

# Advantage™ Database Server Advantage Encryption

## PRODUCT DATASHEET

Advantage Database Server provides many features to protect and secure your data, perhaps none more important than encryption. Advantage data encryption allows your data to be completely protected, secure, and unreadable to unwanted access. There are many compelling reasons to encrypt your data including peace of mind, unauthorized access prevention, and compliance with data protection acts, laws, and certifications.

In today's business it is of critical importance to prevent unauthorized users from transmitting your confidential information to the wrong parties and from modifying and editing your information. Advantage's encryption functionality helps ensure both data protection and privacy.

### **ENCRYPTION BENEFITS**

#### **Peace of Mind**

Knowing your data is completely secure from attack, privacy breaches, or theft allows you to focus on your business, not worrying about prying eyes or potential attacks.

#### **Unauthorized Access Prevention**

Keeping your confidential data confidential is more important than ever in today's business. Encrypting data keeps it safe whether it is lost, stolen, or simply misplaced. This includes keeping data safe against deliberate attacks such as from a disgruntled employee or hacker. It also accounts for the accidental misplacement of data, for example, the safe decommissioning of data on a disk drive that can often times be recovered even after formatting when not encrypted.

#### **Data Protection Act and Certification Compliance**

Encryption is often times mandatory to be compliant with some industry certifications or laws designed to protect and ensure privacy of sensitive data. Applications with databases not meeting these minimum encryption security criteria are ineligible for deployment and therefore not a viable product in that industry.

### **ADVANTAGE ENCRYPTION**

Advantage provides security for your data in a number of important ways including the ability to encrypt stored and transmitted data.

For stored data, Advantage can physically encrypt data in tables to protect that data from unauthorized viewing. Advantage supports encryption of table and memo data in both DBF and ADT tables. Support also exists for encryption of ADT database table header information. The Advantage encryption scheme uses key data derived from a case-sensitive password to encrypt data using industry-standard algorithms.

Tables can be encrypted on a table-by-table basis. When a table is encrypted, all record data including memo and BLOB data is also encrypted. In addition:

- Index data can be encrypted when using data dictionary bound ADT tables.
- Table header data is encrypted when using data dictionary bound ADT tables.
- Data dictionaries, which include all database metadata, can be encrypted.

For transmitted data, Advantage supports encrypted communications for client/server communication across the network. By enabling encrypted communication, you ensure that all data is encrypted on your network, including queries, query results, record data, and all client/server interaction.

## ENCRYPTION OPTIONS

Advantage offers two encryption options.

- The default Advantage encryption engine incorporates a 160-bit, industry-standard RC4 encryption algorithm for servers and clients that ensure data is secure. This encryption functionality is included with all current versions of Advantage.
  - ADS 7.0 or greater - 160-bit RC4 encryption (including DBF memo and BLOB data)
  - ADS v6.0 or greater – 160-bit RC4 encryption (including ADT memo and BLOB data encryption)
- Advantage also offers an additional strong encryption alternative product called the *FIPS Encryption Security Option*. This option adds strong cryptographic functionality to both data storage and communication that can be used in Federal Information Processing Standard (FIPS) 140-2 compliant products. This add-on cryptographic functionality is available through libraries from the OpenSSL project and is not available by default with Advantage Database Server. It must be purchased separately with the FIPS Encryption Security Option add-on product.
  - Requires ADS v10.1 or greater
  - Requires client version 10.1 or greater
  - Transport Layer Security (TLS) v1.0 communications support over TCP/IP using RSA for the key exchange
  - SHA-1 (Secure Hash Algorithm) for message authentication
  - Cipher suites AES128-SHA and AES256-SHA
  - Cipher suite RC4-MD5, which uses RSA for the key exchange, RC4 for encryption and MD5 for message authentication, is also available. This cipher suite is not FIPS-compliant.
  - Advanced Encryption Standard (AES), 128-bit or 256-bit, for data (table) encryption

Note that enabling and using FIPS-compliant cryptography in Advantage Database Server does not make an application conform to FIPS 140-2; all parts of the application must be examined and possibly updated for FIPS-compliance.

## SPECIFICATIONS

### Server Operating Systems

RC4

- Microsoft Windows x86
- Microsoft Windows x84\_64
- Linux x86, x86\_64
- Netware

FIPS Encryption Security Option (AES)

- Microsoft Windows x86
- Microsoft Windows x84\_64
- Linux x86, x86\_64

### Database Server Support

- ADS v6.0 or greater – 160-bit RC4 encryption
- ADS v10.1 – FIPS Encryption Security Option (AES 128-bit or 256-bit)