Acumatica
The Cloud ERP

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

Day 1

xByte Technologies
Acumatica Customer Since 2014

Acumatica
The Cloud ERP

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

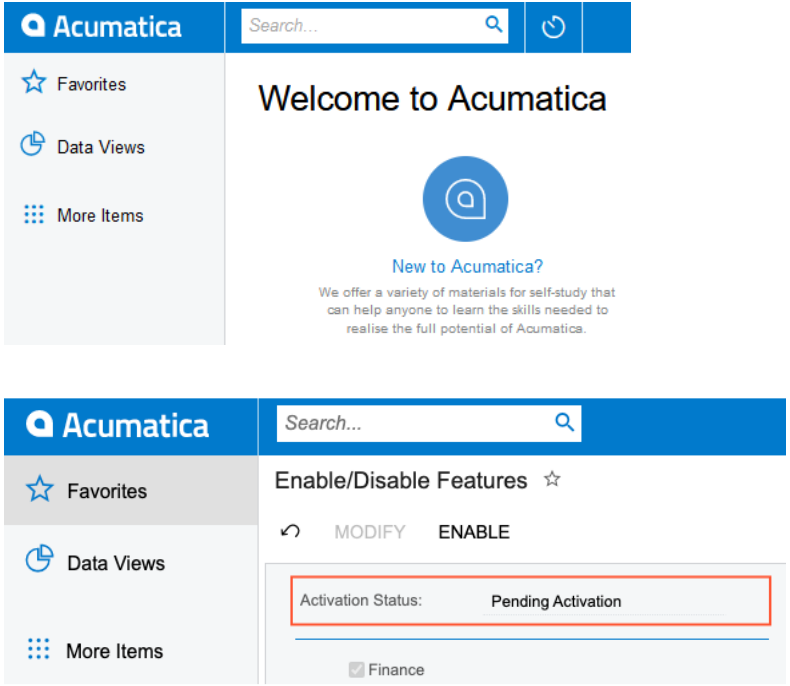
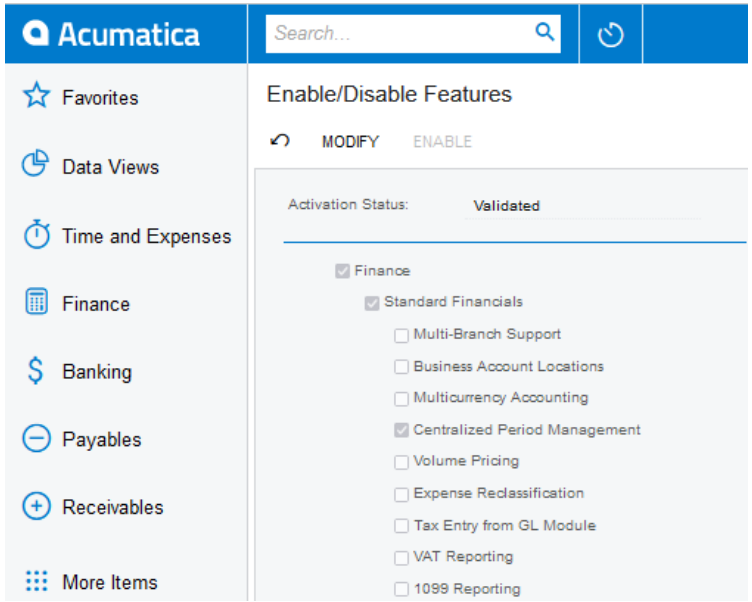
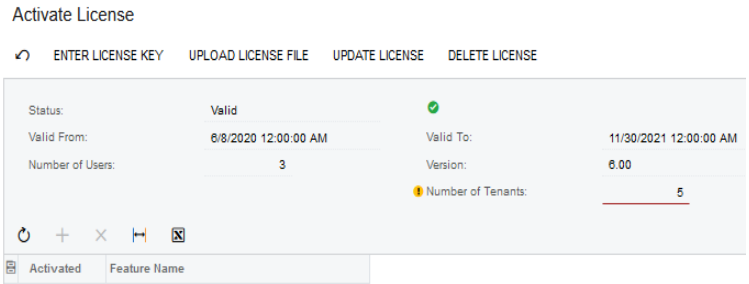


Figure: Activation status of the enabled features



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



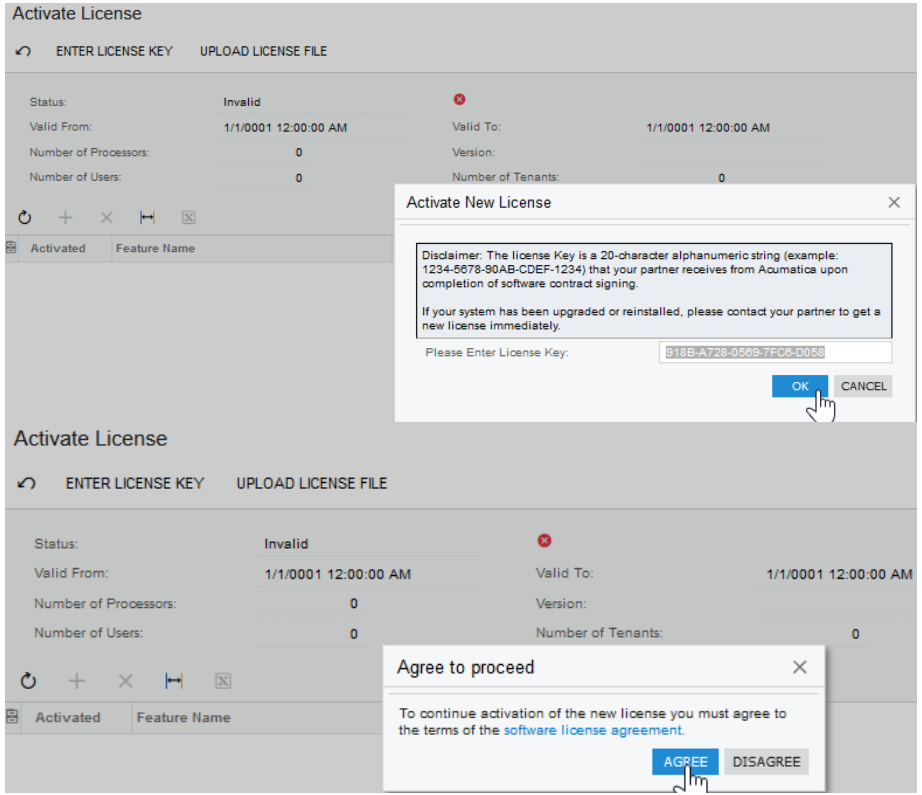
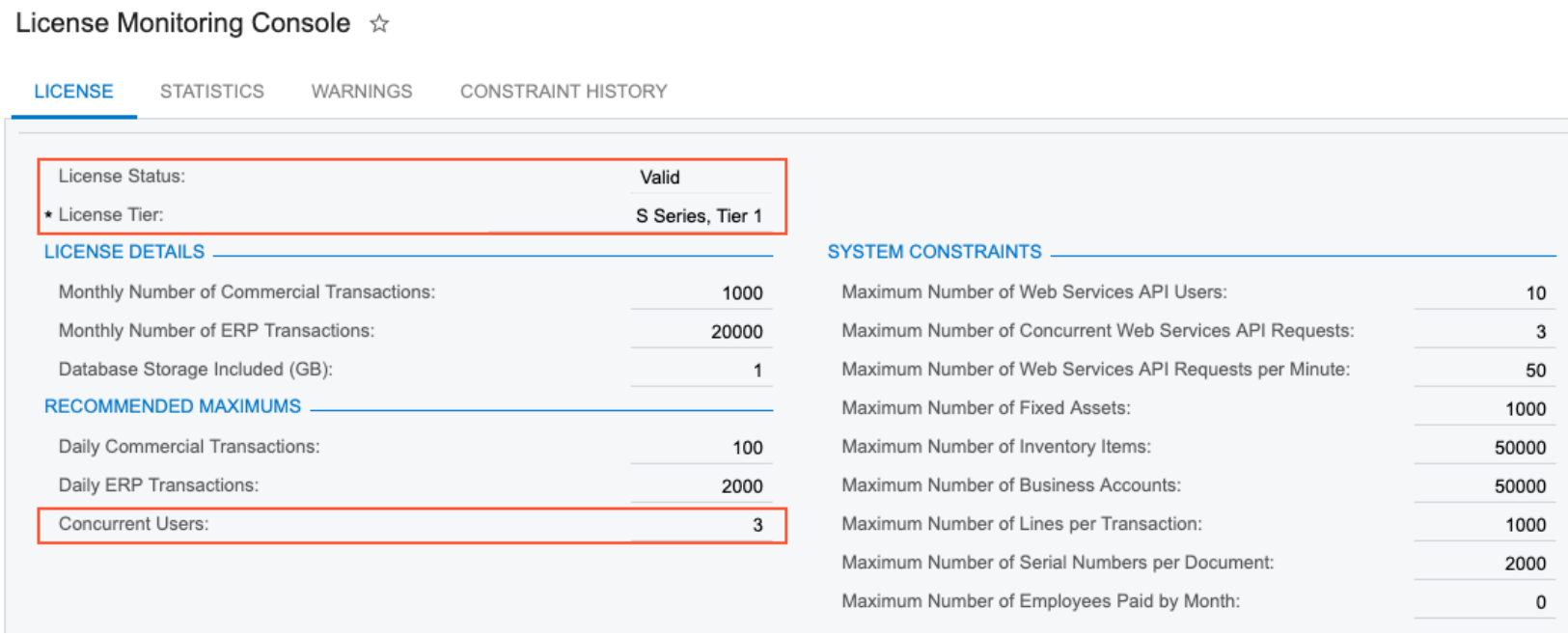


Figure: License Monitoring Console



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

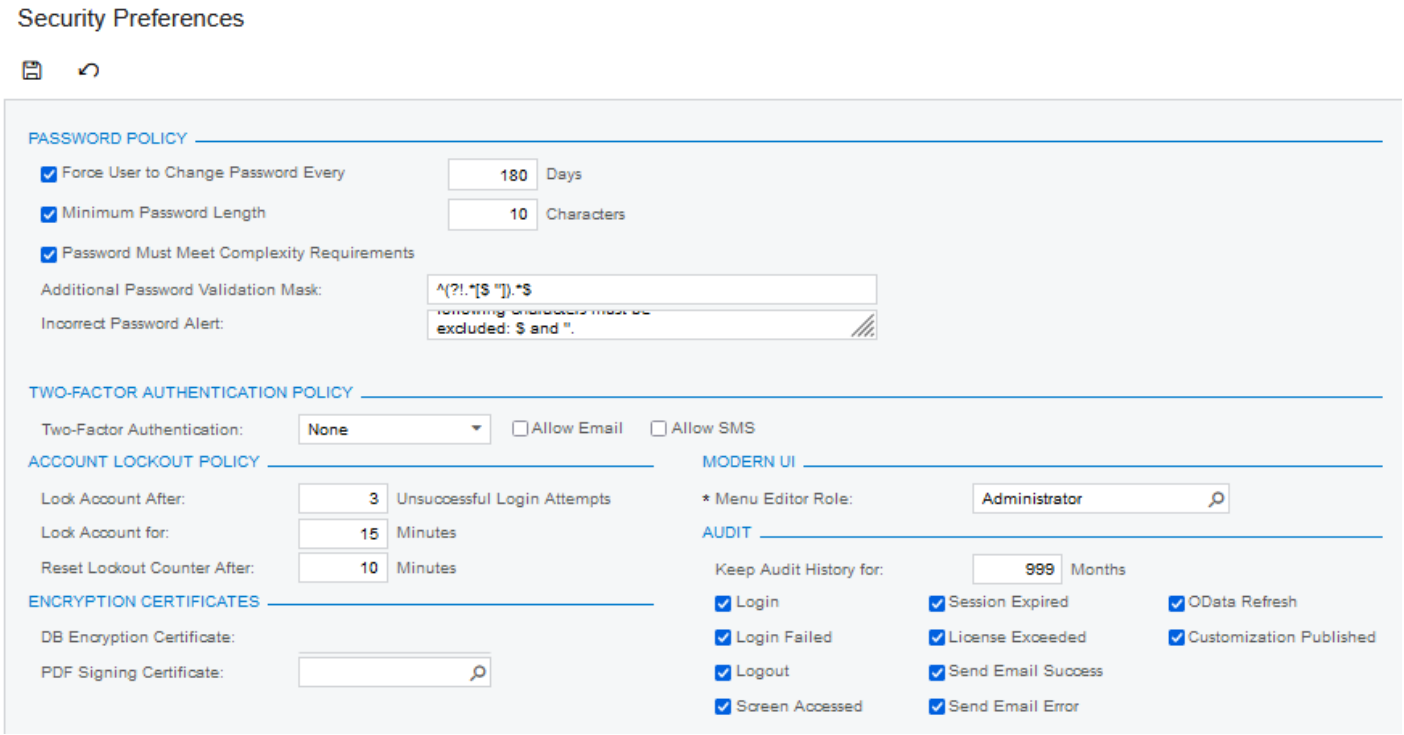
Preparing an Instance: To Configure Secure Access for Implementers

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



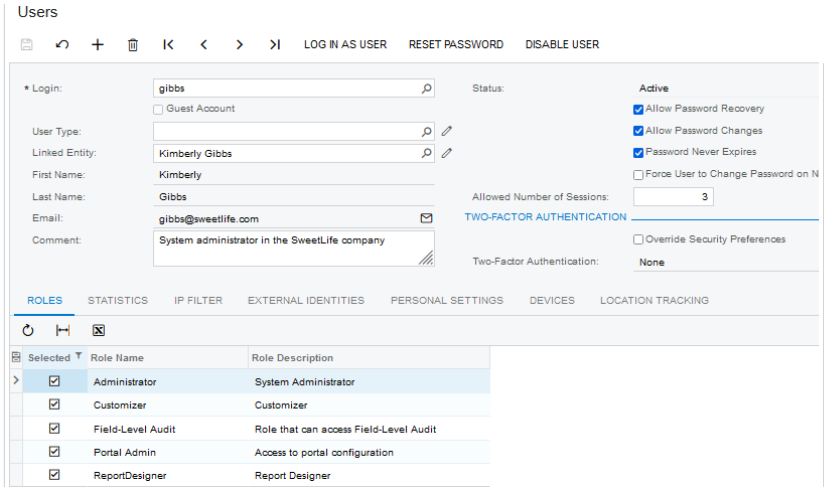
Preparing an Instance: To Configure Secure Access for Implementers

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



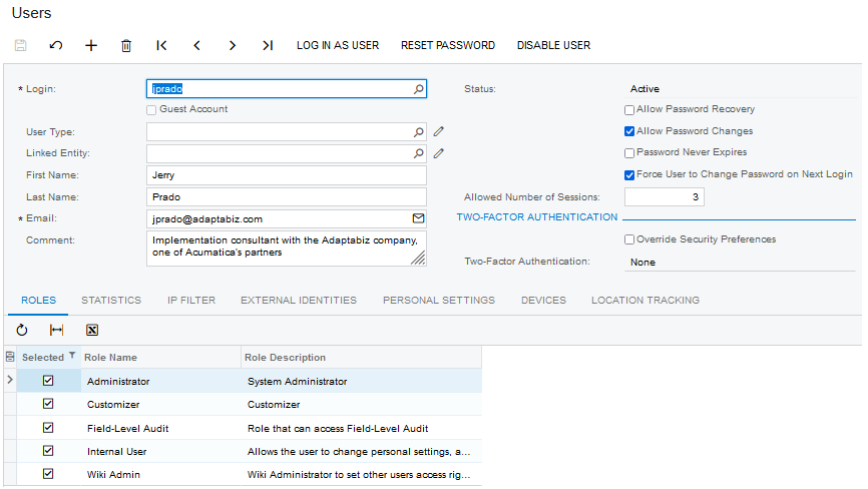


Figure: Custom alert message for incorrect password

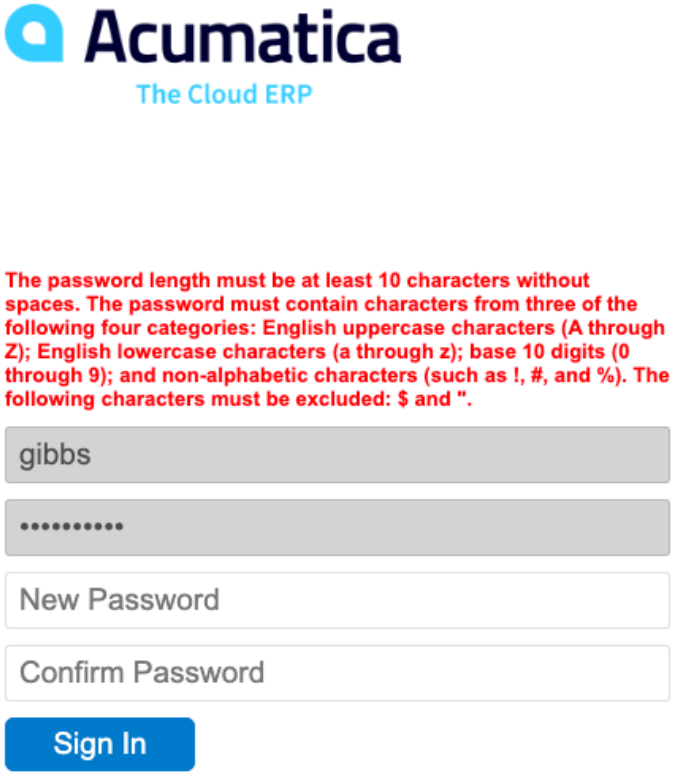
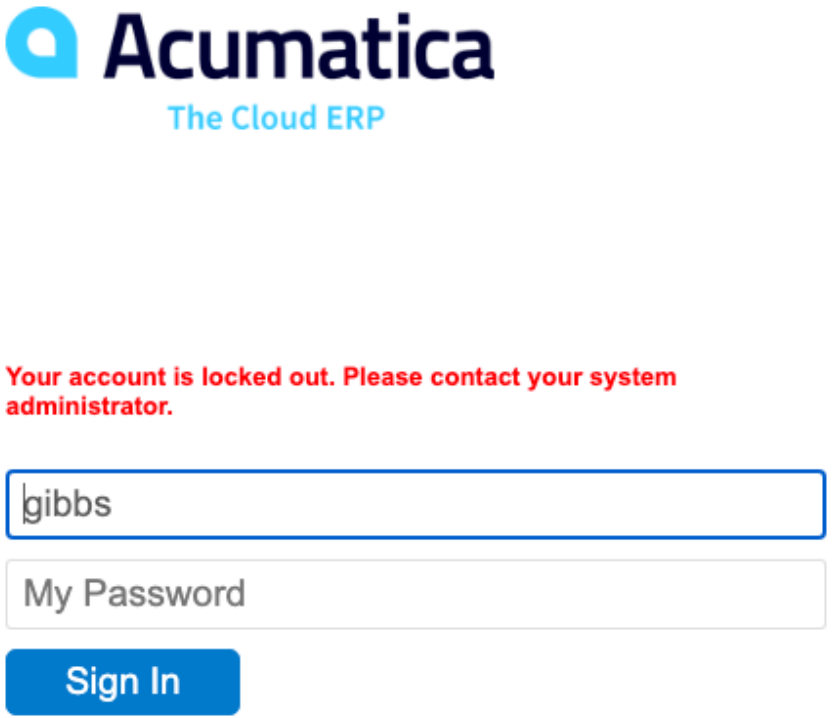


Figure: Account lockout alert message



Day 2

Devil's Peak Brewing Company
Acumatica Customer Since 2016

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 PROPAGADED 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_Access 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 Auditor
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-Branch 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*

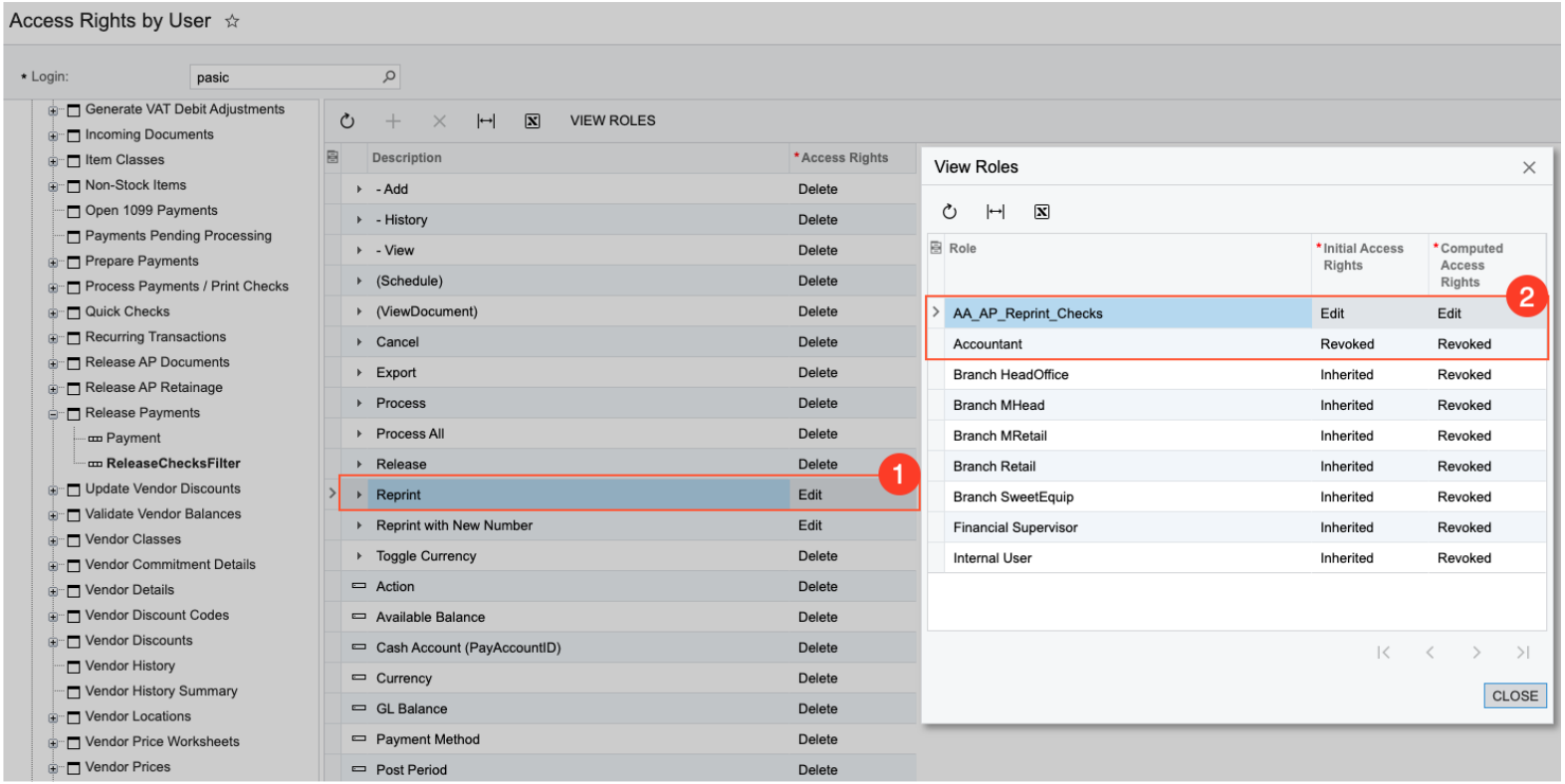
Steps :

(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



User Roles: To Modify Access Rights for a Copied Role

Story

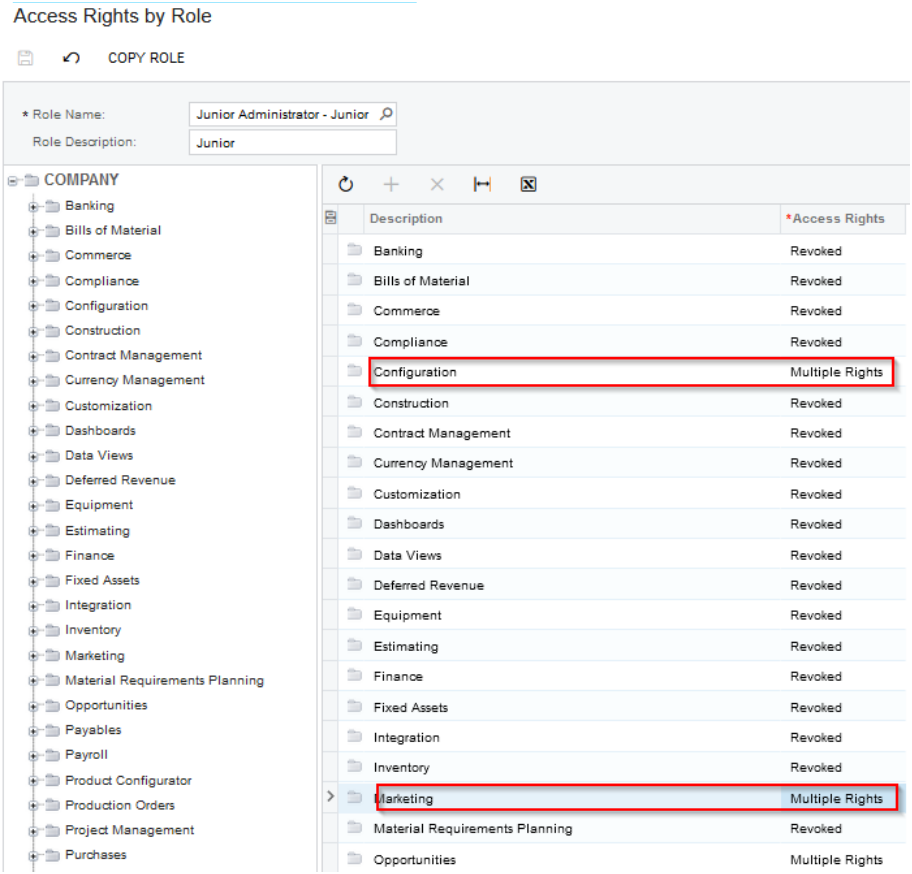
Suppose that due to the company's growth you, as a system administrator, now have an assistant. Initially, the assistant will help you with the creation of user accounts for the new employees. Then you will decide what other responsibilities the assistant will have. To accommodate the assistant's current 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



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 polices. 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)

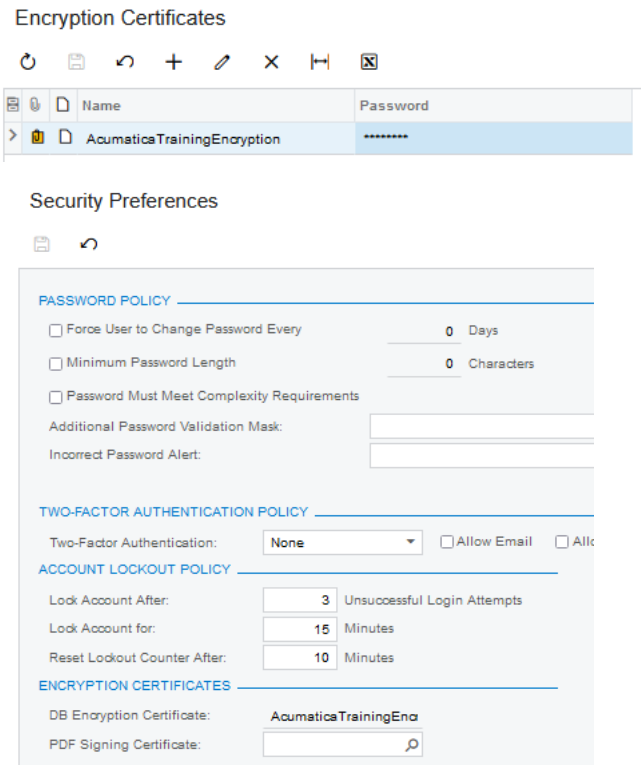
2. Encrypt the Database : Open Certificate Replacement form, specify new Certificate and click Replace Certificate.

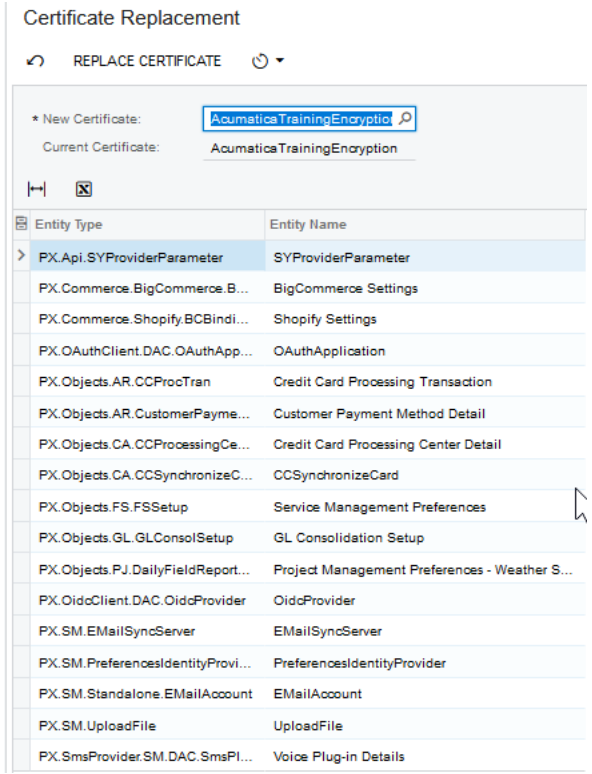
3. Removal of Outdated Certificates : Open Encryption Certificates (SM200530) and click Delete Row.

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 polices. You, as a system administrator, were requested to configure the replacement.





Day 3

Cherrylake, Inc.
Acumatica Customer Since 2013

Acumatica
The Cloud ERP

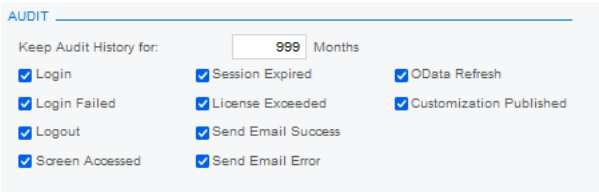
Lesson 3.1: Using System-Wide Security Auditing

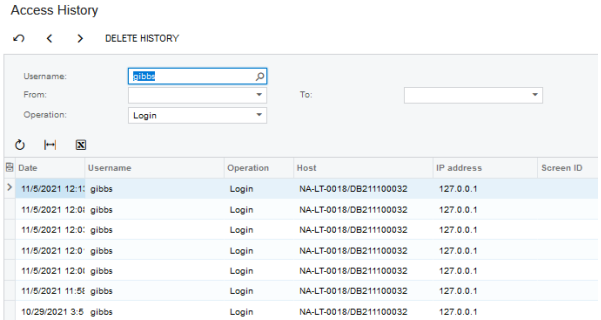
Learning Objectives

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



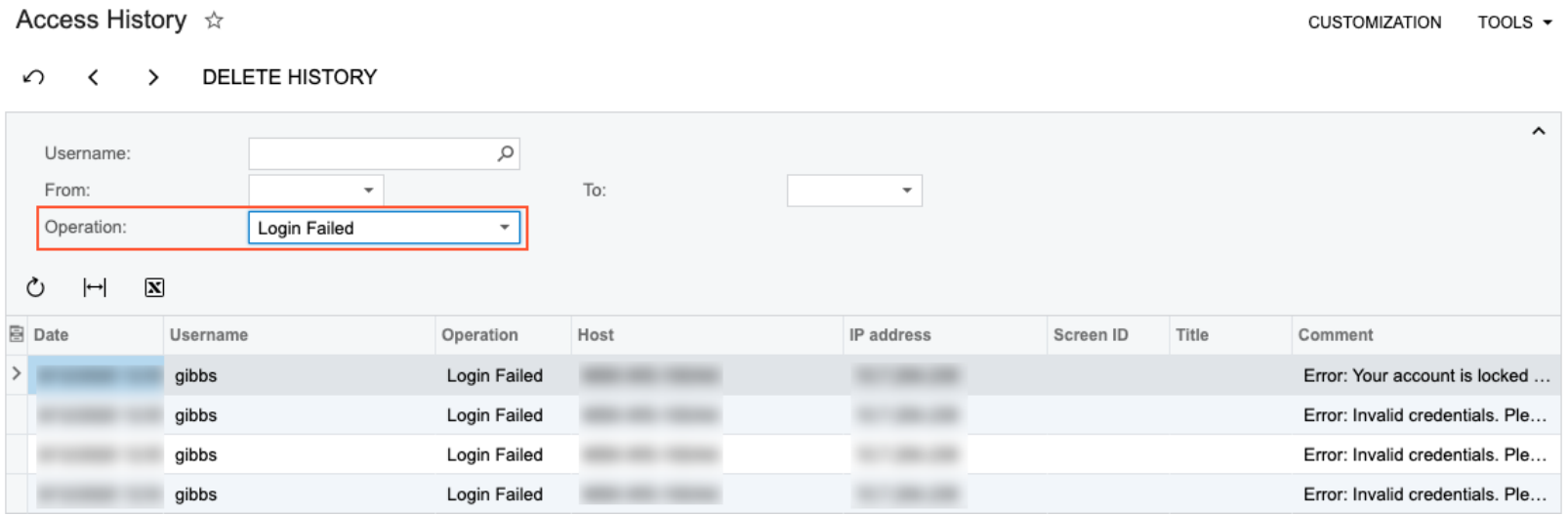


System-Wide Security Auditing: Process Activity

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



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

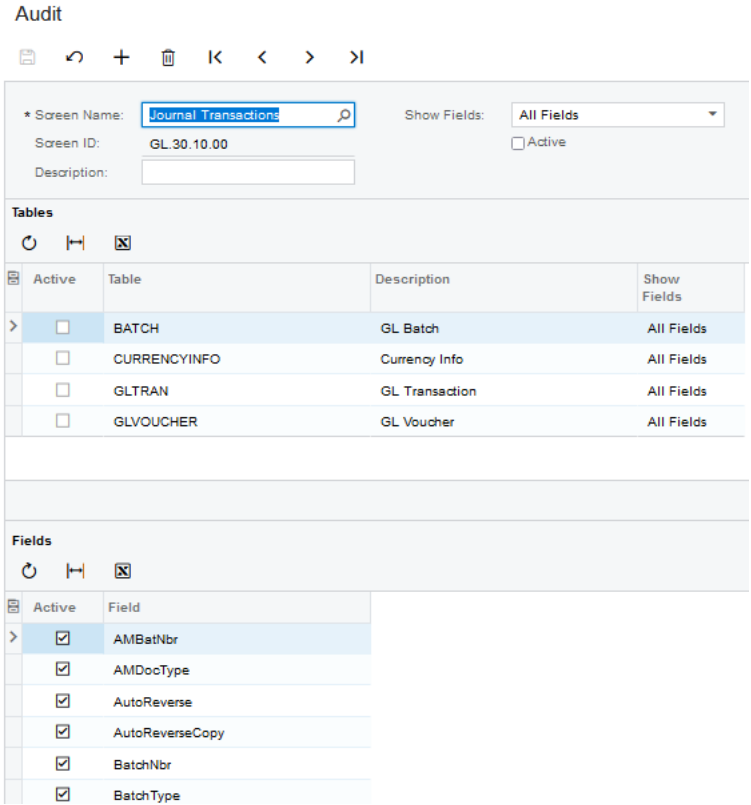
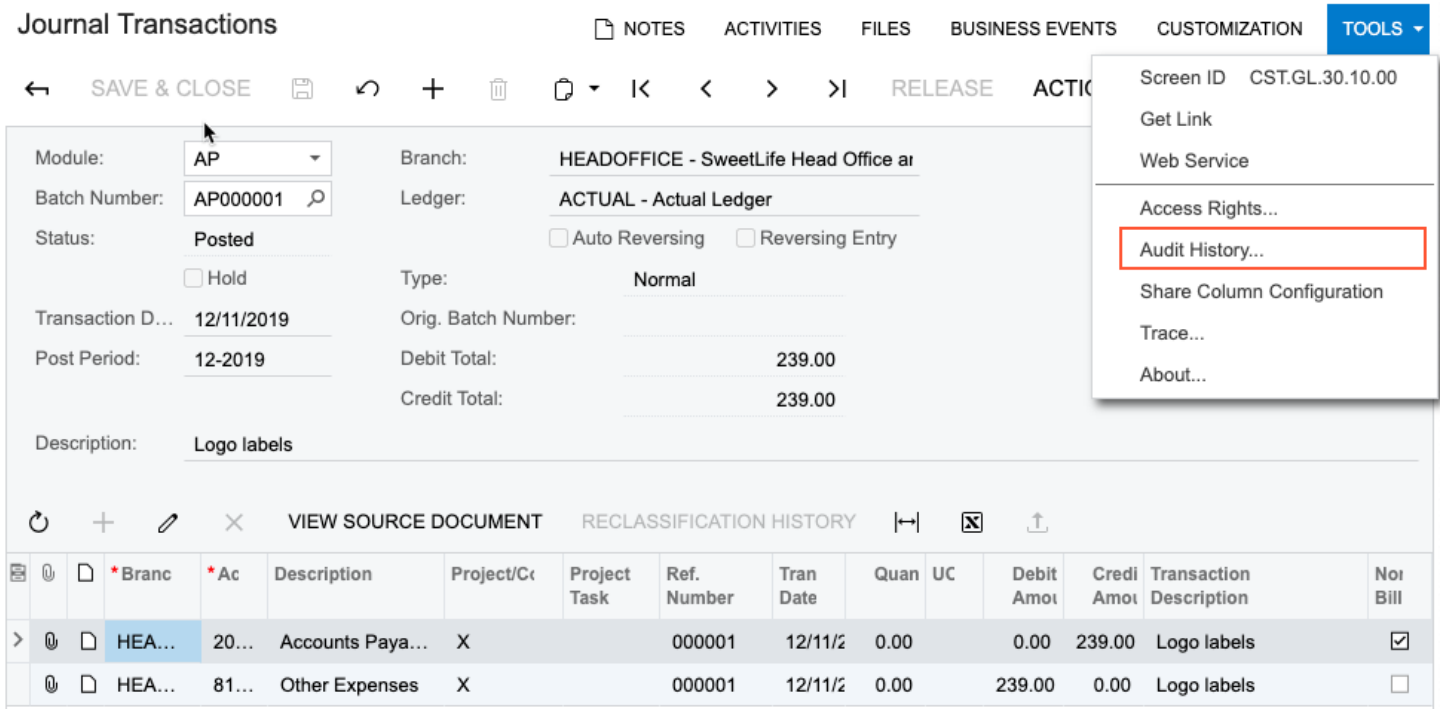


Figure: The available Audit History command for the Journal Transactions form



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

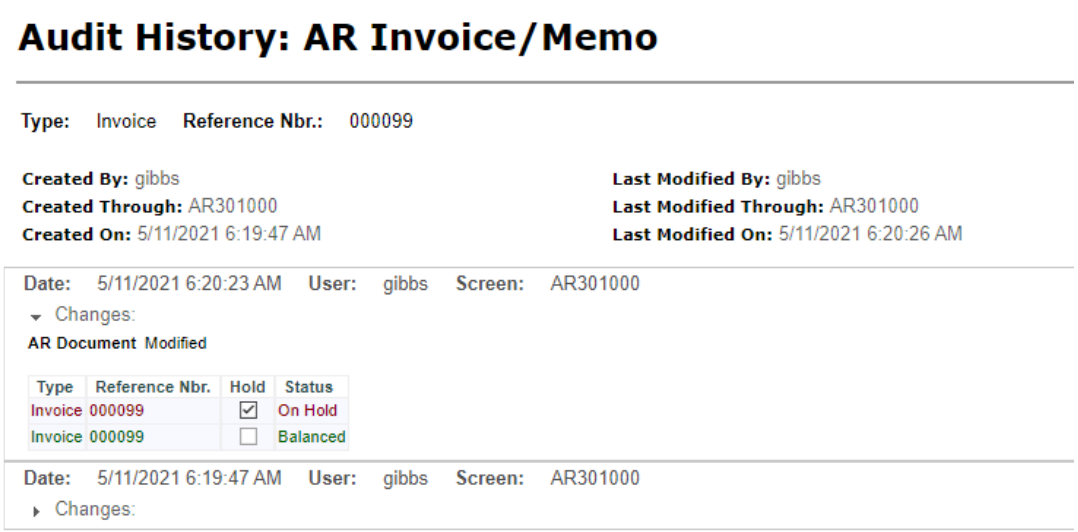
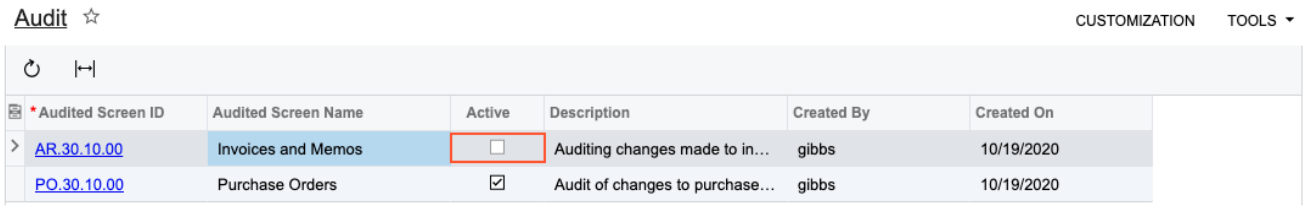


Figure: The cleared Active check box for the Invoices and Memos form



Field-Level Auditing: Process Activity

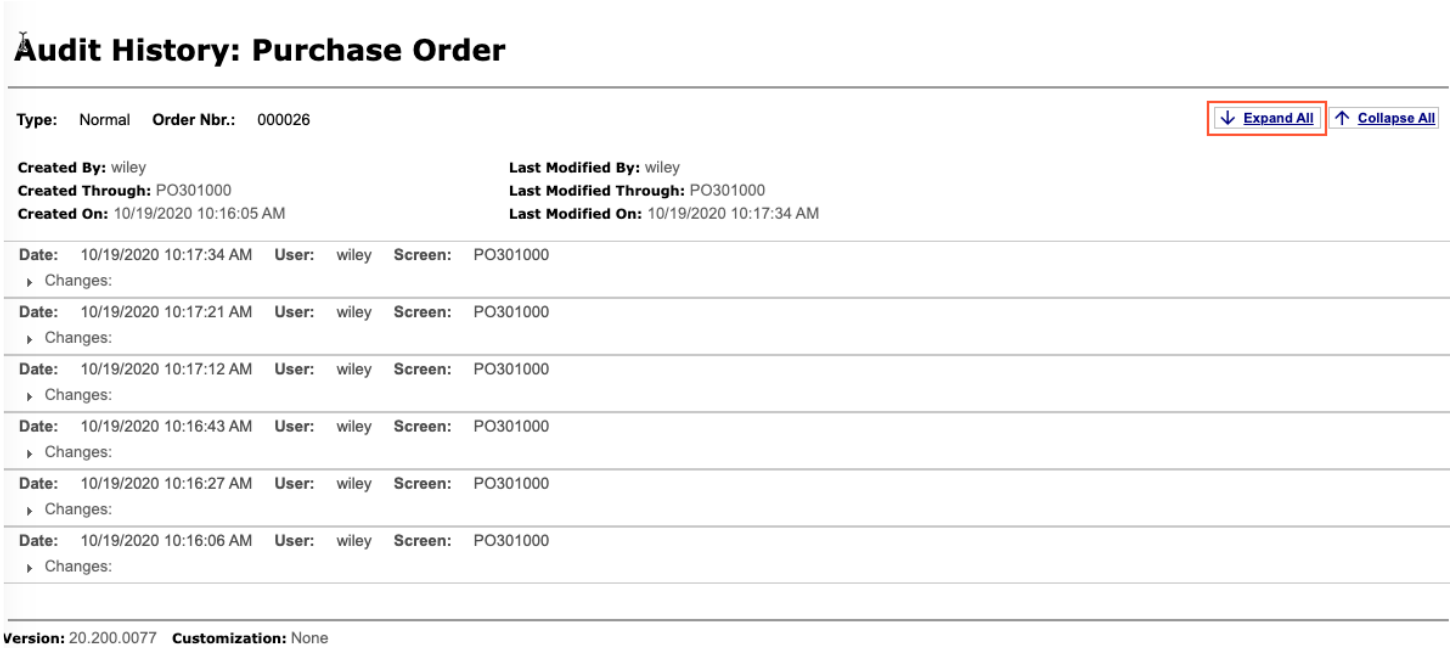
Story

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
Created Through: PO301000
Created On: 10/19/2020 10:16:05 AM

Last Modified By: wiley
Last Modified Through: PO301000
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

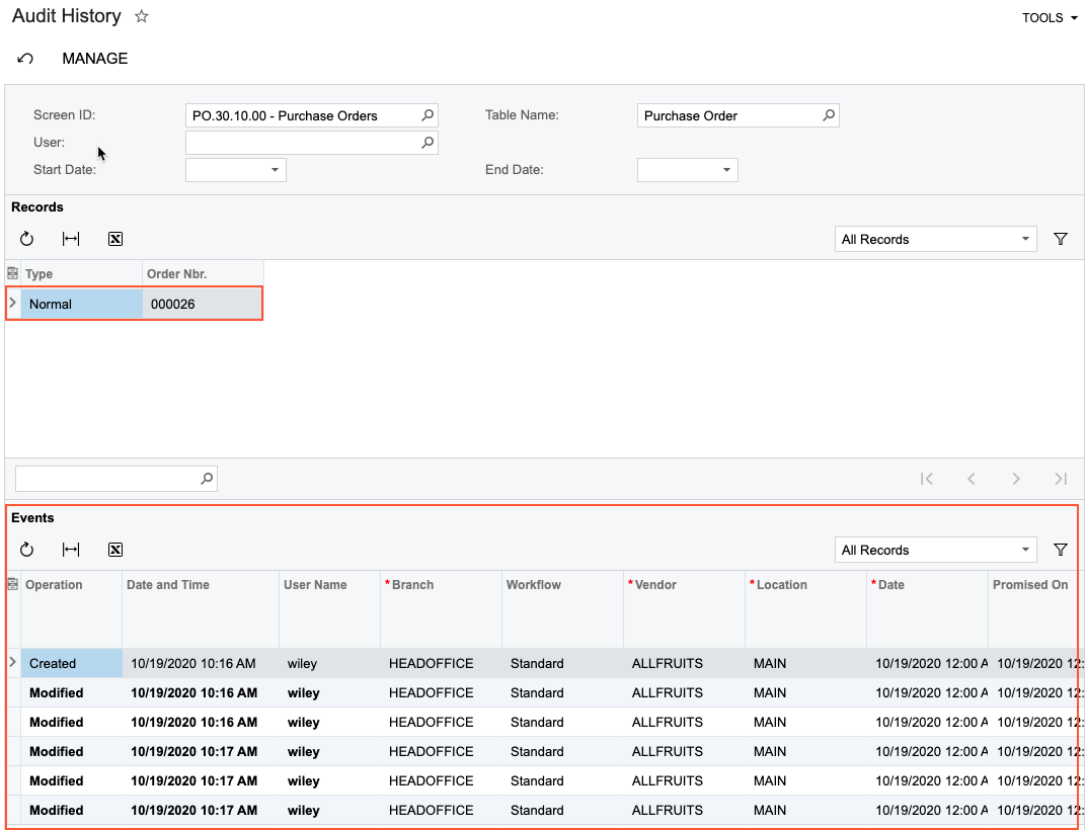
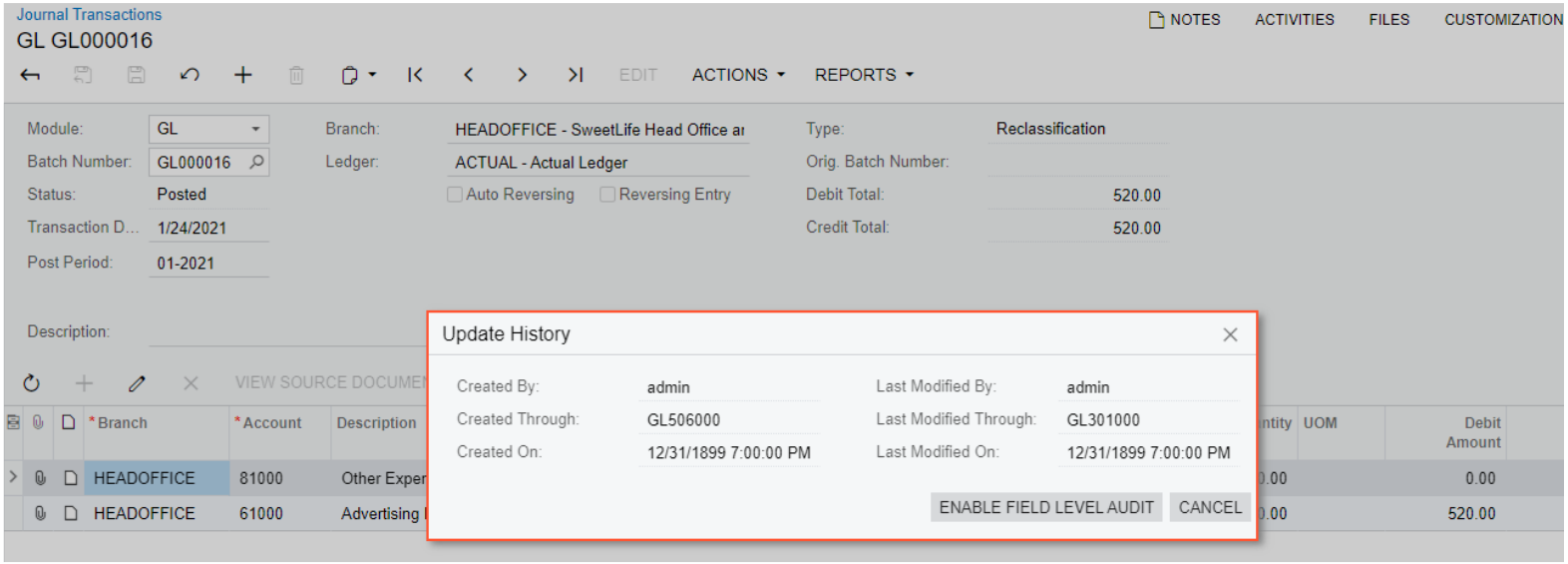


Figure: General information about a document



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

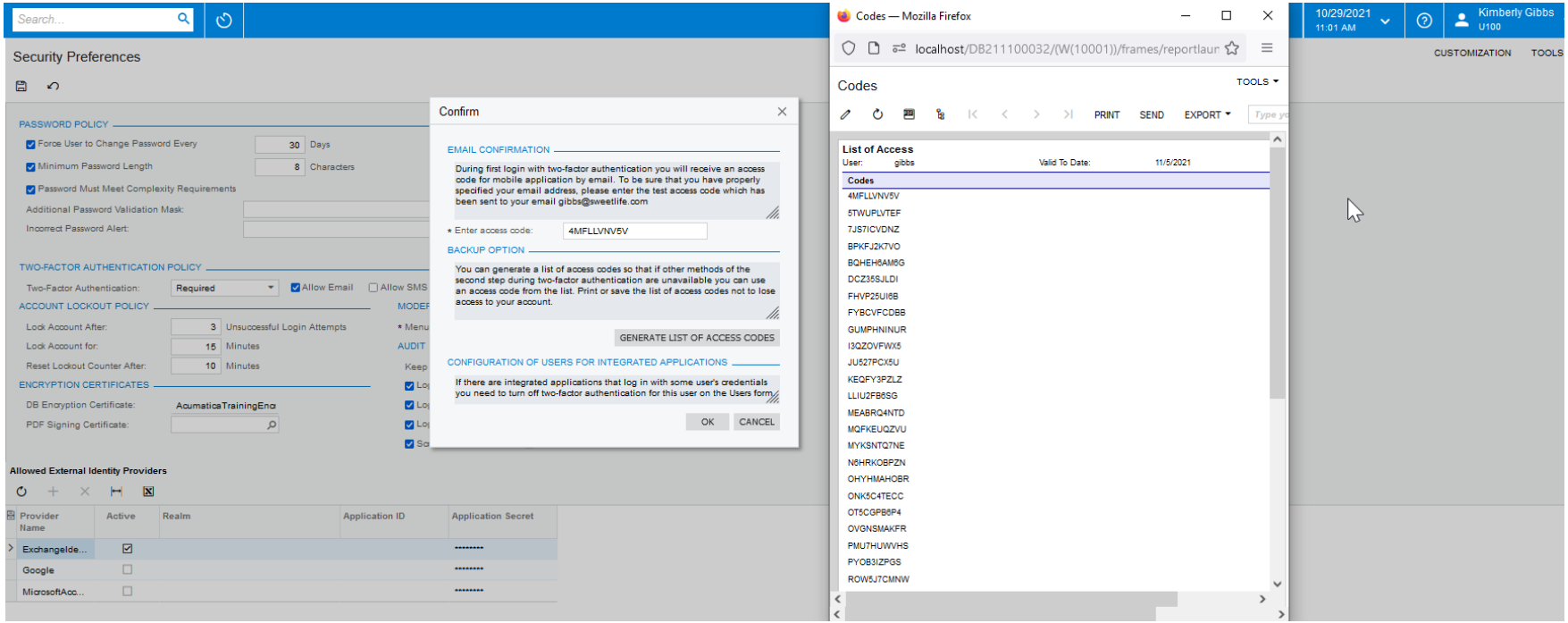


Figure: The default authentication method

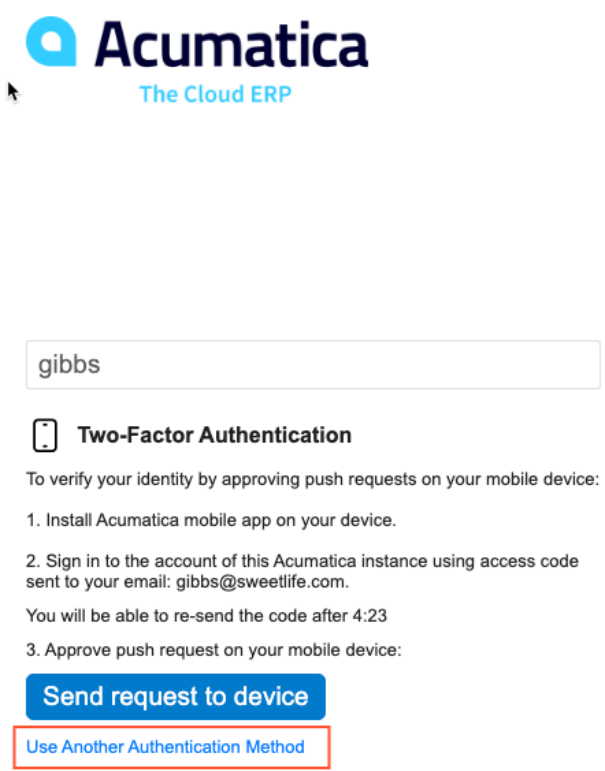


Figure: The available authentication methods

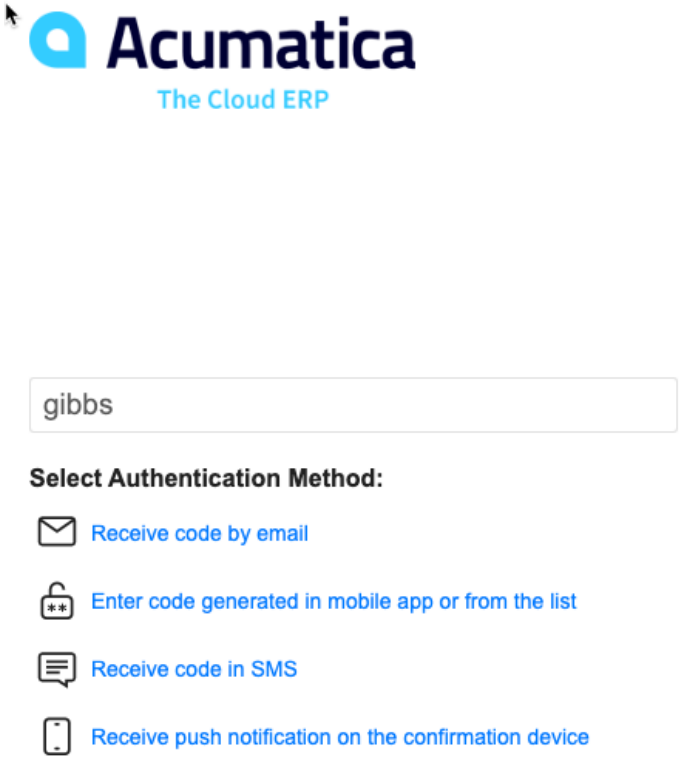


Figure: Generation of an access code by using the mobile app

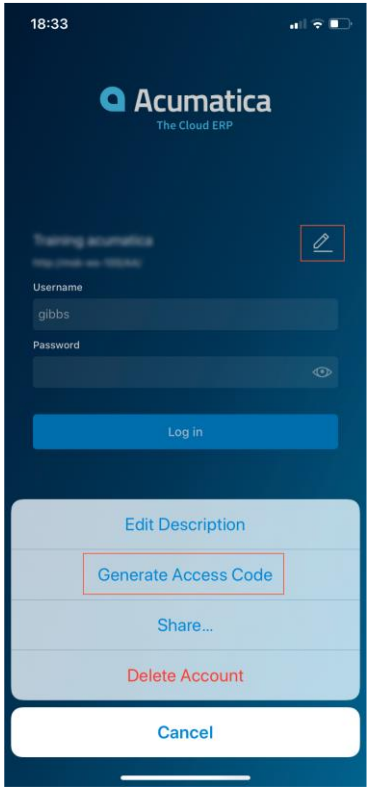


Figure: An approval request sent by the system as a push notification

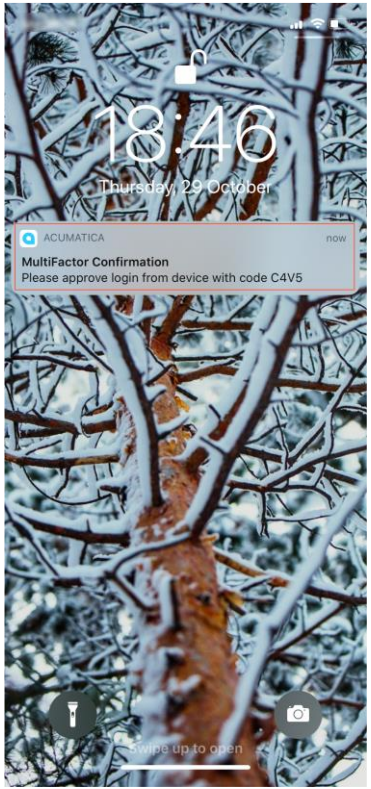


Figure: The Approve button in the Acumatica mobile app

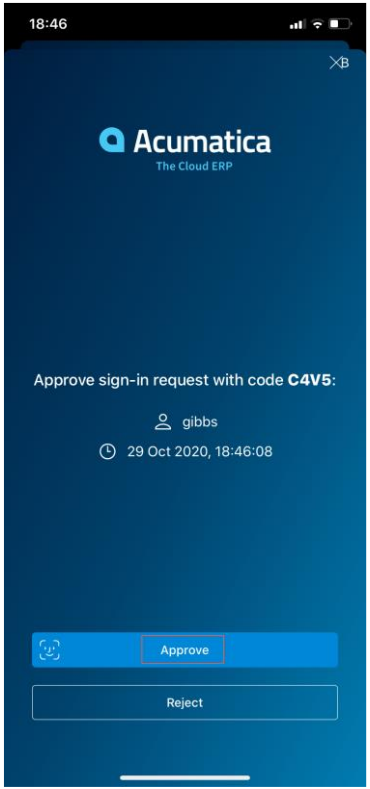


Figure: Access code entered on the first sign-in to the mobile app

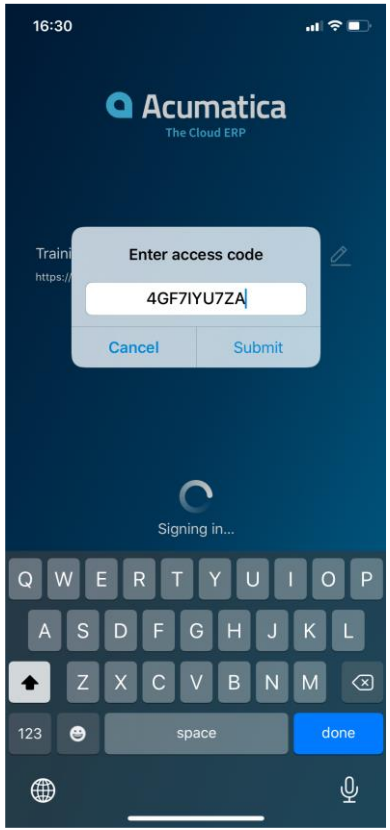
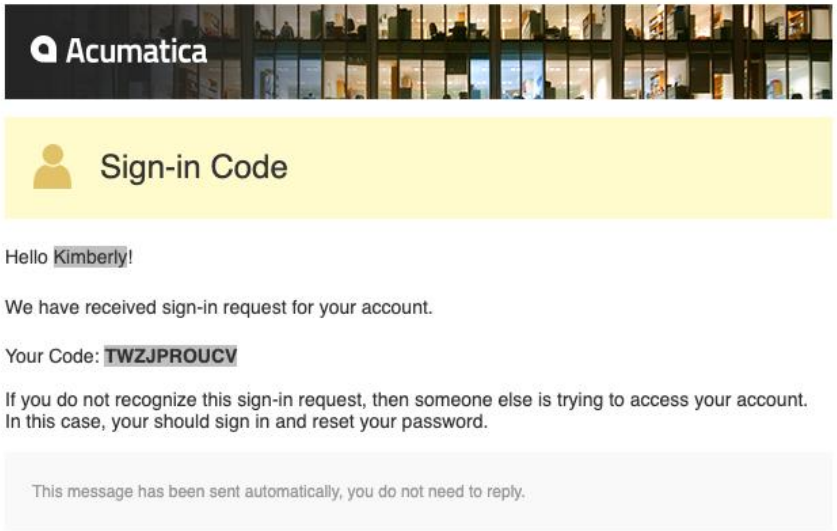


Figure: Sample email with an access code



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.

Acumatica
The Cloud ERP

Thank you

Vagif Tariverdiyev