

Alliance AES Encryption for IBM i

Data Sheet



What is Alliance AES Encryption for IBM i?

Alliance AES Encryption provides AES encryption for sensitive data everywhere it resides on your IBM i platform: Database files, tape, IFS files, Save Files, reports, and messages. With integrated key management you can secure data on your IBM i, Windows, Linux, and UNIX applications using a common, cross-platform strategy. You can encrypt with confidence using the only NIST certified solution for the IBM i.

About 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.



Reduces hardware and software costs and improve application run times with high performance encryption

Meet PCI, HIPAA, and Privacy Notification requirements for strong encryption

Build customer confidence with NIST-certified solutions

Reduce complexity with a cross-platform solution

Avoid field expansion and poorly performing shadow files

Reduce costs with an affordable solution

www.townsendsecurity.com

Encryption

- Advanced Encryption Standard (AES)
- NIST FIPS-197 compliant
- Key sizes: 128, 192, 256
- Modes: ECB, CBC, CTR, OFB, CFB1 to CFB128 (All five NIST modes)

Certiication & Validation

- NIST AES Validation
- NIST certification on IBM System i, IBM z, Windows, Linux, UNIXField encryption

Key Creation

- Pass phrase based encryption (PBE)
- Diffie-Hellman key generation
- RNG key generation
- Protegrity key import
- Split-role key generation

Key Management

- Uses NIST-certified Alliance AES Encryption for Windows

Query & Business Intelligence

- Integration with NGS-IQ for field-level secure BI support

Access Controls

- User access control for commands
- User access control for APIs
- User access control for keys
- PowerTech Authority Broker integration

API's

- High level AES APIs for RPG, Cobol, etc
- Low level AES APIs
- DB2 file encryption commands
- IFS file encryption commands
- Save File encryption commands
- Tape encryption commands
- Create self-decrypting archive command

Field Encryption

- Encrypt fields with AES CBC mode
- Encrypt fields with AES CTR mode (no requirement for field expansion)
- Encrypt fields with AES ECB mode
- Encrypt fields with AES OFB mode
- Encrypt bits with AES CFB1 to CFB128 mode
- Integrated with Alliance key manager
- Integrated with Alliance key server
- ASCII / EBCDIC data conversion
- Base64 and Base16 encoding
- Data masking
- Data masking with substitution
- SHA hash
- PKCS5 padding
- User access control
- Application program access control
- Field level access control

Utilities

- ASCII / EBCDIC data conversion
- Base64 and Base16 (hex) encoding
- Data masking
- Counter and IV generation
- Data hash
- PKCS5 padding
- Triple DES

Compliance Logging

- Selective decryption logging
- Selective encryption logging
- Compliance reports

Monitor & Alert

- System audit journal (QAUDJRN)
- SNMP trap messages
- SMTP email notification
- QSYSOPR message queue
- PowerTech integration

Whole File Encryption

- DB2 file encryption
- Flat file encryption
- IFS / QNTC / NFS file encryption
- Save file (SAVF) encryption

Data Masking

- Mask all but last 4 digits
- Mask credit card number
- Mask name
- Mask address, city, state, zip code
- Mask driver's license
- Mask date

Cross-Platform Support

- Alliance AES Encryption for Windows
- Alliance AES Encryption for Linux (SUSE, Red Hat)
- Alliance AES Encryption for UNIX (AIX, Solaris)
- Alliance AES encryption for zSeries
- Self-decrypting archives for Windows

Discovery & Assessment

- User library discovery
- User file discovery
- Database analysis for sensitive data
- Program analysis and cross-reference
- User-defined search criteria
- Assessment reports

System Requirements

- IBM iSeries OS/400 or i5/OS V5R1 or later

Support

- Software maintenance
- Technical support
- 24/7/365 support available
- On site installation available
- Contract services available

Contact Us

Townsend Security
www.townsendsecurity.com
800.357.1019
360.359.4400