Acumatica Cloud ERP Solution Security and Access Control Best Practices

Working closely with our partner ecosystem is vital to building trust and maintaining the security of our customers. This guide is designed for both Acumatica customers (who own and manage access within their Acumatica Cloud ERP instance) and Acumatica's VAR partners (who advise and support implementation and ongoing governance). To help ensure secure and authorized access to Acumatica Cloud ERP instances, we want to share the following best practices that provide a practical roadmap to maintaining customer security. We tailored this guide for business leaders, project teams, and IT stakeholders and have recommendations and actionable guidance in three areas: (1) Password Policy and Expiration; (2) Role-based Access Control; and (3) Addressing Exposure and Vulnerabilities – following these steps and recommendations will help support your organizational security, compliance and operational efficiency.

Section 1: Password Policy and Expiration Best Practices

Configure password settings in Security Preferences for system-wide rules and on the Users form for per-user overrides.

Recommended System-Wide Settings

- **Force Password Change:** Set to every 90 or 180 days. This balances security and usability.
- **Minimum Password Length:** Require 12 or more characters. Length is more critical than complexity.
- **Password Complexity:** Require upper case, lower case, numbers, and special characters. This prevents common or weak passwords.
- **Password History:** Remember the last ten to 12 passwords to prevent password cycling.
- **Account Lockout:** Lock out accounts for 15 minutes after three to five failed attempts. This provides standard brute-force protection.
- **Lockout Counter Reset:** Reset the counter after ten to 15 minutes for a reasonable retry window.

Per-User Options

- **Password Never Expires:** Use this sparingly. Reserve it primarily for service and integration accounts never for regular users or consultants.
- **Force Change on Next Login:** Apply this when you create new users or after a potential compromise.
- **Enable Self-Service:** Turn on password recovery and self-service changes to empower your users.
- **Modern Guidance:** Combine strong length requirements and multi-factor authentication rather than overly frequent forced changes.

Additional Strong Security Recommendations

- **Enable Multi-Factor Authentication:** We strongly recommend multi-factor authentication via email, text, or an authenticator app.
- **Single Sign-On:** Integrate with Microsoft Entra ID, Okta, or similar providers to streamline secure access.
- **IP Address Restrictions:** Limit logins to approved IP ranges when feasible.
- **Monitor Login Activity:** Regularly review user activity and access history logs to unlock data insights regarding system access.
- **Service Accounts:** Create dedicated accounts for integrations with strong, random passwords and the "Password Never Expires" setting.

Quick Security Setup Checklist

1. Set a company-wide password policy in Security Preferences.
2. Create job-function-based user roles.
3. Assign roles to users.
4. Fine-tune permissions via Access Rights by Role.
5. Test with sample users before a full rollout.
6. Schedule quarterly access and security reviews.

For more information on configuring password settings, please see Preparing an Instance: To Configure Secure Access for Implementers

Section 2: Role-Based Access Control

The Acumatica Cloud ERP solution employs a robust role-based security model. You assign permissions to roles, and users inherit permissions from their assigned roles. You can also combine multiple roles to empower your teams with the exact access they need.

Core Best Practices

- **Principle of Least Privilege:** Grant users only the access required to perform their jobs. Avoid broad "Administrator" or "Full Access" roles unless absolutely necessary.
- **Start with Predefined Roles:** Use the built-in roles in your Acumatica Cloud ERP solution as templates and customize them.
- **Create Task-Based Roles:** Design roles around actual responsibilities, such as AP Clerk, Sales Manager, or Warehouse User, rather than individual users.
- **Granular Permissions:** Control access at multiple levels:
    - Modules and workspaces
    - Individual screens and forms
    - Fields, buttons, columns, and reports
    - Row-level security using Restriction Groups to limit visibility by branch, customer, or inventory item
- **Regular Access Reviews:** Conduct periodic reviews of roles and user assignments, especially after promotions, role changes, or departures (especially for temporary implementation accounts, consultants, and partner personal).
- **Immediate Offboarding:** Disable or delete user accounts immediately when an employee departs to ensure continuous compliance.
- **Avoid Role Proliferation:** Keep the number of roles manageable to simplify maintenance and reduce administrative overhead.

Where to Configure Access

- **Users:** Create and edit users and assign roles.
- **User Roles:** Create and manage custom roles.
- **Access Rights by Role:** Fine-tune permissions to revoke, view, insert, update, or delete records.

For more information on role-based access control, please see: Configuring User Roles

Section 3: Addressing Exposure and Vulnerabilities

If exposure to secure systems has been detected and may be sourced to, for example, an account containing an email address belonging to a former employee of a consultant that was not properly offboarded, the following steps are designed to address vulnerabilities and mitigate the impact.

Immediate (0–48 hours)

1. Disable the account and any other legacy @acumatica.com or ex-consultant accounts.
2. Force password reset + enable Multi-Factor Authentication (MFA) on all users.
3. Review Access History logs for the account and related transactions.

Short-Term (1–2 weeks)

1. Conduct full user & permission audit (Users → Access Rights by Role → Restriction Groups).
2. Enforce strong password policy (expiration, complexity) and MFA globally.
3. Document the incident and notify internal compliance/insurance if required.

Long-Term Process Improvements

1. Adopt a formal **Consultant/Partner Access Offboarding Policy** (template available on request).
2. Update partner SLA to mandate:
    - New accounts for any consultant change of employer.
    - Annual access certification.
    - Quarterly security reviews.
3. Integrate account cleanup into every project closeout and hyper care checklist.
4. Schedule recurring internal super-user training on security best practices via Acumatica University.
5. Consider automated tools or reports to flag dormant/high-privilege accounts.

For additional help and guidance, please visit the Acumatica Community and Help Portal https://community.acumatica.com/ and https://help.acumatica.com