



System Security

Vagif Tariverdiyev

Implementation Specialist

Timing and Agenda

November 10, 2021 -10 AM -11 AM

Day 1

Part 1: Preparing an Instance for Implementation

Lesson 1.1: Activation and Licensing

Lesson 1.2: Configuring System-Wide Security

November 11, 2021 -10 AM -11 AM

Day 2

Part 2: Securing Access to the System

Lesson 2.1: Configuring User Roles

Lesson 2.2: Setting User Access

Lesson 2.3: Encrypting with Digital Certificates

Timing and Agenda

November 12, 2021 -10 AM -11 AM

Day 3

Part 3: Monitoring User Activities

Lesson 3.1: Using System-Wide Security Auditing

Lesson 3.2: Using Field-Level Auditing

Part 4: Using Multifactor Authentication Methods

Lesson 4.1: Configuring Two-Factor Authentication

A black and white photograph showing a man from the waist up, wearing a green t-shirt with "xByte" printed on it. He is leaning over a server rack, focused on his work. The rack is filled with various server components and cables. In the background, other server racks and equipment are visible in a dimly lit room.

Day 1

Lesson 1.1: Preparing an Instance for Implementation

Learning Objectives

In this session, you will learn how to do the following:

- Activate the Acumatica ERP instance by enabling the default set of features
- Activate the product license for the Acumatica ERP instance
- Review product license details

Preparing an Instance: To Enable Features and Activate the License

Story

Suppose that the SweetLife Fruits & Jams company has purchased an Acumatica ERP subscription in Acumatica Business Cloud. The instance has been installed by SaaS engineers. You, as a system administrator, have received the instance URL and the credentials to the *admin* user. Now you need to prepare the instance for implementation. You are the first one to sign in to the instance, and activate and license it with the product key you have obtained from the sales representative. The company has purchased the S1 license tier with three concurrent users and five tenants. In addition to the default set of features, your company has purchased the basic functionality associated with the *Inventory and Order Management* group of features.

Figure: Activation status of initial features

The screenshot shows the Acumatica welcome screen. On the left is a sidebar with icons for Favorites, Data Views, and More Items. The main area displays the message "Welcome to Acumatica" with a large blue circular logo containing a white '@' symbol. Below it is a "New to Acumatica?" section with a brief description of self-study materials.

The screenshot shows the "Enable/Disable Features" screen. The sidebar includes Favorites, Data Views, and More Items. The main content area has a "MODIFY" button and a "ENABLE" button. A box labeled "Activation Status: Pending Activation" is highlighted with a red border. At the bottom, there is a "Finance" section with a single checked checkbox.

Figure: Activation status of the enabled features

The screenshot shows the "Enable/Disable Features" screen with the "VALIDATED" status. The sidebar and main content area are identical to the previous screenshot, but the activation status is now "Validated". The "Finance" section shows several checkboxes, with "Centralized Period Management" being the only one checked.

Activate the product license for the Acumatica ERP instance

Activate License screen before entering
License Key. Click on AGREE and then on
APPLY LICENSE buttons

Activate License

ENTER LICENSE KEY UPLOAD LICENSE FILE UPDATE LICENSE DELETE LICENSE

Status:	Valid		
Valid From:	6/8/2020 12:00:00 AM	Valid To:	11/30/2021 12:00:00 AM
Number of Users:	3	Version:	6.00
		Number of Tenants:	5

Activated	Feature Name

Activate License

ENTER LICENSE KEY UPLOAD LICENSE FILE

Status:	Invalid		
Valid From:	1/1/0001 12:00:00 AM	Valid To:	1/1/0001 12:00:00 AM
Number of Processors:	0	Version:	
Number of Users:	0	Number of Tenants:	0

Activated Feature Name

Activate New License

Disclaimer: The license Key is a 20-character alphanumeric string (example: 1234-5678-90AB-CDEF-1234) that your partner receives from Acumatica upon completion of software contract signing.

If your system has been upgraded or reinstalled, please contact your partner to get a new license immediately.

Please Enter License Key:

OK CANCEL

Activate License

ENTER LICENSE KEY UPLOAD LICENSE FILE

Status:	Invalid		
Valid From:	1/1/0001 12:00:00 AM	Valid To:	1/1/0001 12:00:00 AM
Number of Processors:	0	Version:	
Number of Users:	0	Number of Tenants:	0

Activated Feature Name

Agree to proceed

To continue activation of the new license you must agree to the terms of the [software license agreement](#).

AGREE DISAGREE

Figure: License Monitoring Console

License Monitoring Console ☆

LICENSE STATISTICS WARNINGS CONSTRAINT HISTORY

License Status: Valid
★ License Tier: S Series, Tier 1

LICENSE DETAILS

Monthly Number of Commercial Transactions:	1000
Monthly Number of ERP Transactions:	20000
Database Storage Included (GB):	1

RECOMMENDED MAXIMUMS

Daily Commercial Transactions:	100
Daily ERP Transactions:	2000
Concurrent Users:	3

SYSTEM CONSTRAINTS

Maximum Number of Web Services API Users:	10
Maximum Number of Concurrent Web Services API Requests:	3
Maximum Number of Web Services API Requests per Minute:	50
Maximum Number of Fixed Assets:	1000
Maximum Number of Inventory Items:	50000
Maximum Number of Business Accounts:	50000
Maximum Number of Lines per Transaction:	1000
Maximum Number of Serial Numbers per Document:	2000
Maximum Number of Employees Paid by Month:	0

Lesson 1.2: Configuring System-Wide Security

Learning Objectives

In this session, you will learn how to do the following:

- Configure system-wide security policies
- Create users for people to be involved in further implementation

Preparing an Instance: To Configure Secure Access for Implementers

Story

Suppose that the SweetLife Fruits & Jams company has purchased a cloud subscription for Acumatica ERP. You, as a system administrator, need to configure the secure access for the production tenant of the Acumatica ERP instance.

The company has the following security requirements:

- Users should change their passwords twice a year—that is, every 180 days.
- The minimum password length is 10 symbols without spaces.
- A password must include Latin uppercase and lowercase letters, digits, or special characters, except for \$ and ".
- A user has three attempts to enter a valid password; if an invalid password is entered on the fourth attempt, the user will be locked out for 15 minutes.

Step 1: Configuring the Password Policy

Step 2: Configuring Account Lockout Policies

Security Preferences

File Back

PASSWORD POLICY

Force User to Change Password Every Days
 Minimum Password Length Characters
 Password Must Meet Complexity Requirements

Additional Password Validation Mask:
Following characters must be excluded: \$ and ".

Incorrect Password Alert:

TWO-FACTOR AUTHENTICATION POLICY

Two-Factor Authentication: Allow Email Allow SMS

ACCOUNT LOCKOUT POLICY

Lock Account After: Unsuccessful Login Attempts
Lock Account for: Minutes
Reset Lockout Counter After: Minutes

MODERN UI

* Menu Editor Role:

AUDIT

Keep Audit History for: Months

Login Session Expired OData Refresh
 Login Failed License Exceeded Customization Published
 Logout Send Email Success
 Screen Accessed Send Email Error

Preparing an Instance: To Configure Secure Access for Implementers

Story

- The system should reset the lockout counter when it has been 10 minutes since the first failed sign-in. That is, if a user enters the third invalid password 11 minutes after the first failed attempt, the system will not lock out the user, because the count of failed attempts was restarted 10 minutes after the first failed attempt.

The following people are to be involved in the implementation process:

- You—Kimberly Gibbs, the system administrator with the SweetLife Fruits & Jams company
- Jerry Prado, who is an implementation consultant with the Adaptabiz company, one of Acumatica's partners

Step 3: Adding a User accounts

Users

* Login: gibbs Status: Active

User Type: Kimberly Gibbs

First Name: Kimberly

Last Name: Gibbs

Email: gibbs@sweetlife.com

Comment: System administrator in the SweetLife company

Allowed Number of Sessions: 3

TWO-FACTOR AUTHENTICATION

Two-Factor Authentication: None

Guest Account

Allow Password Recovery

Allow Password Changes

Password Never Expires

Force User to Change Password on Next Login

Override Security Preferences

ROLES STATISTICS IP FILTER EXTERNAL IDENTITIES PERSONAL SETTINGS DEVICES LOCATION TRACKING

Selected	Role Name	Role Description
<input checked="" type="checkbox"/>	Administrator	System Administrator
<input checked="" type="checkbox"/>	Customizer	Customizer
<input checked="" type="checkbox"/>	Field-Level Audit	Role that can access Field-Level Audit
<input checked="" type="checkbox"/>	Portal Admin	Access to portal configuration
<input checked="" type="checkbox"/>	ReportDesigner	Report Designer

Users

* Login: jprado Status: Active

User Type: Jerry Prado

First Name: Jerry

Last Name: Prado

Email: jprado@adaptabiz.com

Comment: Implementation consultant with the Adaptabiz company, one of Acumatica's partners

Allowed Number of Sessions: 3

TWO-FACTOR AUTHENTICATION

Two-Factor Authentication: None

Guest Account

Allow Password Recovery

Allow Password Changes

Password Never Expires

Force User to Change Password on Next Login

Override Security Preferences

ROLES STATISTICS IP FILTER EXTERNAL IDENTITIES PERSONAL SETTINGS DEVICES LOCATION TRACKING

Selected	Role Name	Role Description
<input checked="" type="checkbox"/>	Administrator	System Administrator
<input checked="" type="checkbox"/>	Customizer	Customizer
<input checked="" type="checkbox"/>	Field-Level Audit	Role that can access Field-Level Audit
<input checked="" type="checkbox"/>	Internal User	Allows the user to change personal settings, a...
<input checked="" type="checkbox"/>	Wiki Admin	Wiki Administrator to set other users access rig...

Figure: Custom alert message for incorrect password



The password length must be at least 10 characters without spaces. The password must contain characters from three of the following four categories: English uppercase characters (A through Z); English lowercase characters (a through z); base 10 digits (0 through 9); and non-alphabetic characters (such as !, #, and %). The following characters must be excluded: \$ and ".

Figure: Account lockout alert message



Your account is locked out. Please contact your system administrator.

A close-up photograph of a person's arm and hand pouring beer from a tap into a glass. The glass is branded with the Devil's Peak logo, featuring a spade symbol and the text "Devil's Peak BREWING COMPANY". The background shows more of the brewery equipment.

Day 2

Devil's Peak Brewing Company
Acumatica Customer Since 2016

 **Acumatica**
The Cloud ERP

Lesson 2.1: Configuring User Roles

Learning Objectives

In this session, you will learn how to do the following:

- Create a user role and specify access rights to system objects for this role
- Modify access rights to system objects for a copy of an existing role
- Give access to only particular forms in the system and revoke access to all other system objects
- Review the access rights a role has to system objects

User Roles: To Configure Roles for Four Access Tiers

Story

Suppose that the SweetLife Fruits & Jams company has purchased an Acumatica ERP subscription in Acumatica Business Cloud. The instance has been installed by SaaS engineers, and a basic company configuration has been performed. The company has decided to have four access tiers:

- **Configurator**: Roles from this tier give access to only the configuration settings of a functional area.
- **Manager**: Roles from this tier allow users to work with the entities, inquiries, and reports of a functional area without any restrictions and view configuration settings.
- **Clerk**: Roles from this tier allow users to only add new records and edit record details within a functional area.
- **Auditor**: Roles from this tier allow users to only view records, inquiries, and reports associated with a functional area.

You, as a system administrator, have decided to start implementation of the tiers with the general ledger functional area, and you will define one role for each tier. By default, the forms related to this area are grouped under the **Finance** workspace.

Lesson 2.1: Configuring User Roles

Restriction Levels : A user role in Acumatica ERP is a set of access rights to system objects. By defining access rights for a system object, you set the restriction level a user with the role will have for this object. The restriction level defines the set of operations a user may perform with the object. The highest restriction level allows a user to perform any operation with an object, up to its deletion, and the lowest restriction level denies access to an object.

System Objects Grouping : All objects in Acumatica grouped in tree nodes. At each level of nodes access rights are PROPAGATED to nested objects or nested objects INHERIT access right from parent.

- 1. Tenant:** A tenant node nests all workspaces configured in the system. The system propagates the access rights set to a role for this node to all workspaces in the tenant.
- 2. Workspace:** A workspace node nests all forms added to the workspace. The system propagates the access rights set to a role for this node to all forms within the workspace.
- 3. Form:** A form node may or may not nest several containers with the form elements. Nested containers inherit the access rights set to a role for a form.
- 4. Form container:** A container node nests form elements, such as boxes and actions. Nested elements inherit the access rights set to a role for a container.
- 5. Form element:** An element node is on the lowest level of the object hierarchy and inherits its access rights from its parent container.

Predefined Roles : Acumatica ERP provides a set of predefined roles, which is expanded with every major release of Acumatica ERP. We recommend using the predefined roles while you configure user access to the system during implementation. With every major release of Acumatica ERP multiple new forms are added. If you have modified access rights to a system entity for a predefined role, then the system preserves your changes during the upgrade but updates access rights to other entities for this role, if any were added, deleted, or updated with the new release.

Role Creation Process : Planning, Creation, Modification (you can use Access Rights by Screen or Access Rights by Role forms). You can update role or use combination of the roles.

Lesson 2.1: Configuring User Roles

Modify access right to roles created to Finance node:

AA_GL_Auditor : View Only

AA_GL_Configurator : Not Set

AA_GL_Manager : Delete

AA_GL_Clerk : Not Set

Then review
User_Roles_GL_4Tier_Acc
ess files and modify access
to the rest of the form on
GL workspace.

Form ID	Form Title	Category	GL_Configurator	GL_Manager	GL_Clerk	GL_Audit
GL.61.20.01	GL_Budget Edit	Report	Not Set	Granted	Not Set	View Only
GL.61.10.00	GL_Edit Account Distribution	Report	Not Set	Granted	Not Set	View Only
GL.61.05.00	GL_Edit Detailed	Report	Not Set	Granted	Not Set	View Only
GL.61.15.00	GL_Edit Summary	Report	Not Set	Granted	Not Set	View Only
GL.64.15.00	GL_Recurring Transactions	Report	Not Set	Granted	Not Set	View Only
GL.64.05.00	GL_Recurring Transactions Detailed	Report	Not Set	Granted	Not Set	View Only
GL.62.05.00	GL_Register	Report	Not Set	Granted	Not Set	View Only
GL.62.10.00	GL_Register Detailed	Report	Not Set	Granted	Not Set	View Only
GL.69.00.10	GL_Reversing Batches	Report	Not Set	Granted	Not Set	View Only
GL.63.35.00	Transactions for Account	Report	Not Set	Granted	Not Set	View Only
GL.63.30.00	Transactions for Period	Report	Not Set	Granted	Not Set	View Only
GL.63.25.00	Trial Balance Detailed	Report	Not Set	Granted	Not Set	View Only
GL.63.20.00	Trial Balance Summary	Report	Not Set	Granted	Not Set	View Only
GL.20.45.00	Allocations	Profile	Delete	View Only	Not Set	Not Set
GL.30.20.10	Budgets	Profile	Not Set	Delete	Insert	View Only
GL.20.25.00	Chart of Accounts	Profile	Delete	View Only	Not Set	Not Set
GL.20.11.00	Company Financial Calendar	Profile	Delete	View Only	Not Set	Not Set
GL.30.10.00	Journal Transactions	Profile	Not Set	Delete	Insert	View Only
GL.30.40.00	Journal Vouchers	Profile	Not Set	Delete	Insert	View Only
GL.20.10.00	Master Financial Calendar	Profile	Delete	View Only	Not Set	Not Set
GL.20.35.00	Recurring Transactions	Profile	Delete	View Only	Not Set	Not Set
GL.30.30.10	Trial Balance	Profile	Not Set	Delete	Insert	View Only
GL.50.40.00	Generate Recurring Transactions	Processes	Not Set	Delete	Not Set	Not Set
GL.50.90.00	Import Consolidation Data	Processes	Not Set	Delete	Not Set	Not Set
GL.50.30.00	Manage Financial Periods	Processes	Not Set	Delete	Not Set	Not Set
GL.50.20.00	Post Transactions	Processes	Not Set	Delete	Not Set	Not Set
GL.50.60.00	Reclassify Transactions	Processes	Not Set	Delete	Not Set	Not Set
GL.50.55.10	Release Budgets	Processes	Not Set	Delete	Not Set	Not Set
GL.50.10.00	Release Transactions	Processes	Not Set	Delete	Not Set	Not Set
GL.50.15.00	Release Vouchers	Processes	Not Set	Delete	Not Set	Not Set
GL.50.45.00	Run Allocations	Processes	Not Set	Delete	Not Set	Not Set
GL.50.99.00	Validate Account History	Processes	Not Set	Delete	Not Set	Not Set
GL.20.20.00	Account Classes	Preferences	Delete	View Only	Not Set	Not Set
GL.20.50.00	Budget Configuration	Preferences	Delete	View Only	Not Set	Not Set
GL.10.30.00	Consolidation	Preferences	Delete	View Only	Not Set	Not Set
GL.10.10.00	Financial Year	Preferences	Delete	View Only	Not Set	Not Set
GL.10.20.00	General Ledger Preferences	Preferences	Delete	View Only	Not Set	Not Set
GL.10.10.10	Inter-Branche Account Mapping	Preferences	Delete	View Only	Not Set	Not Set
GL.20.15.00	Ledgers	Preferences	Delete	View Only	Not Set	Not Set
GL.20.30.00	Subaccounts	Preferences	Delete	View Only	Not Set	Not Set
GL.10.60.00	Voucher Entry Codes	Preferences	Delete	View Only	Not Set	Not Set
GL.40.20.00	Account by Period	Inquiry	Not Set	Delete	Not Set	View Only
GL.40.30.00	Account by Subaccount	Inquiry	Not Set	Delete	Not Set	View Only
GL.40.40.00	Account Details	Inquiry	Not Set	Delete	Not Set	View Only
GL.40.10.00	Account Summary	Inquiry	Not Set	Delete	Not Set	View Only
GL.63.40.00	Balance Sheet	ARM Report	Not Set	Delete	Not Set	View Only
GL.63.45.00	Balance Sheet - Comparative	ARM Report	Not Set	Delete	Not Set	View Only
GL.63.65.00	Cash Flow	ARM Report	Not Set	Delete	Not Set	View Only
GL.63.50.00	Profit & Loss	ARM Report	Not Set	Delete	Not Set	View Only
GL.63.55.00	Profit & Loss - Comparative	ARM Report	Not Set	Delete	Not Set	View Only
GL.63.60.00	Profit & Loss - Quarterly	ARM Report	Not Set	Delete	Not Set	View Only

User Roles: To Configure a Role with Granular Access

Story

Suppose that the CFO of the SweetLife Fruits & Jams company has decided that only employees authorized by the CFO are allowed to reprint checks. To accommodate this requirement, you, as a system administrator, have decided to create a granular role that will give access to the reprinting of checks only and forbid access to this operation for all other roles. As a result, only users that have full access to accounts payable (that is, only users assigned with a role that gives this access) can be authorized to reprint checks by being assigned this granular role on request from the CFO.

User Roles: To Configure a Role with Granular Access

Table: Restriction-level modifications needed for configuring access to form elements

Roles / System Objects	Release Payments (form)		ReleaseChecksFilter (form container)		Reprint and Reprint with New Number (form elements stored in the container)	
	Initial Level	Configured Level	Initial Level	Configured Level	Initial Level	Configured Level
AA_AP_Reprint_Checks	Not Set	Revoked	Inherited	Revoked	Inherited	Edit
Accountant	Delete	Delete	Inherited	Delete	Inherited	Revoked
Purchasing Manager	Delete	Delete	Inherited	Delete	Inherited	Revoked

Steps :

- (1) Create User Role (AA_AP_Reprint_Checks)
- (2) Set access Right to the Form (Use Access Rights By Screen : for AP>expand Release Payments (AP505200) node and in the right pane, for AA_Ap_Reprint_Check role in Access Rights column select Reevoked)
- (3) Modify access Rights to the Container and Form Elements : Expand Release Payments node and select ReleaseChecksFilter, then specify Revoked for AA_AP_Reprint_Checks role and Delete for Accountant and Purchasing Manager roles.

Figure: The list of roles assigned to the selected user that affect the user's access to the Reprint element

Access Rights by User ★

* Login: basic

VIEW ROLES

Description	Access Rights
> - Add	Delete
> - History	Delete
> - View	Delete
> (Schedule)	Delete
> (ViewDocument)	Delete
> Cancel	Delete
> Export	Delete
> Process	Delete
> Process All	Delete
> Release	Delete
> Reprint	1 Edit
> Reprint with New Number	Edit
> Toggle Currency	Delete
> Action	Delete
> Available Balance	Delete
> Cash Account (PayAccountID)	Delete
> Currency	Delete
> GL Balance	Delete
> Payment Method	Delete
> Post Period	Delete

View Roles

Role	*Initial Access Rights	*Computed Access Rights
AA_AP_Reprint_Checks	Edit	2 Edit
Accountant	Revoked	Revoked
Branch HeadOffice	Inherited	Revoked
Branch MHead	Inherited	Revoked
Branch MRetail	Inherited	Revoked
Branch Retail	Inherited	Revoked
Branch SweetEquip	Inherited	Revoked
Financial Supervisor	Inherited	Revoked
Internal User	Inherited	Revoked

User Roles: To Modify Access Rights for a Copied Role

Story

Suppose that due to the company's growth you, as a system administrator, now have an assistant. Initially, the assistant will help you with the creation of user accounts for the new employees. Then you will decide what other responsibilities the assistant will have. To accommodate the assistant's current job responsibilities, you have decided to copy your existing role (*Administrator*) and modify access rights for the copy.

Step 1: Copy a Role (Open Administrator role and create a copy naming it as Junior administrator).

Step 2: Modify Access Rights to Selected User Role (1. Select Revoked to ALL workspaces, 2. Select Delete access to Configuration>Employees, Marketing>Contacts, User Security>Users)

Step 3: Review access to Workspaces after changes made

User Roles: To Modify Access Rights for a Copied Role

Access Rights by Role

COPY ROLE

* Role Name: Junior Administrator - Junior

Role Description: Junior

COMPANY

Description	*Access Rights
Banking	Revoked
Bills of Material	Revoked
Commerce	Revoked
Compliance	Revoked
Configuration	Revoked
Construction	Revoked
Contract Management	Revoked
Currency Management	Revoked
Customization	Revoked
Dashboards	Revoked
Data Views	Revoked
Deferred Revenue	Revoked
Equipment	Revoked
Estimating	Revoked
Finance	Revoked
Fixed Assets	Revoked
Integration	Revoked
Inventory	Revoked
Marketing	Multiple Rights
Material Requirements Planning	Revoked
Opportunities	Revoked
Payables	Revoked
Payroll	Revoked
Product Configurator	Revoked
Production Orders	Revoked
Project Management	Revoked
Purchases	Multiple Rights

Lesson 2.2: Setting User Access

Learning Objectives

In this session, you will learn how to do the following:

- Create a user account and assign roles, which combine to provide the access rights necessary for the user to perform job responsibilities, to the user account
- Assign a role to multiple users
- Modify access for an existing user account
- Review users' access to system objects

User Access: To Add a User Account

Story

Suppose that you, as a system administrator, have received a request to add a user account for a new employee: Sarah Kent, who has taken the position of warehouse worker. The request has been justified and approved by the corresponding manager.

User Creation Steps : 1. Create record by specifying username, e-mail, First and Last names (Not mandatory), 2. Add at least one role to the user

Generate and Share Credentials : Password could be generated in Password box (you could overwrite the value). You can click Reset Password to create new password for existing user. If system email account is configured system sends an e-mail with credentials to address specified on User>Email box.

User Access Security: In addition to system wide security, you can specify user specific configuration for : password recovery, password change, force password change, password expiration, individual network restriction and user account deactivation.

User Access: To Assign a Role to Multiple Users

Story

Suppose that you, as a system administrator, have received a number of access requests to the generic inquiries that are exposed through the OData protocol—that is, the generic inquiries for which the **Expose via OData** check box is selected on the *Generic Inquiry* (SM208000) form. The access to these inquiries is provided by the predefined *BI* role.

The access requests for the following users have been justified and approved by their respective managers:

- Ian Pick, sales department lead (with the username *pick*)
- Bill Owen, marketing manager (with the username *owen*)

User Access: To Modify Access for a User Account

Story

Suppose that you, as a system administrator, have received a request to modify access for Andrew Barber (formerly a warehouse worker) due to his transfer to a new job position— packline operator. This request has been justified and approved by his manager.

Lesson 2.3: Encrypting with Digital Certificates

Learning Objectives

In this session, you will learn how to do the following:

- Upload digital certificates to be used for database encryption or PDF signing.
- Replace default encryption method used for Acumatica ERP database with a certificate of your choice.
- Configure signing of PDF files generated for reports in the system.

Digital Certificates to store sensitive information in the database encrypted and to authenticate documents (PDF files) that are shared or send electronically (can be purchased from recognized certification authority).

Lesson 2.3: Encrypting with Digital Certificates

Story

Suppose that SweetLife Fruits & Jams company decided to replace the default encryption algorithm used in Acumatica ERP to encrypt sensitive data stored in the database with some other encryption certificate due to company security policies. You, as a system administrator, were requested to configure the replacement.

Steps :

1. Certificate registration (sample provided) on Encryption Certificates (SM200530) form (provide name, password and attach file)
2. Encrypt the Database : Open Certificate Replacement form, specify new Certificate and click Replace Certificate.
3. Removal of Outdated Certificates : Open Encryption Certificates (SM200530) and click Delete Row.

Digital Certificates: To Encrypt the Database

Story

Suppose that SweetLife Fruits & Jams company decided to replace the default encryption algorithm used in Acumatica ERP to encrypt sensitive data stored in the database with some other encryption certificate due to company security policies. You, as a system administrator, were requested to configure the replacement.

Encryption Certificates

Name	Password
AcumaticaTrainingEncryption	*****

Security Preferences

PASSWORD POLICY

Two-Factor Authentication: None

ACCOUNT LOCKOUT POLICY

Lock Account After: 3 Unsuccessful Login Attempts

Lock Account for: 15 Minutes

Reset Lockout Counter After: 10 Minutes

ENCRYPTION CERTIFICATES

DB Encryption Certificate: AcumaticaTrainingEna

PDF Signing Certificate:

Certificate Replacement

REPLACE CERTIFICATE

* New Certificate:

Current Certificate:

Entity Type	Entity Name
PX.Api.SYProviderParameter	SYProviderParameter
PX.Commerce.BigCommerce.B...	BigCommerce Settings
PX.Commerce.Shopify.BCBindi...	Shopify Settings
PX.OAuthClient.DAC.OAuthApp...	OAuthApplication
PX.Objects.AR.CCProcTran	Credit Card Processing Transaction
PX.Objects.AR.CustomerPayme...	Customer Payment Method Detail
PX.Objects.CA.CCProcessingCe...	Credit Card Processing Center Detail
PX.Objects.CA.CCSynchronizeC...	CCSynchronizeCard
PX.Objects.FS.FSSetup	Service Management Preferences
PX.Objects.GL.GLConsolSetup	GL Consolidation Setup
PX.Objects.PJ.DailyFieldReport...	Project Management Preferences - Weather S...
PX.OidcClient.DAC.OidcProvider	OidcProvider
PX.SM.EMailSyncServer	EMailSyncServer
PX.SM.PreferencesIdentityProv...	PreferencesIdentityProvider
PX.SM.Standalone.EMailAccount	EMailAccount
PX.SM.UploadFile	UploadFile
PX.SmsProvider.SM.DAC.SmsPl...	Voice Plug-in Details

A close-up photograph of a small potted plant. The plant is growing in a shallow, round metal tray. It has three distinct stems with clusters of bright green, oval-shaped leaves at the top. The background is slightly blurred, showing what appears to be a person's legs and clothing.

Day 3

Lesson 3.1: Using System-Wide Security Auditing

Learning Objectives

In this session, you will learn how to do the following:

- Enable the auditing of specific user and system activities
- Review the audit trails related to selected system events

Enabling Auditing settings on Security Preference (SM201060) , Audit section and review results under Access History (SM201045) screen

The left screenshot shows the 'AUDIT' section of the Security Preference screen (SM201060). It includes a dropdown for 'Keep Audit History for:' set to 999 Months, and a list of checked audit items: Login, Session Expired, OData Refresh, Login Failed, License Exceeded, Customization Published, Logout, Send Email Success, and Screen Accessed.

The right screenshot shows the 'Access History' screen (SM201045). It has search fields for Username (set to gibbs), From, To, and Operation (set to Login). Below is a table of access history entries:

Date	Username	Operation	Host	IP address	Screen ID
11/5/2021 12:11	gibbs	Login	NA-LT-0018/DB211100032	127.0.0.1	
11/5/2021 12:01	gibbs	Login	NA-LT-0018/DB211100032	127.0.0.1	
11/5/2021 12:01	gibbs	Login	NA-LT-0018/DB211100032	127.0.0.1	
11/5/2021 12:01	gibbs	Login	NA-LT-0018/DB211100032	127.0.0.1	
11/5/2021 12:01	gibbs	Login	NA-LT-0018/DB211100032	127.0.0.1	
11/5/2021 11:51	gibbs	Login	NA-LT-0018/DB211100032	127.0.0.1	
10/28/2021 3:51	gibbs	Login	NA-LT-0018/DB211100032	127.0.0.1	

System-Wide Security Auditing: Process Activity

Story

Suppose that in addition to the auditing of user activities that is configured by default, the management of your company would like to track the publication of customizations and forced user sign-outs due to the maximum number of users, as specified in the license, being exceeded.

Figure: List of Login Failed events

Access History ☆

CUSTOMIZATION TOOLS ▾

↶ ⏪ ⏩ ⏴ DELETE HISTORY

Username: 🔎

From: To:

Operation: ▼

⟳ ⌛ ✖

Date	Username	Operation	Host	IP address	Screen ID	Title	Comment
> [REDACTED]	gibbs	Login Failed	[REDACTED]	[REDACTED]			Error: Your account is locked ...
[REDACTED]	gibbs	Login Failed	[REDACTED]	[REDACTED]			Error: Invalid credentials. Ple...
[REDACTED]	gibbs	Login Failed	[REDACTED]	[REDACTED]			Error: Invalid credentials. Ple...
[REDACTED]	gibbs	Login Failed	[REDACTED]	[REDACTED]			Error: Invalid credentials. Ple...

Lesson 3.2: Using Field-Level Auditing

Learning Objectives

In this session, you will learn how to do the following:

- Configure users' access to the field-level auditing capabilities according to their job descriptions
- Configure the level of detail to be audited for a specific form
- Turn on and off auditing for a specific form
- Review the audit trail for a specific record

Note : The functionality is available if the *Field-Level Audit* feature is enabled on the [Enable/Disable Features](#) (CS100000) form.

Lesson 3.2: Using Field-Level Auditing

Configuration of access to Field-Level Auditing :

Turn On/Off configuration on Audit form

Review Audit results on audit History form

View audit trial for a particular form directly from audited form (predefined Field-Level audit role should be assigned to user), select Tool>audit History (right top corner of the screen). If Audit History command is not shown this form not support field level auditing.

Setup of Auditing of a Form (Audit form) : Select required tables (Tables Section) , Select required fields (Field section, you can specify ALL or UI fields), Select Active to activate functionality. Review sample on changes on Audit History screen

Audit

* Screen Name: **Journal Transactions** Show Fields: **All Fields** Active

Tables

Active	Table	Description	Show Fields
<input type="checkbox"/>	BATCH	GL Batch	All Fields
<input type="checkbox"/>	CURRENCYINFO	Currency Info	All Fields
<input type="checkbox"/>	GLTRAN	GL Transaction	All Fields
<input type="checkbox"/>	GLVOUCHER	GL Voucher	All Fields

Fields

Active	Field
<input checked="" type="checkbox"/>	AMBatchNbr
<input checked="" type="checkbox"/>	AMDocType
<input checked="" type="checkbox"/>	AutoReverse
<input checked="" type="checkbox"/>	AutoReverseCopy
<input checked="" type="checkbox"/>	BatchNbr
<input checked="" type="checkbox"/>	BatchType

Figure: The available Audit History command for the Journal Transactions form

Journal Transactions

NOTES ACTIVITIES FILES BUSINESS EVENTS CUSTOMIZATION
TOOLS

SAVE & CLOSE
RELEASE
ACTION

Module:	AP	Branch:	HEADOFFICE - SweetLife Head Office ar		
Batch Number:	AP000001	Ledger:	ACTUAL - Actual Ledger		
Status:	Posted	<input type="checkbox"/> Auto Reversing <input type="checkbox"/> Reversing Entry			
<input type="checkbox"/> Hold		Type:	Normal		
Transaction D...	12/11/2019	Orig. Batch Number:			
Post Period:	12-2019	Debit Total:	239.00		
		Credit Total:	239.00		
Description:	Logo labels				

- Screen ID CST.GL.30.10.00
- Get Link
- Web Service
- Access Rights...
- Audit History...**
- Share Column Configuration
- Trace...
- About...

VIEW SOURCE DOCUMENT RECLASSIFICATION HISTORY
UP

	Branc	*Ac	Description	Project/C	Project Task	Ref. Number	Tran Date	Quan	UC	Debit Amo	Credi Amo	Transaction Description	No Bill
>	HEA...	20...	Accounts Paya...	X		000001	12/11/2	0.00		0.00	239.00	Logo labels	<input checked="" type="checkbox"/>
>	HEA...	81...	Other Expenses	X		000001	12/11/2	0.00		239.00	0.00	Logo labels	<input type="checkbox"/>

Field-Level Auditing: Implementation Activity

Story

Suppose that the corporate controller of the SweetLife Fruits & Jams company has requested that you, a system administrator, set up the auditing of changes made by users to the fields displayed on the *Invoices and Memos* (AR301000) form.

Steps : 1. Configure and Turning On Auditing for a Form (Screen : Invoice and memos, UI Fields, Select All tables and Fields), 2. Review User Actions on Invoice and Memos Screen : a. Add gibbs to Audit History Access role b. Process / change AR invoice and review results on Tools>Audit History c. Turn off Auditing, Update AR invoice and review results on Tools>Audit History (Open Audit (SM205520) inquiry form, click on screen id and unselect required)

Figure: Audit history for the invoice

Audit History: AR Invoice/Memo

Type: Invoice Reference Nbr.: 000099

Created By: gibbs

Last Modified By: gibbs

Created Through: AR301000

Last Modified Through: AR301000

Created On: 5/11/2021 6:19:47 AM

Last Modified On: 5/11/2021 6:20:26 AM

Date: 5/11/2021 6:20:23 AM User: gibbs Screen: AR301000

▼ Changes:

AR Document Modified

Type	Reference Nbr.	Hold	Status
Invoice	000099	<input checked="" type="checkbox"/>	On Hold
Invoice	000099	<input type="checkbox"/>	Balanced

Date: 5/11/2021 6:19:47 AM User: gibbs Screen: AR301000

► Changes:

Figure: The cleared Active check box for the Invoices and Memos form

Audit ☆

CUSTOMIZATION TOOLS ▾

* Audited Screen ID	Audited Screen Name	Active	Description	Created By	Created On
AR.30.10.00	Invoices and Memos	<input type="checkbox"/>	Auditing changes made to in...	gibbs	10/19/2020
PO.30.10.00	Purchase Orders	<input checked="" type="checkbox"/>	Audit of changes to purchase...	gibbs	10/19/2020

Field-Level Auditing: Process Activity

Story

Suppose that the corporate controller of the SweetLife Fruits & Jams company, Jasmine Reece, has decided to review an audit trail for a recently canceled purchase order. The corporate controller would like to review the audit trail for the order directly from the *Purchase Orders* (PO301000) form, as well as changes to the document on the *Audit History* (SM205530) inquiry form.

Configuration Overview : Field-Level audit and Audit History access roles have been assigned to Jasmine Reece (user reece). Field-level auditing have been configured for PO form.

Steps: 1. Review Auditing History for Particular Document (Click Tools>audit History from same screen), 2. Review the Auditing History for Multiple Documents (Open Audit History screen specify date and document type), 3. Review General information about records only (Tools>Audit History) when auditing have not been configured.

Figure: Audit history for the purchase order

Audit History: Purchase Order

Type: Normal Order Nbr.: 000026

[↓ Expand All](#) [↑ Collapse All](#)

Created By: wiley

Last Modified By: wiley

Created Through: PO301000

Last Modified Through: PO301000

Created On: 10/19/2020 10:16:05 AM

Last Modified On: 10/19/2020 10:17:34 AM

Date: 10/19/2020 10:17:34 AM **User:** wiley **Screen:** PO301000

► Changes:

Date: 10/19/2020 10:17:21 AM **User:** wiley **Screen:** PO301000

► Changes:

Date: 10/19/2020 10:17:12 AM **User:** wiley **Screen:** PO301000

► Changes:

Date: 10/19/2020 10:16:43 AM **User:** wiley **Screen:** PO301000

► Changes:

Date: 10/19/2020 10:16:27 AM **User:** wiley **Screen:** PO301000

► Changes:

Date: 10/19/2020 10:16:06 AM **User:** wiley **Screen:** PO301000

► Changes:

Version: 20.200.0077 **Customization:** None

Figure: Audit history for a purchase order

Audit History ☆

TOOLS ▾

◀ MANAGE

Screen ID: PO.30.10.00 - Purchase Orders Table Name: Purchase Order

User: Start Date: End Date:

Records

Type Order Nbr.

Normal 000026

All Records

Events

All Records

Operation Date and Time User Name Branch Workflow *Vendor *Location *Date Promised On

Operation	Date and Time	User Name	Branch	Workflow	*Vendor	*Location	*Date	Promised On
Created	10/19/2020 10:16 AM	wiley	HEADOFFICE	Standard	ALLFRUITS	MAIN	10/19/2020 12:00 A	10/19/2020 12:00 P
Modified	10/19/2020 10:16 AM	wiley	HEADOFFICE	Standard	ALLFRUITS	MAIN	10/19/2020 12:00 A	10/19/2020 12:00 P
Modified	10/19/2020 10:16 AM	wiley	HEADOFFICE	Standard	ALLFRUITS	MAIN	10/19/2020 12:00 A	10/19/2020 12:00 P
Modified	10/19/2020 10:17 AM	wiley	HEADOFFICE	Standard	ALLFRUITS	MAIN	10/19/2020 12:00 A	10/19/2020 12:00 P
Modified	10/19/2020 10:17 AM	wiley	HEADOFFICE	Standard	ALLFRUITS	MAIN	10/19/2020 12:00 A	10/19/2020 12:00 P
Modified	10/19/2020 10:17 AM	wiley	HEADOFFICE	Standard	ALLFRUITS	MAIN	10/19/2020 12:00 A	10/19/2020 12:00 P

Figure: General information about a document

Journal Transactions
GL GL000016

Module: GL Branch: HEAOFFICE - SweetLife Head Office at Type: Reclassification
Batch Number: GL000016 Orig. Batch Number:
Status: Posted Ledger: ACTUAL - Actual Ledger
Transaction D... 1/24/2021 Debit Total: 520.00
Post Period: 01-2021 Credit Total: 520.00

Description:

Update History

Created By:	admin	Last Modified By:	admin
Created Through:	GL506000	Last Modified Through:	GL301000
Created On:	12/31/1899 7:00:00 PM	Last Modified On:	12/31/1899 7:00:00 PM
Quantity	UOM	Debit Amount	
0.00		0.00	
0.00		520.00	

ENABLE FIELD LEVEL AUDIT CANCEL

VIEW SOURCE DOCUMENT

*Branch	*Account	Description
HEADOFFICE	81000	Other Expenses
HEADOFFICE	61000	Advertising

Lesson 4.1: Configuring Two-Factor Authentication

General Purpose and Types of Multifactor Authentications

In most of the cases multifactor authentications involves TWO mechanisms : the following could be combines : username and password, token or key fob, mobile device, email, smart card or USD device, Fingerprint reader (or Biometric device), VPNs.

Acumatica offers ability to configure two-factors authentication without setting integration with multifactor service providers. If enabled, user must present additional to user credentials evidence (factor). The second factor : Access Code or Sign-In approval send from user's mobile device (Access code could be generated using Web application or Mobile device or can be send by e-mail and SMS/text message). Some multifactor system configured only when the risk profile of system entry is high, for example sign in from unfamiliar IP, after office hours from unfamiliar device.

Lesson 4.1: Configuring Two-Factor Authentication

Learning Objectives

In this session, you will learn how to do the following:

- Activate two-factor authentication system-wide and individually for a user
- Generate a list of access codes
- Configure the delivery of access codes by email or through a short message service (SMS) message
- Authenticate yourself by using an access code generated with a mobile device or by approving a push request

Two-Factor Authentication: Implementation Activity

Story

Suppose that the SweetLife Fruits & Jams company has decided to use two-factor authentication to prevent unauthorized system access. The users of the system should be able to authenticate themselves by using an access code received from the system administrator, a one-time code received by email, or the Acumatica app.

You, as a system administrator, have decided to first test the activation for yourself and then activate it for all users.

Figure: Confirm dialog box for the activation of two-factor authentication

The screenshot displays the Acumatica Security Preferences screen on the left and a 'Confirm' dialog box in the center.

Security Preferences Screen (Left):

- PASSWORD POLICY:**
 - Force User to Change Password Every 30 Days
 - Minimum Password Length 8 Characters
 - Password Must Meet Complexity Requirements
- TWO-FACTOR AUTHENTICATION POLICY:**
 - Two-Factor Authentication: Required
 - Allow Email
 - Allow SMS
- ACCOUNT LOCKOUT POLICY:**
 - Lock Account After: 3 Unsuccessful Login Attempts
 - Lock Account for: 15 Minutes
 - Reset Lockout Counter After: 10 Minutes
- ENCRYPTION CERTIFICATES:**
 - DB Encryption Certificate: AcumaticaTrainingEnv
 - PDF Signing Certificate: [Placeholder]
- Allowed External Identity Providers:**

Provider Name	Active	Realm	Application ID	Application Secret
Exchange...	<input checked="" type="checkbox"/>		*****	
Google	<input type="checkbox"/>		*****	
MicrosoftAcc...	<input type="checkbox"/>		*****	

Confirm Dialog Box (Center):

EMAIL CONFIRMATION

During first login with two-factor authentication you will receive an access code for mobile application by email. To be sure that you have properly specified your email address, please enter the test access code which has been sent to your email gibbs@sweetlife.com

* Enter access code:

BACKUP OPTION

You can generate a list of access codes so that if other methods of the second step during two-factor authentication are unavailable you can use an access code from the list. Print or save the list of access codes not to lose access to your account.

GENERATE LIST OF ACCESS CODES

CONFIGURATION OF USERS FOR INTEGRATED APPLICATIONS

If there are integrated applications that log in with some user's credentials, you need to turn off two-factor authentication for this user on the Users form.

Buttons: OK, CANCEL

Codes Screen (Right):

Codes — Mozilla Firefox
localhost/DB21110032/(W(10001))/frames/reportlaur
10/29/2021 11:01 AM
Kimberly Gibbs u100
CUSTOMIZATION TOOLS

List of Access
User: gibbs Valid To Date: 11/5/2021
Codes
4MFLLNVN5V
5TWUPLVTEF
7JSJICVDNZ
BPKJ2K7VO
BQHEH8AM6G
DCZ35SLJDI
FHVP25UH8
FYBCVFCDBB
GUMPHINUR
I3QZOVFWX5
JU527PCX5U
KEQFY3PZLZ
LIU2F85G
MEABRO4HTD
MQFKEUQZVU
MYKSNTQTNE
N9HRKOBPZN
OHYHMAHOB
ONK5C4TECC
OT5CGFBP4
OVGNSMAKFR
FMU7HUWVHS
PYOB3IZPGS
ROW5J7CMNW

Figure: The default authentication method

The screenshot shows the Acumatica mobile application's login screen. At the top, the Acumatica logo and "The Cloud ERP" text are visible. Below that is a search bar containing the text "gibbs". Underneath the search bar, there is a section titled "Two-Factor Authentication" with the sub-instruction: "To verify your identity by approving push requests on your mobile device:". A numbered list follows: 1. Install Acumatica mobile app on your device. 2. Sign in to the account of this Acumatica instance using access code sent to your email: gibbs@sweetlife.com. Below this, it says "You will be able to re-send the code after 4:23". Another numbered list continues: 3. Approve push request on your mobile device. At the bottom left is a blue button labeled "Send request to device", and at the bottom right is a link "Use Another Authentication Method" which is highlighted with a red border.

Figure: The available authentication methods

The screenshot shows the same Acumatica mobile application interface as the previous figure, but the "Two-Factor Authentication" section is no longer present. Instead, there is a new section titled "Select Authentication Method:" followed by four options: 1. "Receive code by email" (represented by an envelope icon), 2. "Enter code generated in mobile app or from the list" (represented by a key icon with two asterisks), 3. "Receive code in SMS" (represented by a speech bubble icon), and 4. "Receive push notification on the confirmation device" (represented by a smartphone icon).

Figure: Generation of an access code by using the mobile app

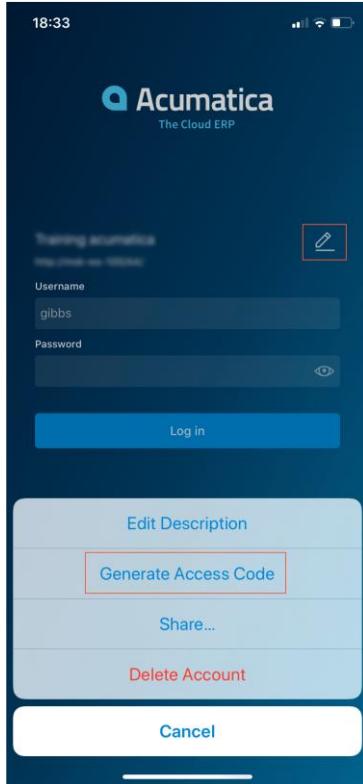


Figure: An approval request sent by the system as a push notification

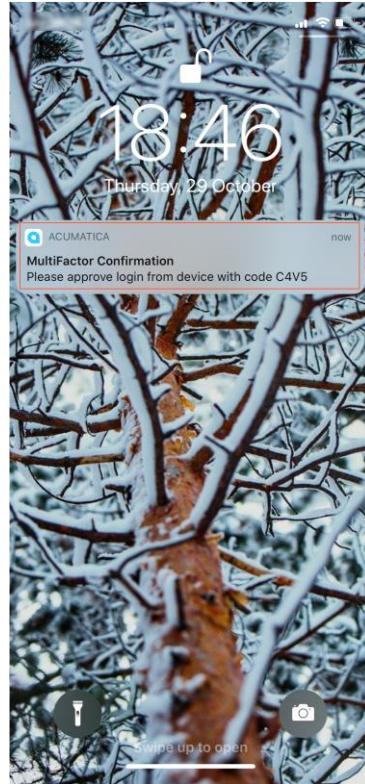


Figure: The Approve button in the Acumatica mobile app



Figure: Access code entered on the first sign-in to the mobile app

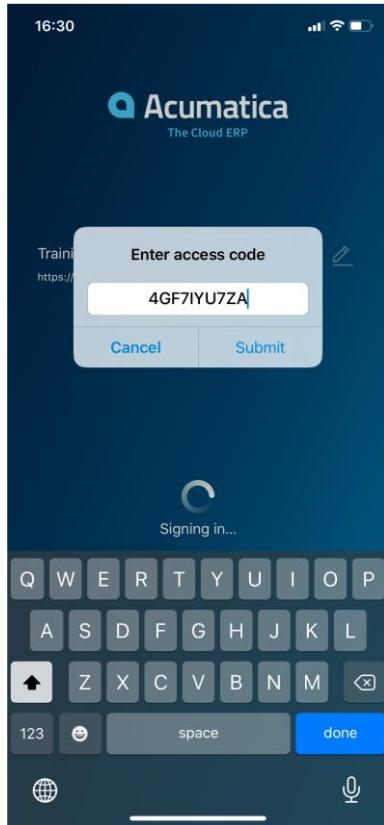
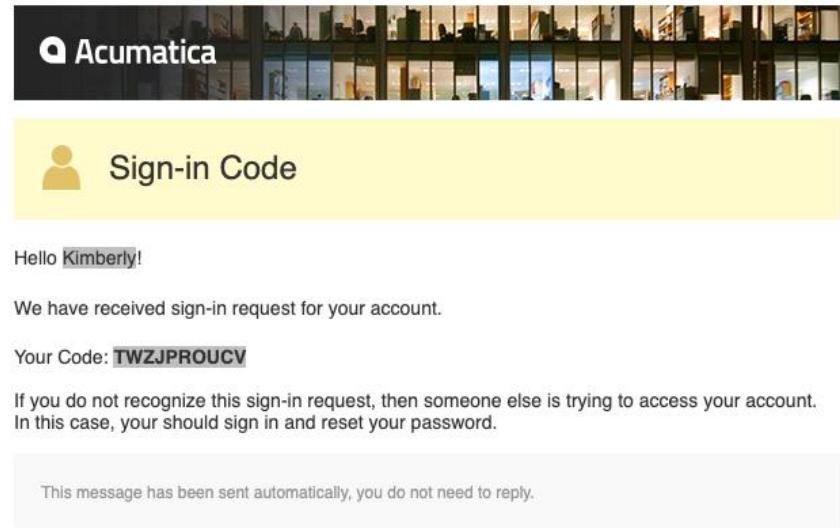


Figure: Sample email with an access code



Feedback

Your feedback is appreciated

<https://www.surveymonkey.com/r/OnlineTraining2021>



No Reliance

This document is subject to change without notice. Acumatica cannot guarantee completion of any future products or program features/enhancements described in this document, and no reliance should be placed on their availability.

Confidentiality: This document, including any files contained herein, is confidential information of Acumatica and should not be disclosed to third parties.



Thank you

Vagif Tariverdiyev