Multi-Layered ERP Security

Acumatica provides a comprehensive security framework to safeguard your data, giving you the confidence to grow on a trusted, reliable platform.

- Control user access with role-based permissions, two-factor authentication, and single sign-on
- Safeguard information with advanced encryption
- Meet GDPR, ISO/IEC, SOX, and other security compliance standards with complete audit trails

Key business benefits

- Safeguard your data with a secure foundation designed to protect you from system access to storage.
- Manage risk and meet compliance standards like GDPR and ISO/IEC 27001 efficiently.
- Employ industry-leading encryption and data handling protocols to keep data secure, whether at rest or in transit.
- Leverage a world-class, high-performing cloud ERP with 99.9% guaranteed uptime.
- Use granular, role-based access controls and comprehensive audit trails to manage user permissions and track all system activity.

Related resources

- Acumatica Security Webpage > LEARN MORE
- Mozaic Customer Success Story > LEARN MORE

Securing the Future: Safeguard Your Data, Users, and Systems with Layered Protection

Acumatica is built on the conviction that thriving businesses need tools that empower them to innovate and collaborate with confidence. We've engineered a comprehensive, multi-level security framework to safeguard your data at every stage, from initial system access to data entry, transmission, and storage.

Our defense-in-depth strategy integrates administrative, technical, and physical controls to protect your systems and data. By hosting our SaaS solution on Amazon Web Services (AWS), our customers gain the benefits of the world's most advanced cloud infrastructure. We proactively mitigate risks behind the scenes, so you can focus on what matters most: growing your business with confidence.

Our security approach gives you:

- **Multi-Layered Defense:** Application, data, and infrastructure security form overlapping layers of protection, eliminating single points of failure.

- **World-Class Infrastructure:** Leveraging AWS provides a secure, resilient foundation with state-of-the-art physical security and redundancy.

- **Proactive Threat Management:** We manage vulnerabilities through regular scanning, penetration testing, and disciplined patching to stay ahead of emerging threats.

- **Complete Control and Visibility:** Granular, role-based permissions and audit trails let you manage who sees what, keeping data secure and compliant.

"Smartnumbers works with some really high-profile and sensitive organizations…and so security is really important to us. Acumatica has taken a lot of that burden off our hands. They've got great security policies and with the data residing on AWS, we know that it's really well looked after."

–Chris Drake, Chief Financial Officer, Smartnumbers

> CUSTOMER STORIES

User Login Accounts

Authorize system access with a unique login for every user. Assign accounts to UI, API, or Unrestricted types to control access through the application interface, web services, or both.

Cybersecurity

Implement end-to-end identity management, data protection, and strong authentication to reduce risk. Our approach includes trust validation, cloud security, compliance, two-way data monitoring, and data encryption.

GDPR Compliant

Comply with the European Union's General Data Protection Regulation (GDPR). Track user consent to store and process private information and easily hide or erase it if consent expires.

Single Sign On (SSO)

Simplify user access and enhance security by integrating with providers like Active Directory (AD), Microsoft Entra ID, and other services that support OpenID Connect (such as Google, OneLogin, and Okta).

User Access Rights

Assign and configure granular access rights to specific application areas, including forms, screens, and individual fields. Manage permissions through user roles or directly on user accounts.

Multi-Factor Authentication Enforcement

Add an extra layer of security to user accounts. Require a second verification step via email, SMS, or a push notification from the Acumatica Mobile App to grant system access. You can enforce MFA for access across web, mobile, and APIs.

System-Wide Security Preferences

Define and manage system-wide security settings for your organization, including password policies, lockout rules for unsuccessful login attempts, encryption certificates, and audit settings.

Login and Session Controls

Protect against brute-force attacks by setting policies that lock out accounts after multiple failed login attempts. You can also automatically sign users out after a defined period of inactivity, minimizing the risk of unauthorized access from unattended workstations.

IP Filters

Limit system access by listing approved IP address ranges for each user account. Logins from IP addresses outside the specified range are automatically denied.

Device Management

Control which devices can connect to your system. The platform automatically registers mobile devices with a user's login account for improved tracking. You can also require registration and administrative approval for new devices, enhancing security at all entry points.

Comprehensive Audit Trail

Continuously track and log all system activity. You can define how many months to retain the audit history of all user operations, including modifications to user permissions and system configurations, to support compliance audits.

Role-Based Security Roles

Tailor security roles to match organizational structures. Assign users only the access and permissions needed for their responsibilities and streamline oversight with predefined roles.

Security Settings by Tenant, Company, and Branch

Configure security preferences at multiple organizational levels—individual tenant, company, or branch—to support complex, multi-entity environments and ensure fine-grained control.

Session Timeout Controls

Automatically sign users out after periods of inactivity, minimizing the risk of unauthorized access from unattended workstations.

Data Encryption:

Secure all data in transit using TLS 1.2 encryption. You can use either an Acumatica-provided certificate or your own to protect data as it moves between the server and the client.

Encryption Certificate Management

Easily manage and update encryption certificates for your organization, ensuring your data remains encrypted and secure.

Delegated Administration

Allow select users to manage user accounts and security settings without granting them unnecessary or broader access, enabling secure delegation and streamlined compliance.

User Activity Monitoring

Gain visibility into user actions and potential security incidents. The system can alert you to unusual activities, such as abnormal login locations or times, to help you detect and respond to threats.

HTTPS (Data in Transit Protection)

Secure all data in transit using TLS 1.2 encryption. You can use either an Acumatica-provided certificate or your own to protect data as it moves between the server and the client.

Multi-Entity Security

Configure security preferences at multiple organizational levels—individual tenant, company, or branch—to support complex, multi-entity environments and ensure fine-grained control.