PROGRESS® OPENEDGE®

TRANSPARENT DATA ENCRYPTION (TDE)

INTRODUCTION

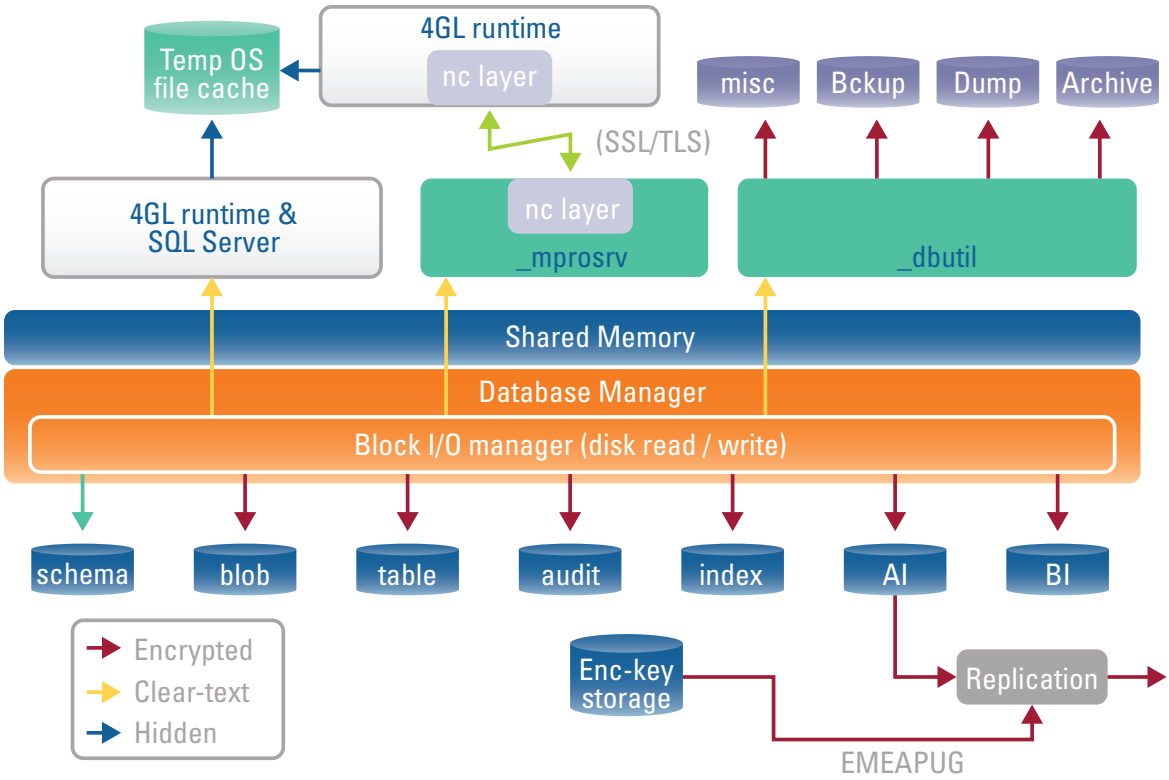
When valuable data is lost or stolen, there can be a serious business impact. As a result of past losses of this nature, now there are often requirements that sensitive financial or health-related data be encrypted while on disk. Loss or exposure of sensitive information can have significant impact on a company, including financial and legal penalties, as well as damage to its reputation.

Progress® OpenEdge® Transparent Data Encryption (TDE) is a new feature introduced in Progress® OpenEdge® 10.2B that protects your data when stored on disk.

Transparent Data Encryption operates with data-at-rest, i.e., data stored on disk. Other OpenEdge technologies have addressed network encryption and other requirements in the data lifecycle.

OPENEDGE TRANSPARENT DATA ENCRYPTION

OpenEdge TDE uses the most advanced encryption approach for database use. TDE uses standard encryption libraries and best-practice encryption key management to provide transparent encryption of information in your database.



TDE protects OpenEdge data at the table and index level, so you can protect one, some, or all tables—without needing to encrypt your entire database. Protection is set by the policies you define on-line, much as auditing levels are set today in OpenEdge. Just set your policy to encrypt the tables and indexes containing sensitive data.

With Transparent Data Encryption, data or index blocks written to disk are encrypted for safe storage, and data (or index) blocks read from disk are decrypted, for use by your application. Data written to backups and dumps (see note below) is also encrypted. As a result, operating system (OS) copies of the database, encrypted backups, and binary dumps will be protected.

Whether the data is from the database files themselves, a backup set or a binary dump, the basic operations are the same. Data "at rest" (written out) is encrypted*.

For your application, the important thing is that application data and indexes be unencrypted during access so the application runs as expected. An

Sometimes it is necessary to create binary dump files for routine database maintenance. For this reason, binary dumps for maintenance work are unencrypted by default.

important capability of the TDE approach is that indexes still work for finding data within a range. Other approaches encrypt the fields of individual keys in data records, so your application can only find records by an exact match against an encrypted value; selecting data by range does not work. Unlike the other approaches, TDE requires no application changes and all application features still work as before— hence, the term "transparent."

OPENEDGE TDE KEY MANAGEMENT

Key management is critical to successful operation of a production system that uses encryption. OpenEdge TDE includes both policy tools and a secure encryption key store. Encryption key storage is kept separate from the database and is protected by a strong passphrase to prevent unauthorized access, further ensuring the safety of your data.

You have the ability to run your production application with TDE and change encryption keys at the same time. Changeover to the new key will happen in the background until your encrypted storage tables and indexes are all upgraded. No downtime is required.

You can also change TDE policies while in production use. You can also add a new field to a table and then decide to have that table encrypted afterwards.

SUMMARY

OpenEdge Transparent Data Encryption services help you provide privacy for sensitive data in your application, whether your business is in retail (PCI-DSS requirements), financial services (PCI-DSS), healthcare (HIPAA requirements), or any other industry that handles sensitive data. These requirements together with the European Union Directive on Data Protection drive many software initiatives related to sensitive data. With use of this optional OpenEdge feature, your data will be protected on disk, in backups, and (optionally) even in binary dump files. Best of all, OpenEdge Transparent Data Encryption requires no changes to your application, user procedures, or DBA management processes. This means the costs to your production operation are truly minimized.

PROGRESS SOFTWARE

Progress Software Corporation (NASDAQ: PRGS) is a global software company that enables enterprises to be operationally responsive to changing conditions and customer interactions as they occur. Our goal is to enable our customers to capitalize on new opportunities, drive greater efficiencies, and reduce risk. Progress offers a comprehensive portfolio of best-in-class infrastructure software spanning event-driven visibility and real-time response, open integration, data access and integration, and application development and management—all supporting on-premises and SaaS/cloud deployments. Progress maximizes the benefits of operational responsiveness while minimizing IT complexity and total cost of ownership.

WORLDWIDE HEADQUARTERS

Progress Software Corporation, 14 Oak Park, Bedford, MA 01730 USA
Tel: +1 781 280-4000 Fax: +1 781 280-4095 On the Web at: www.progress.com

Find us on facebook.com/progresssw twitter.com/progresssw youtube.com/progresssw

For regional international office locations and contact information, please refer to the Web page below:
www.progress.com/worldwide

Rev. 5/11 | 6525-132563