for Apache Hadoop* (IDH)	Available now
	Gazzang zNcrypt*	Available now

Tools **Libraries**	Intel® Complier, V11.0	Available now
	Microsoft* Visual Studio 2008 SP1	Available now
	GNU Compiler Collection, GCC v4.4.0	Available now
	Microsoft Crypto Next Generation*, CNG WS2008R2	Available now
	Intel® Integrated Performance Primitives crypto library V7.0	Available now
	Network Security Services, NSS 3.12.3	Available now
	OpenJDK* 1.6 (via NSS)	Available now
	Solaris* 10 Java Cryptographic Framework	Available now
	RSA* BSAFE Crypto Kernel	Available now
	SAP* SAPCryptoLib	Available now
	IBM* Global Security Kit (GSKit)	Available now
	IAIK-JCE version 5.0	Available now
	Linux Crypto API	Available now
	Crypto++* Library 5.6.1	Available now
	Libgcrypt* version 1.5.0	Available now
	Dm-crypt	Available now

	FreeBSD’s OpenCrypto API	Available now
	7-Zip* 9.1	Available now

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