Alliance AES/400 FieldProc
Frequently Asked Questions

FAQ INDEX

This document contains a collection of the answers to the most common questions people ask about Alliance AES/400 FieldProc.

Townsend SECURITY

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360 357 9047

Architecture & Capabilities

Q: Do I have to convert DDS files to SQL DDL in order to use FieldProc?

No, you do not have to convert DDS files to SQL in order to use FieldProc. There are some minor restrictions that you need to know. For example, you should not use the Change Physical File (CHGPF) command on DDS files that use FieldProc (See the IBM SQL reference guide for other restrictions). Most of our customers use FieldProc with DDS files.

Q: Do I need to know SQL to use Alliance AES/400 FieldProc?

No, Alliance AES/400 performs any needed SQL operations for you. There is no need to use SQL to configure or activate FieldProc, and no SQL knowledge is required.

Q: Does FieldProc work on internally described files?

No, the IBM DB2 FieldProc facility only works on externally described files created with DDS or with SQL.

Q: Can I encrypt multiple fields in a file?

Yes, Alliance AES/400 supports encrypting multiple fields (columns) in a single file.

Q: Do I have to use SQL for application access to FieldProc?

No, the IBM DB2 FieldProc implementation is compatible with both RPG (OPM and ILE versions) as well as with native SQL applications. You should be aware of some limitations when accessing a FieldProc encrypted file from RPG and COBOL applications. There are significant limitations with RPG access to encrypted indexes (key fields). See the section below about the Alliance AES/400 OAR/SQL module to help solve this limitation.

Q: Do I have to change field sizes or lengths with FieldProc?

No, the implementation of FieldProc will not require any changes to fields sizes or types in your IBM i DB2 database. Numeric fields will appear and function as expected in your RPG and COBOL applications.

Q: Do I have to change my RPG or COBOL applications to use FieldProc?

No, no program or file changes are required to use FieldProc. The DB2 FieldProc implementation is done at the database level and is transparent to your application.

Q: Do I have to recompile my RPG or COBOL applications to use FieldProc?

No, there is no requirement to recompile RPG applications or to change files.

Q: Can I encrypt numeric fields with FieldProc?

Yes, you can encrypt numeric fields with FieldProc. The encrypted numeric fields will be transparent to applications. That is, when an application writes the numeric value to the file the Alliance AES/400 FieldProc application will encrypt the column on insertion into a record (row). On decryption the numeric field is returned to your application in the proper format.

Q: Can I encrypt data, time, and timestamp fields?

Yes. You should be aware of some limitations around default values for date and time fields. But encryption of these types of fields is supported by FieldProc and by Alliance AES/400.

Q: Can I use SQL on files created with DDS?

Yes, you can use SQL operations on files that are created on DDS. The SQL syntax is the same as for files created with native SQL operations or with DDL. There are certain column attributes and operations that are not supported by DDS, but SQL will work as expected with DDS files. And you can use legacy RPG applications and modern SQL applications on these files.

Q: Can my data get corrupted by FieldProc?

The IBM FieldProc implementation will not corrupt data when used properly, and IBM places the FieldProc operations under commitment control. So, if an error is encountered when starting or ending FieldProc, the changes are rolled back for the entire file. You should be aware of the limitations of FieldProc with DDS files. For example, you should avoid the use of the Change Physical File (CHGPF) command with files under FieldProc control. As long as you are aware of the small number of limitations related to DDS files you will not experience issues with corrupted data.

Q: Can I encrypted key fields (index fields) with FieldProc?

Yes, the IBM FieldProc implementation supports the encryption of key fields (also known as SQL indexes). While encrypted indexes work very well with native SQL applications, there are limitations with legacy RPG applications that use encrypted key fields. It is common that RPG applications will have problems with sequence and range operations with encrypted indexes. You may find subfile displays and reports with missing or improperly ordered information. This is due to the use of legacy record-oriented key access in RPG applications. Alliance AES/400 provides an optional module that converts legacy RPG record-oriented I/O operations to native SQL operations through the Open Access for RPG (OAR) facility for RPG applications. Contact Townsend Security for more information about the OAR/SQL module.

Q: Are there any limitations for logical files?

Yes, join logical files created with DDS and which join on encrypted index fields generally will not work. The symptom will be that the attempt to start FieldProc will fail, or the attempt to create the DDS join logical file will fail. For normal DDS logical files (not join type) you can create the logical file over encrypted indexes. See the Alliance AES/400 documentation for the steps to do this. Native SQL join operations are not affected by this limitation.

Q: Are there any limitations on the size of files or the number of records?

No, Alliance AES/400 does not impose any file size constraints or constraints on the number of records in the file.

Q: Is data encrypted in journals?

Yes, when files that are under FieldProc control are also journalled, the data in the journal is encrypted. If the journal entries are applied to the file on another system (remote journaling) the data will remain encrypted in the target file.

Q: Does the product library need to be in the system or user library list (QSYSLIBL, QUSRLIBL) for FieldProc encryption?

No, the library ALLAES100 does not need to be in the system or user library list. Nor does the library need to be in a user library list. The FieldProc application itself will add the library as it is needed. Note that if you are using the OAR/SQL module the library OAR must be in the user's library list for any application that uses the OAR/SQL service program.

Q: What IBM or third-party licensed products are needed to run Alliance AES/400?

If you are using the Alliance Key Manager solution to protect encryption keys, you must install and configure the no-charge IBM licensed program Digital Certificate Manager. No other IBM or third-party application is required.

Q: How are software upgrades performed?

Townsend Security periodically makes new versions of Alliance AES/400 available to users. The installation process involves renaming the current library to a save name, restoring the new version, and then running an update program to copy configurations and license to the new version of the product library. The old version remains unchanged in order to support fallback operations.

Q: How do I transfer data to a Windows or Linux system?

When data is copied from a file that is under FieldProc encryption control the data is automatically decrypted by FieldProc. This is true when you read data from the file in RPG, or copy the file with an IBM copy command such as CPYF, and when you use FTP to transfer the file. If you need to transfer the data in encrypted format you must extract the file to a local library (QTEMP can be used to protect the data from attackers) and encrypted the data using one of the Alliance AES/400 encryption APIs for RPG. You can also copy data to an IFS directory and encrypt the entire file using the Alliance AES/400 IFS encryption command. The entire file will be encrypted with standard AES and can be decrypted on Windows or Linux.

Q: How do I transfer data to an outside vendor or service provider in encrypted format?

If the outside vendor uses an IBM i server you can encrypt a flat file with the Alliance AES/400 DB2 encryption command. That file can then be transferred to the outside vendor or service provider. If the outside service provider uses a Windows or Linux system you can transfer the information as described in the previous question above.

Q: How is Alliance AES/400 licensed?

Alliance AES/400 is licensed to an individual logical partition (LPAR), serial number, and processor group. A 30-day evaluation license is automatically installed when you access the installation menu option for a trial license. The evaluation license can be extended by Townsend Security by requesting an extension from your account manager.

Q: Can I install multiple copies of Alliance AES/400 in a logical partition?

AES/400 can be installed on a logical partition. You can install Alliance AES/400 in one independent auxiliary storage pool (iASP). However, only one copy of the product may be installed on any one logical partition. You can, however, use different encryption keys for databases and files in different iASP partitions.

User Access Controls

Q: How is user access implemented?

When you create a FieldProc definition in Alliance AES/400 you can specify that user access control be enabled. When access controls are enabled you then specify through the configuration menu (Option 4 to Work With User Control) to define the specific users with access to the column. This option also supports group profiles. Alliance AES/400 uses a whitelist approach to user access and does not use native object authority or user profile authority.

Q: Do you use native IBM i user authorities for FieldProc access control?

No, Alliance AES/400 uses a whitelist approach to providing access to FieldProc encrypted fields. It does not use object level authority or user profile authority for this purpose. This means that you can restrict highly authorized users such as QSECOFR and any user with All Object (*ALLOBJ) from access to FieldProc encrypted data.

Q: How is the FieldProc library secured?

The Alliance AES/400 library (ALLAES100) is secured by an authorization specific to this application. The library and all objects in the library are secured by the authorization list. The objects in the library are owned by a specific user profile named ALLAESOWN which has no ability to sign on to the IBM i server.

Q: Does the FieldProc application support group profiles?

Yes, when specifying user access controls and data masking options you can specify group profiles. Alliance AES/400 FieldProc also looks at the supplemental groups to resolve access authority.

Q: Does the FieldProc application support supplemental groups?

Yes, when specifying user access controls and data masking Alliance AES/400 will inspect user profile entries in a user's supplemental group.

Q: Can I protect encrypted data from QSECOFR and users with All Object (*ALLOBJ) authority?

Yes, Alliance AES/400 FieldProc uses a whitelist approach to access control. This means that you can exclude the QSECOFR and other highly privileged users from access to encrypted sensitive data. Alliance AES/400 does not use native object authority or user profile authority to determine access rights. This approach is in alignment with security best practices.

Q: Does Alliance AES/400 support two factor authentication?

Yes, when the Alliance Two Factor Authentication product is installed you can configure Alliance AES/400 to require 2FA authentication for all configuration options.

Encrypted Indexes

Q: Can you encrypt key fields (indexes) with FieldProc?

Yes, IBM's DB2 FieldProc implementation supports the encryption of key fields and SQL indexes. While native SQL applications which use the SQL Query Engine will work as expected, there can be severe limitations for RPG applications that use the legacy I/O operations such as CHAIN, READ, SETLL and so forth. See the description of the Townsend Security OAR/SQL module for information on how to handle the problems with encrypted indexes.

Q: Are there any limitations with encrypted indexes?

Yes, legacy RPG applications which use record-oriented operations such as CHAIN, READ, SETLL and other operations will NOT work as expected on encrypted key fields. This is because RPG applications do not use the SQL Query Engine for database operations. Instead, when RPG applications process FieldProc encrypted fields they convert the I/O request to the encrypted value and operate on the DB2 database using the encrypted value. This will cause empty subfile displays, invalid ordering of data, empty reports, and so forth.

This limitation can be overcome through the use of the Townsend Security OAR/SQL software which converts native RPG operations to SQL. The result is that RPG application logic will remain the same but the interface to the DB2 database will be through SQL. This resolves the problems with encrypted indexes in RPG.

Q: What is your Open Access for RPG (OAR) SQL module?

The Open Access for RPG SQL module from Townsend Security is software that converts legacy RPG file operations such as CHAIN, READ, SETLL, and so forth to native SQL operations using the Open Access for RPG file extension interface. It is used to solve the problem with encrypted indexes.

Q: How does the OAR/SQL interface work?

The Open Access for RPG interface is used to replace the native RPG file operations with your own code library. The Townsend Security OAR/SQL software provides a full mapping of RPG file operations to native SQL operations. This is accomplished through a file extension specification in the RPG application. When enabled, all input/output operations for a file are passed to the OAR/SQL module and it uses SQL to perform the operation. You have immediate conversion to the native SQL Query Engine for your RPG files.

Q: Do I have to change my RPG applications to work with OAR/SQL?

Yes, you must add one line of code that is an extension to the file ("F") specification in your RPG application. This file extension specification points to the OAR/SQL module. You must then recompile your program. This one-line code change is all that is needed for the file.

Q: Does the OAR/SQL module work with COBOL?

No, IBM has not implemented the Open Access for RPG technology in COBOL.

Audit Logging

Q: Are configuration changes recorded in an audit log?

Yes, all significant configuration changes to Alliance AES/400 are logged to the IBM security audit journal QAUDJRN.

Q: Can I audit the users who decrypt sensitive data?

Yes, you can specify that decryption events be audited to the IBM security audit journal QAUDJRN. You can specify this on a column-by-column basis.

Q: Are key management changes recorded in an audit log?

Yes, Alliance Key Manager records all key retrieval, encryption service, and encryption key management changes and events to an audit log. These audit log entries can be transferred to a log collection or SIEM server in real time.

Data Masking

Q: Does your product support data masking? How is this done?

Yes, you can mask decrypted sensitive data using masking rules defined in the FieldProc configuration panels and in the user control panel. This can be defined on a user-by-user basis and supports group profiles. You can also specify a default masking policy that can be used to force data masking for all users not authorized to see the decrypted version of the data. You can mask all of the data, all but the first 6 bytes of data, all but the last 4 bytes of data, and so forth. The masking rules meet PCI-DSS guidelines for data masking.

Q: Do I have to define data masking for every user?

No, you can define masking rules for users that are allowed to see all or part of the sensitive data and then define a default rule for all users not otherwise defined to the system. The default masking rule can be to mask the entire field. With this approach you only need to define users who are authorized to see all or part of the unencrypted data.

Q: Does data masking support group profiles?

Yes, data masking rules can be applied on a group profile basis.

Q: Can I use different data masking for different users?

Yes, you can specify the data masking for each user. You can set up some users to only see fully masked data, some users to see partially masked data, and some users who can see the fully unmasked data. You can do this for specific users and for group profiles.

Q: Can I set up different masking rules on different fields (columns)?

Yes, if you specify different encryption keys for the fields you can specify different masking rules for each user and field.

Q: Does your product support PCI-DSS requirements for masking of credit card numbers?

Yes, you can mask all of the field for users not authorized to view credit card numbers, all but the first 6 characters of the card number, and all but the last 4 characters of the card number.

Encryption Technology

Q: Is your encryption based on standards (AES)?

Yes, the AES encryption libraries used by Alliance AES/400 are validated to NIST AES standards. See certificate number 1340 here.

Q: Is your encryption compatible with other encryption libraries on Windows and Linux?

Yes, Alliance AES encryption is compatible with any other NIST-compliant implementation of the Advanced Encryption Standard (AES) or compliant version of Rijndael encryption. For example, you can use Windows .NET libraries to decrypt data encrypted by Alliance AES/400. The same is true for the OpenSSL encryption library on Linux and other platforms.

Q: What keysize do you use for AES encryption?

The FieldProc application uses 256-bit AES encryption. This is in line with recommendations by the US government for strong encryption including Quantum Computing based encryption.

IBM & Third-Party Utilities

Q: Can I use DFU (DBU, Query, FTP, etc.) on files that are encrypted with FieldProc?

Yes, any IBM or third party file utility or tool should be compatible with Alliance AES/400 FieldProc encryption. You can use DFU, DBU, DSPPFM and other commands to view and/or update data protected by Alliance AES/400 FieldProc encryption.

Q: What happens when I copy a file that has encrypted fields?

If you use the Copy File (CPYF) command and the data is encrypted in the source file, but not encrypted in the target file, the data will be decrypted as a part of the copy operation. The target file will be unencrypted while the source file remains encrypted. If you copy data from an unencrypted file to an encrypted target file the data will be encrypted. The Create Duplicate Object (CRTDUPOBJ) command will create an encrypted copy of the original file that has FieldProc controls enabled.

Q: What happens when I copy a file that is not encrypted to a file that is encrypted?

The FieldProc application will encrypt the data in the target file.

Business Continuity (Save, Restore, & High-Availability

Q: Do I use special commands to backup files protected with FieldProc?

No, you will use normal IBM save and restore commands to save files that are under Fieldproc control. The saved images of the data will remain encrypted. Use normal IBM restore commands to restore the data. Files protected with FieldProc can also be saved with the IBM BRMS application.

Q: Are there any special considerations for restoring files to a backup system?

Yes, the Alliance AES/400 application must be present on the backup system before restoring a file protected by FieldProc. Restore the ALLAES100 library with the FieldProc definitions before restoring the file that is protected.

If you use the Alliance Key Manager solution you must also configure Digital Certificate Manager with the appropriate CA certificate and signed client certificate to communicate with Alliance Key Manager.

Q: Can I restore a file under FieldProc control to a different library?

Yes, you can restore a file under FieldProc control to a different library. However, the column under FieldProc control will continue to reference the original FieldProc program and library. This means that the original library and file must exist in order for FieldProc to work. There is no method provided by IBM to change the FieldProc definition without stopping and restarting FieldProc encryption.

Q: Do I need a copy of Alliance AES/400 on a system where I restore a file?

Yes, if you want to be able to access the data in the file. You can easily restore a file without the presence of the Alliance AES/400 application. You will not receive an error if the Alliance AES/400 product is not installed on the system where the restore takes place. However, any attempt to view or process the data will result in a fatal error. Accessing the data will cause DB2 to attempt to encrypt or decrypt the data and the Alliance AES/400 FieldProc program will be called, if the Alliance AES/400 product is not installed this will result in a fatal error.

Q: Is my data encrypted on backup?

Yes, all normal IBM save commands will preserve the encrypted status of columns under FieldProc control.

Q: Is Alliance AES/400 compatible with MIMIX (Vision, iTerra, DataMirror, etc)?

Yes, Townsend Security customers use a variety of mirroring solutions for production files under FieldProc control and for the Alliance AES/400 library. See the Alliance AES/400 user reference manual for information about mirroring.

Is Alliance AES/400 compatible with independent auxiliary storage pool (iASP)?

Yes, you can install Alliance AES/400 in a single iASP on your IBM i server. It can then protect files with FieldProc encryption in the iASP as will as in the *SYSTEM base pool.

Key Management

Q: Do you provide local key management on the IBM i server?

Yes, you can define and use local keys with Alliance AES/400 FieldProc.

Q: Do you provide support for external key managers?

Yes, Alliance AES/400 supports our own FIPS 140-2 compliant key management solution Alliance Key Manager. We also support the SafeNet/Gemalto DataSecure key server through a partnership agreement. You can find more information about Alliance Key Manager here.

Q: Do you provide your key manager as a hardware security module (HSM)?

Yes, Alliance Key Manager is available as a network-attached hardware security module (HSM). This is a 1u rackmount server in a tamper evident case. The server is highly redundant with dual hot-swappable RAID disk drives, dual power supplies, redundant NICs and so forth.

Q: Do you provide your key manager as a VMware virtual machine?

Yes, Alliance Key Manager is available as a complete VMware software appliance ready to deploy in any VMware vSphere, ESXi and vCloud platform. Alliance Key Manager is validated for PCI compliance by Coalfire, a QSA certified PCI auditor. The Product Applicability Guide and statement of compliance can be downloaded here.

Q: Can the key manager be used with other systems (Windows, Linux, etc.)?

Yes, Alliance Key Manager supports a wide variety of operating systems and databases including Windows, Linux, IBM System z Mainframe, Microsoft SQL Server, MongoDB and many others. The same key server can be used with these platforms and with the IBM i server.

Q: Does your key management solution meet PCI-DSS and PA-DSS standards?

Yes, Alliance Key Manager has been validated by Coalfire, a qualified security assessor for PCI-DSS in VMware environments. The same key management software is used on the hardware security modules and in the cloud (Azure, AWS, vCloud). You can find and view the Product Applicability Guide and PCI validate here.

Q: Can I mirror the local key store to another system?

Yes, you can use any replication or data mirroring tool to mirror the Alliance AES/400 product to a high availability or backup system. A number of customers are using MIMIX, iTerra, Vision, DataMirror and other solutions with Alliance AES/400.

Q: Do you support data encryption key rollover (key change)?

Yes, you can use key rollover in both the local key store and with Alliance Key Manager. Encryption key rollover (key change) is managed by the Alliance AES/400 FieldProc application. Please see the Alliance AES/400 installation and user guide for information on how to perform key rollover.

Q: Do you support key encryption key rollover?

Yes, Alliance Key Manager support key encryption key (KEK) rollover as often as you wish. Normally you would perform KEK rollover once a year or once every two years, but you can establish the appropriate key rollover period for your environment.

Performance

Q: Will FieldProc affect performance?

Yes, any encryption solution for data at rest will impose some performance penalty. How large the impact is depends on many factors including:

- The performance of the AES encryption libraries.
- The performance of the FieldProc encryption program.
- The CPU and storage workloads of the IBM i server
- The mix of interactive and batch workloads of the IBM i server.
- And many other factors...

Alliance AES/400 minimizes the impact of AES encryption by using its own NIST-validated AES encryption libraries. These libraries are more than 100 times faster than comparable IBM AES encryption APIs on a typical Power6 or Power7 system. The libraries are more than 50 times faster than IBM libraries on Power8 systems. This provides a major advantage for customers who need optimal performance.

Additionally the Alliance AES/400 FieldProc programs are optimized for speed. The architecture of FieldProc involves the dynamic call to the FieldProc program for each column and row. This architecture accounts for more than 90% of the performance impact.

The only way to know the relative impact of FieldProc encryption on your application is to actually perform a proof-of-concept implementation on your system. Townsend Security provides its Alliance AES/400 FieldProc solution as a fully functional evaluation so that you can assess the performance impact in your environment. This is the only way to understand the actual performance impacts.

Q: How will encrypting multiple fields in a file affect performance?

Because of the optimization of the Alliance AES/400 FieldProc application the performance impact of encrypting multiple fields (columns) in a table is minimal. See the previous discussion of performance.

Q: Will FieldProc encryption affect backup and restore performance?

Yes, due to the fact that encrypted data cannot be compressed very well, your backups may take a bit longer and consume slightly more storage. For most IBM i customers this impact is not significant. If you encrypt very large fields your impact may be more significant.

Q: How fast are your encryption libraries?

Alliance AES/400 encryption libraries are optimized for speed on the IBM i platform. They are more than 100 times faster than native IBM i AES encryption libraries on Power6 and Power7 platforms, and more than 50 times faster on Power8 platforms with on-processor AES encryption capabilities. On a Power6/Power7 system rated at 3500 CPW Alliance AES/400 encrypts 1 million credit card numbers in 0.70 CPU seconds. On a Power8 system rated at 39,500 CPW Alliance AES/400 encrypts 1 million credit card numbers in 0.33 CPU seconds. There is no faster and more efficient encryption library for the IBM i server.

Compliance

Q: Is your AES encryption based on industry standards?

Yes, the Alliance AES/400 AES encryption libraries are validated to the NIST FIPS-197 standard for AES encryption. Townsend Security is the only IBM i security vendor with NIST validated AES encryption for FieldProc for the IBM i server platform.

Q: Is your key management based on industry standards such as NIST?

Yes, Alliance Key Manager is FIPS 140-2 Level 1 compliant (certificate 1449). Alliance Key Manager is also validated to the OASIS Key Management Interoperability Protocol (KMIP) for symmetric keys at version 1.0.

Q: Is your application PCI compliant?

Yes, Alliance Key Manager has been validated to the PCI-DSS standard by Coalfire, an approved QSA auditor, for the VMware platform. The same key management software runs in the hardware security modules (HSM) and in cloud platforms such as Amazon Web Services, Microsoft Azure, and IBM SoftLayer.

Discovery

Q: Are there tools in Alliance AES/400 to help me discover and locate sensitive data?

Yes, Alliance AES/400 provides database scanning software to help you locate credit card numbers. The scanning software can detect credit card numbers that meet LUHN check digit edits as well as all common Bank Information Number (BIN) prefixes for credit card numbers. You can scan a single file, all files in a library, or all user libraries.

Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, SOX, and other regulatory compliance requirements.

You can contact Townsend Security for an initial consultation at the following locations:

Web: www.townsendsecurity.com
Phone: (800) 357-1019 or (360) 359-4400
International: +1 360 359 4400
Email: info@townsendsecurity.com
Twitter: @townsendsecure