

Alliance AES Encryption Cross-Platform FAQ



Finding A Common Approach to AES Encryption

Sensitive data travels between internal servers, external customers and suppliers, and over wireless networks. Incompatibilities between encryption technologies results in lost time, excessive cost, and a heightened risk of data loss.

Alliance AES encryption solutions work on all Enterprise application platforms in a common way and support all of the NIST AES encryption standards. This results in smooth implementations, better security, as well as reduced cost.

Maximizing Your Investment In IT Expertise

The modern Enterprise runs many server operating systems and hardware platforms. Applications are developed with a variety of programming languages. How can IT professionals reduce complexity and costs? One way is to deploy solutions that work the same way everywhere.



Platforms

MicrosoftWindows
XP/2000/2003/2008

IBM i i5/OS (AS/400, iSeries)

IBM z z/OS (Mainframe)

Red Hat Linux on Intel x86

Red Hat Linux on Intel x86_64

Red Hat Linux on POWER

SUSE Linux on Intel x86

SUSE Linux on Intel x86_64

SUSE Linux on POWER

IBM AIX

Sun Solaris

And more . . .

www.townsendsecurity.com

What Platforms Are Supported By Alliance AES Encryption?

Alliance AES encryption is in use on a wide variety of computing platforms, and the platform base is being extended as needed. Here are the current platforms supported by Alliance AES encryption:

IBM i (AS/400, iSeries)
IBM z z/OS (Mainframe)
Microsoft Windows 2000/XP/2003/2008 and SharePoint
SUSE Linux Enterprise 9, 10 Intel
SUSE Linux Enterprise 9, 10 64-bit POWER
Red Hat Enterprise 4, 5 on Intel
Red Hat Enterprise 4, 5 on 64-bit POWER
IBM AIX 5.3 and 6.1
Sun Solaris 8, 9 on 64-bit Sparc

The broad base of supported operating systems means that you can deploy safe and certified encryption solutions on all of your Enterprise server platforms. We also work with systems integrators and independent software vendors to provide support on other computing platforms.

How Will Alliance AES Encryption Solve Compatibility Problems?

Alliance provides a common set of encryption APIs on every supported platform. This means that your developers only need to learn one API and it will work the same way on all platforms. You can encrypt on Windows 2003, decrypt on IBM I, and encrypt again on Oracle database using the same AES encryption library.

The Alliance AES encryption APIs support all of the NIST approved key sizes and modes of encryption. This means that you don't have to worry about AES encryption incompatibilities as data moves between you and your customers and vendors. Alliance supports the following encryption key sizes:

- 128-bit
- 192-bit
- 256-bit

Alliance supports all of the NIST-approved modes of data encryption:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter (CTR)
- Output Feed Back (OFB)
- Cipher Feed Back (CFB)

Alliance AES Encryption stands alone in its support for all of the encryption key sizes, modes of encryption, and all of the Enterprise server platforms.

Programming Languages

Alliance encryption APIs are designed to work with the Microsoft .NET, VBNET, C#, C and C++ programming environments. In Microsoft environments the encryption support is provided through Dynamic Link Libraries (DLL). For Linux and UNIX development Alliance APIs will be a natural fit. Developers can use C, C++ or Java (through JNI or JNA) to use the encryption APIs. On Linux and UNIX the Alliance encryption support is provided in Shared Libraries. IBM I customers use RPG and Cobol to create applications. The IBM i support is provided through service programs.

Will Alliance AES Work With Our Oracle (IBM DB2, Microsoft SQL Server) Database?

Yes, Alliance AES customers are securing data in all major database systems using strong AES encryption. Encrypted data can be stored in binary format or in character string format. If you store encrypted data in binary format you may need to change the field characteristic to support BINARY data. Most database systems will attempt to do code-page conversion on non-binary character data, so converting the field type to BINARY will be necessary. If you convert the encrypted value to a Base64 or Base16 encoded value no change is needed to a character field type.

Can Alliance AES Encryption Be Used With Point-Of-Sale Systems?

Yes, Alliance encryption support has been incorporated into point-of-sale systems to provide data security on the terminal, and compatible encryption with central servers. We work with a POS vendor to assist in the use of encryption on the terminal and can generally handle even older POS operating systems. Once data is encrypted in transaction log files the data can be transmitted securely to a central server or payment processing server. Alliance customers have integrated DataVantage, Micros, SalePoint, and other POS solutions with Alliance AES encryption.

Our PDAs Use 128-bit AES For Encryption, Will Alliance AES Be Compatible?

Alliance AES Encryption solutions are certified by NIST to be compatible with the standard for AES. You can use Alliance AES encryption in PDA applications, and Alliance AES encryption can process encrypted data from any data security application that implements the standard.

Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.