

Acumatica Cloud ERP Encryption Overview

Date: August 27, 2025
Version: 1.7

Your Trusted Partner in Secure ERP Solutions

Acumatica
The Cloud ERP

CONTENTS

Executive Summary 3

Acumatica's Encryption Implementation 3

How Acumatica Supports Your Success with Encryption 3

Acumatica's Encryption Approach 4

- Encryption That Works for You 4

Encryption at a Glance 4

- Your Data, Your Control 4
- Tailored and Accurate Solutions 4
- Secure Data Management 4

Your Questions . . . Answered 5

- What Encryption Standards do Acumatica Cloud ERP use for Data Protection? 5
- How does Acumatica encrypt data at rest and in transit? 5
- Can I customize encryption for specific fields in my data? 5
- Does Acumatica support full database encryption? 5
- What is the performance impact of enabling encryption? 5
- How does Acumatica handle encryption key management? 5
- Who has access to the data? How is this access controlled and monitored? 5
- What security compliance certifications do you hold? 6
- Will Acumatica provide me with an SSL certificate, or can I use my own? 6
- What if I need to delete or anonymize encrypted data? 6
- Are backups encrypted, and how long are they retained? 6
- How often do you perform data backups? 6
- What are the advantages of the optional paid backup access service? 6

APPENDIX A 7

- Default Encrypted Fields in Acumatica in Acumatica Cloud ERP Database 7

Executive Summary

Welcome to Acumatica's Encryption Overview. We are committed to empowering your business with innovative ERP solutions that prioritize security, privacy, and efficiency through robust encryption practices. Our cloud-based ERP system leverages advanced encryption capabilities, including built-in tools and seamless connections to standard protocols and AWS infrastructure, to protect your operations.

This report highlights how Acumatica ensures your data is secure, with encryption using AES-256 at rest and TLS 1.2/1.3 in transit, GDPR compliance, and adherence to NIST SP 800- 53, NIST Cybersecurity Framework (CSF), and Center for Internet Security (CIS) standards. Your data is stored in dedicated database instances, and our internal systems are hosted on AWS. Importantly, with a robust roadmap for encryption enhancements in data-at-rest, data-in-transit, and integrations, we're ready to support your business goals. Key features include customizable encryption configurations and user-controlled data processing, ensuring you stay in charge of your information.

Explore how Acumatica can transform your business while keeping security first through effective encryption.

Acumatica's Encryption Implementation

At Acumatica, we understand that your business needs powerful, secure, and flexible ERP tools to stay competitive. Our ERP platform leverages encryption to streamline processes, boost decision-making, and drive growth. This customer-facing report outlines how we implement encryption, how we protect your data, and what you can expect from our ongoing innovations in security.

This updated report includes clear, concise answers to your questions about our encryption implementation in an FAQ format, with a focus on data security, including encryption and dedicated storage in our trusted AWS environments. Whether you're exploring encryption practices for the first time or looking to customize configurations, were here to support you every step of the way.

How Acumatica Supports Your Success with Encryption

- **Get Started with Confidence:** Explore how Acumatica leverages encryption to enhance your operations. Test our customizable integrations to see how they fit your business.
- **Stay Secure:** Use our opt-out options for external services and schedule regular compliance reviews to align with your policies.
- **Look Ahead:** Utilize encryption enhancements in 2025 R2, which offer even more ways to tailor encryption to your needs. Contact our team for detailed specs on data storage and encryption.
- **Partner with Us:** Reach out to our support team for personalized guidance on implementing encryption in our ERP solutions.

Acumatica is your partner in secure, innovative ERP, ready to power your business forward with advanced encryption.

Acumatica's Encryption Approach

Encryption That Works for You

Acumatica's encryption implementation is designed with your business in mind. Whether you're using our built-in encryption tools or connecting to protocols like TLS, we make integration easy and effective.

Encryption at a Glance

Layer	Standard	Scope	Status
At Rest	AES-256	All sensitive fields (SSN, CC, bank) + extensible	**Default & automatic**
In Transit	TLS 1.3 (default)	All web, API, mobile traffic	**Enforced globally**
Backups	AES-256	Full database & file backups	**Encrypted & geo-redundant**
Full DB (TDE)	SQL Server TDE	Optional	**Private Cloud only**

Performance Impact: <5% (Acumatica benchmark)

Your Data, Your Control

Acumatica prioritizes customer's data security with encryption compliance, and GDPR adherence. Data processed by Acumatica Cloud ERP is securely stored in dedicated database instances and our internal storage on AWS, trusted platforms for enterprise- grade security.Customers decide when and how personal data is processed, with opt-out options for external services.

Tailored and Accurate Solutions

With encryption tools (minimum viable product preview available in 2025 R2), you can customize encryption configurations to fit your unique needs, from analytics to reporting. Acumatica's encryption results are validated through your business rules, ensuring reliability and giving you the option to review outputs before use. See APPENDIX A for more information.

Secure Data Management

Customers control their data lifecycle, from storage to deletion. Acumatica's systems use dedicated database instances and AWS for secure encryption processing, with temporary storage that's deleted after use. Anonymization and encryption further protect customers' sensitive information, giving customers peace of mind.

Some details, like specific encryption configurations, may require further discussion with Acumatica's Partners and/or Support team to ensure we meet your exact needs.

Acumatica
The Cloud ERP

Your Questions . . . Answered

Below, Acumatica addresses some common questions about how Acumatica leverages encryption, providing answers to help customers understand how Acumatica works for them.

What Encryption Standards do Acumatica Cloud ERP use for Data Protection?

Acumatica employs AES-256 for data at rest (the same standard used by banks and the U.S. military) and TLS 1.3 (with TLS 1.2 fallback) for data in transit. This ensures end-to-end security without requiring additional setup, protecting sensitive information like credit card numbers and SSNs by default.

How does Acumatica encrypt data at rest and in transit?

Acumatica ensures security with encryption at rest (AES-256 or equivalent), compliance, and secure user access management. Customer data is protected by the same strict standards as our SaaS environment, with opt-out options for services that temporarily send data externally.

Can I customize encryption for specific fields in my data?

Yes, encryption is applied by default to sensitive fields (e.g., SSNs, credit cards), but customers can extend it to additional text fields via the Encryption Management workspace (introduced in 2024 R1). This point-and-click configuration respects role-based access controls and adds minimal overhead.

Does Acumatica support full database encryption?

Full database encryption via SQL Server's Transparent Data Encryption (TDE) is supported but recommended only for Private Cloud Subscription (PCS) deployments, where you manage your infrastructure. It's not supported in SaaS environments to avoid performance impacts.

What is the performance impact of enabling encryption?

Selective field-level encryption has less than 5% overhead on average, per Acumatica benchmarks, making it efficient for daily operations. We recommend this over full-database methods to prevent query slowdowns, ensuring your ERP remains fast and responsive.

How does Acumatica handle encryption key management?

Selective Keys are managed securely by default in SaaS environments, with automatic rotation during major releases. Customers are not able to maintain keys for SaaS Hosted environments however, in on-prem model (PCS), customers can use a CMK solution for full control ensuring the customer’s ability to oversee key lifecycle without relying on Acumatica.

Who has access to the data? How is this access controlled and monitored?

Under Acumatica’s shared responsibility model, customers control who accesses their data within their Acumatica Cloud ERP instance by managing user permissions and input data. Acumatica processes only authorized data, secured by robust measures and processed through business logic before being displayed or saved. Acumatica ensures secure hosting and backups but does not access customer data beyond platform operation and security needs (Telemetry), as outlined in Acumatica’s Data Processing Addendum.

What security compliance certifications do you hold?

SOC 1 Type II and SOC 2 Type II.

Will Acumatica provide me with an SSL certificate, or can I use my own?

Acumatica will always provide an Acumatica URL that is protected by SSL standards. However, Acumatica also recommends that you use your own certificate if you would like to have your own custom URL.

What if I need to delete or anonymize encrypted data?

You maintain full control over data deletion through your policies, aligning with GDPR's right-to-be-forgotten. Sensitive data can be anonymized for added privacy, and nothing persists on user devices after sessions end. Contact your Acumatica partner for guidance on custom anonymization.

Are backups encrypted, and how long are they retained?

Yes, all backups are encrypted with AES-256 and stored in S3 storage. We perform daily backups. This provides robust protection while meeting compliance needs.

How often do you perform data backups?

Reference https://www.acumatica.com/faq/.

Please reference Section Automated Backups and Database Snapshots.

What are the advantages of the optional paid backup access service?

The optional paid backup access service provides you with anytime access to 10 days of rolling backups. This allows you to download and store a copy of your data using SFTP. Standard fees apply if you need to restore or roll back your production environment. Subscribers to this service get this benefit in addition to all standard backup procedures.

If these don't cover a specific concern, customers can refer to the full FAQ at acumatica.com/FAQ.

Acumatica
The Cloud ERP

APPENDIX A

Default Encrypted Fields in Acumatica in Acumatica Cloud ERP Database

In Acumatica Cloud ERP, sensitive data is encrypted at rest in the SQL Server database using AES-256 encryption by default. This selective field-level encryption is handled through the application's data access layer (using attributes like PXRSACryptStringAttribute in the framework) and applies automatically to specific sensitive fields without requiring manual configuration. The encryption protects against unauthorized direct database access, such as in the event of a stolen backup.

Acumatica encrypts the following categories of fields by default. Note that exact database column names can vary slightly by version, but they correspond to these logical fields in key tables. Acumatica does not publish an exhaustive public schema for security reasons, but these are the consistently referenced defaults:

Category	Example Fields/Tables	Description/Purpose
Credit Card Information	CardNumber, CCID (e.g., in PMCard, PMSetup, or ARSalesCreditCard tables)	Full credit card numbers and tokenized IDs for payment processing (e.g., Authorize.net integration). Encrypted to comply with PCI DSS.
Social Security Numbers (SSN)	TaxRegistrationID (e.g., in Vendor, Customer, or EPEmployee tables)	Employee or vendor tax IDs; often used for payroll and compliance reporting.
User Passwords	Password (e.g., in Users table)	Hashed and encrypted user credentials for authentication.
Email/SMS Account Credentials	EmailUsername, EmailPassword, SMSAccountID, SMSAccountKey (e.g., in SMEmailSetup or SMSSetup tables)	SMTP/IMAP credentials for email notifications and SMS gateways.
Payroll/Salary Details (USA/CAN)	PayRate, Salary (e.g., in EPEmployee or PPDTimeActivity tables)	Employee compensation data to protect privacy.

Key Notes

- **Selective Encryption:** Only text-based sensitive fields are targeted to minimize performance overhead. You can extend encryption to additional fields via customizations (e.g., replacing PXDBString with PXRSACryptStringAttribute in DACs).
- **Decryption Behavior:** Fields decrypt automatically in the UI and API responses for authorized users, but remain encrypted in exports, Generic Inquiries (GI), or direct SQL queries for security.
- **Certificates:** Encryption relies on RSA digital certificates (purchased from a certification authority) configured in the system settings.
- **Cloud-Specific:** In Acumatica Cloud (hosted on AWS), all data is encrypted at rest and in transit. Private cloud or on-premises setups may require additional SQL Server Transparent Data Encryption (TDE) for full-database coverage, though this isn't default or officially tested.

GDPR-Relevant Category (Art. 4/9)	Example Fields/Tables	Description/GDPR Purpose
Identification & Tax Data (Personal identifiers, e.g., SSN/EIN)	TaxRegistrationID, SSN (e.g., in Customer, Vendor, EPEmployee tables)	Encrypts tax IDs for customers, vendors, and employees; protects against re-identification in breaches (Art. 5(1)(c) minimization). Supports right to erasure (Art. 17) via retention policies.
Financial/Payment Data (Economic identifiers, e.g., card details)	CardNumber, CCID (e.g., in PMCard, ARSalesCreditCard tables)	Tokenized credit card info for payments; ensures PCI DSS alignment within GDPR (Art. 32(1)(a) pseudonymization). Prevents unauthorized processing in transit/at rest.
Employment & Compensation Data (Employee special categories if health/sensitive)	PayRate, Salary, BirthDate (e.g., in EPEmployee, PPDTimeActivity tables)	Employee payroll and demographic details; safeguards privacy in HR processing (Art. 88 employment data). Audit trails log changes for accountability (Art. 5(2)).
Authentication Credentials (User access data)	Password (hashed/encrypted in Users table)	User login credentials; enforces secure authentication (Art. 32(1)(b)) to prevent unauthorized personal data access.
Communication Credentials (Account data for notifications)	EmailPassword, SMSAccountKey (e.g., in SMEmailSetup, SMSSetup tables)	SMTP/SMS credentials; protects against interception in automated communications involving personal data (e.g., consent emails, Art. 7).

Key GDPR-Centric Notes

- **Risk-Based Protection:** Encryption targets high-risk personal data to mitigate breach notifications (Art. 33/34). All data is also encrypted in transit (TLS 1.2+) and backed up securely.
- **Customization for Compliance:** Extend encryption to additional personal data fields (e.g., via custom DACs) using RSA certificates from certified authorities. This supports data protection impact assessments (Art. 35).
- **Broader Controls:** Role-based access (RBAC), multi-factor authentication (MFA), and 24/7 monitoring complement encryption. Consent management and right-to-be-forgotten tools handle processing restrictions.
- **Cloud Enhancements:** Hosted on AWS with EU data centers; no personal data stored client-side. Acumatica acts as a processor under GDPR-approved DPAs.

Acumatica
The Cloud ERP

Acumatica Cloud ERP is a comprehensive business management solution that was born in the cloud and built for more connected, collaborative ways of working. Designed explicitly to enable small and mid-market companies to thrive in today's digital economy, Acumatica's flexible solution, customer-friendly business practices, and industry-specific functionality help growing businesses adapt to fast-moving markets and take control of their future.

For more information on Acumatica,
visit www.acumatica.com or follow us on LinkedIn.

Acumatica
The Cloud ERP