

End-User Course

System Administration

System Security 2025 R1

Revision: 6/2/2025

Contents

Copyright.....	4
How to Use This Course.....	5
Company Story.....	8
Part 1: Preparing an Instance for Implementation.....	10
Preparing an Instance: General Information.....	10
Lesson 1.1: Activating Acumatica ERP and Enabling Features.....	10
Preparing an Instance: Activation and Licensing.....	11
Preparing an Instance: To Enable Features and Activate the License.....	13
Lesson 1.2: Configuring System-Wide Security.....	16
Preparing an Instance: System-Wide Security Policy.....	16
Preparing an Instance: To Configure Secure Access for Implementers.....	18
Part 2: Securing Access to the System.....	23
Lesson 2.1: Configuring User Roles.....	23
User Roles: General Information.....	23
User Roles: To Configure Roles for Four Access Tiers.....	26
User Roles: To Configure a Role with Granular Access.....	28
User Roles: To Modify Access Rights for a Copied Role.....	31
Lesson 2.2: Setting Up User Access.....	32
User Access: General Information.....	32
User Access: User Access Security.....	35
User Access: To Add a User Account.....	36
User Access: To Assign a Role to Multiple Users.....	37
User Access: To Modify Access for a User Account.....	38
Lesson 2.3: Encrypting with Digital Certificates.....	38
Digital Certificates: General Information.....	38
Digital Certificates: To Encrypt the Database.....	40
Part 3: Monitoring User Activities.....	42
Lesson 3.1: Using System-Wide Security Auditing.....	42
System-Wide Security Auditing: General Information.....	42
System-Wide Security Auditing: Process Activity	43
Lesson 3.2: Using Field-Level Auditing.....	44
Field-Level Auditing: General Information.....	44
Field-Level Auditing: Implementation Activity.....	47
Field-Level Auditing: Process Activity.....	49

Part 4: Using Multifactor Authentication Methods.....	53
General Purpose and Types of Multifactor Authentication.....	53
Lesson 4.1: Configuring Two-Factor Authentication.....	54
Two-Factor Authentication: General Information.....	54
Two-Factor Authentication: Implementation Activity.....	60
Additional Materials.....	63
Appendix 1: Preparing an Instance for Implementation.....	63
Preparing an Instance: Implementation Checklist.....	63
Appendix 2: Securing Access to the System	64
User Roles: Restriction Level Options.....	64
User Roles: Planning of Access Configuration.....	67
User Roles: Calculation of the Restriction Level for a User.....	68
User Roles: Predefined Roles.....	70
User Roles: Restrictions on Changing the Business Date.....	74
User Access: Related Reports and Forms.....	75
User Access: Mobile Devices.....	76
Digital Certificates: Implementation Checklist.....	77
Appendix 3: Monitoring User Activities.....	78
Field-Level Auditing: Implementation Checklist.....	78
Appendix 4: Using Multifactor Authentication Methods.....	79
Two Factor Authentication: Implementation Checklist.....	79
Multifactor Authentication in Acumatica ERP.....	80

Copyright

© 2025 Acumatica, Inc.

ALL RIGHTS RESERVED.

No part of this document may be reproduced, copied, or transmitted without the express prior consent of Acumatica, Inc.

3075 112th Avenue NE, Suite 200, Bellevue, WA 98004, USA

Restricted Rights

The product is provided with restricted rights. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in the applicable License and Services Agreement and in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable.

Disclaimer

Acumatica, Inc. makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Acumatica, Inc. reserves the right to revise this document and make changes in its content at any time, without obligation to notify any person or entity of such revisions or changes.

Trademarks

Acumatica is a registered trademark of Acumatica, Inc. HubSpot is a registered trademark of HubSpot, Inc. Microsoft Exchange and Microsoft Exchange Server are registered trademarks of Microsoft Corporation. All other product names and services herein are trademarks or service marks of their respective companies.

Software Version: 2025 R1

Last Updated: 06/02/2025

How to Use This Course

This end-user course introduces configuring of system security in Acumatica ERP. You will start from preparing an instance for implementation and securing user access to the system. You will also learn about monitoring of user activities and configuring two-factor authentication.

What Is in This Guide

The guide includes the *Company Story* topic, process activities, and *Additional Materials* topics, as needed. *Company Story* explains the organizational structure of the company preconfigured in the *U100* dataset, as well as the company's business processes and requirements. The primary content of a guide is configuration lessons and process lessons. Each of the process activities of the course is dedicated to a particular user scenario and consists of processing steps that you complete.



The process activities are independent and can be completed in any order.

Which Training Environment You Should Use

This course must be completed on Acumatica ERP 2025 R1. For this course, you will use the following tenants:

- An Acumatica ERP tenant without any preloaded dataset (out-of-the-box)
- An Acumatica ERP tenant with the *U100* dataset preloaded; this data set provides the preconfigured settings and entities you will need as you complete the course.

You can find detailed instructions on creating the tenants below.

What Is in a Configuration Lesson

A *configuration lesson*—that is, a lesson dedicated to the configuration of system settings and entities—provides a brief overview of the required system configuration and a description of other settings that could affect the configuration workflow.

Each configuration lesson includes at least one implementation activity that you have to complete in your Acumatica ERP instance to configure the core system settings or to prepare system entities.

What Is in a Process Lesson

A *process lesson*—that is, a lesson dedicated to the performing of a particular business process—includes a brief user scenario and a description of the process workflow. It can also include process diagrams that illustrate the user scenario supported by this process. The lesson also provides a brief overview of the settings that need to be specified and the entities that need to be prepared in the system before you start to perform this business process.

Each process lesson includes at least one process activity that you have to complete in your Acumatica ERP instance to learn how to perform the described business process.

What Is in Additional Materials

In the **Additional Materials** part, you can find the following additional information related to the lessons:

- Implementation checklists
- Additional information related to system security

What the Documentation Resources Are

The complete Acumatica ERP documentation is available on <https://help.acumatica.com/> and is included in the Acumatica ERP instance. While viewing any form used in the course, you can click the **Open Help** button in the top pane of the Acumatica ERP screen to bring up a form-specific Help menu; you can use the links on this menu to quickly access form-related information and activities and to open a reference topic with detailed descriptions of the form elements.

How to Create a Tenant with an Out-of-the-Box Company

To add to an existing Acumatica ERP instance a tenant with an out-of-the-box company, perform the following instructions:

1. Launch the Acumatica ERP instance and sign in.
2. Open the *Tenants* (SM203520) form, and click **Add New Record** on the form toolbar.
3. In the **Login Name** box, type a name to be used for the tenant.
4. On the form toolbar, click **Save**.

The system creates the tenant.

5. Sign out of the current tenant.

You are now on the Welcome page and you can sign in to the tenant you have just created.

How to Create a Tenant with the U100 Dataset

Before you complete this course, you need to add a tenant with the *U100* dataset to an existing Acumatica ERP instance. You will then prepare the tenant for completing the activities. To complete this preparation, perform the following instructions:

1. Go to [Amazon Storage](#).
2. Open the folder that corresponds to the version of your Acumatica ERP instance.
3. In this folder, open the **Snapshots** folder and download the *u100.zip* file.
4. Launch the Acumatica ERP instance and sign in.
5. Open the *Tenants* (SM203520) form and click **Add New Record** on the form toolbar.
6. In the **Login Name** box, type the name to be used for the tenant.
7. On the form toolbar, click **Save**.



When you create a system tenant, you may be signed out after its creation, depending on how many non-System tenants your Acumatica ERP instance already had:

- If you started with one non-System tenant (to which you are signed in) and you create a new one, the system signs you out to switch from single-tenant mode to multitenant mode.
- If the instance had multiple non-System tenants and you create another, it is already in multitenant mode. Instead of being signed out, you wait until the system completes the operation and then proceed.

8. On the **Snapshots** tab, click **Import Snapshot**.
 9. In the **Upload Snapshot Package** dialog box, select the *u100.zip* file, which you have downloaded, and click **Upload**.
- The system uploads the snapshot and lists it on the **Snapshots** tab of the *Tenants* form.
10. Open the [Apply Updates](#) (SM203510) form and click **Schedule Lockout**.

11. In the **Schedule Lockout** dialog box, click **OK**.
12. Open the [Tenants](#) form again.
13. On the form toolbar, click **Restore Snapshot**.
14. If the **Warning** dialog box appears, click **Yes**.
15. In the **Restore Snapshot** dialog box, make sure that the correct snapshot package is being uploaded and click **OK**. The system will restore the snapshot and sign you out.
16. Sign in to the tenant that you have just created.
17. Open the [Apply Updates](#) form again.
18. On the form toolbar, click **Stop Lockout**.

Which Credentials You Should Use

To complete the lessons, sign in as the following users with the following passwords:

1. Lesson 1.1: The *admin* username and the *setup* password (or the password provided to you by the person who did the installation)
2. Lesson 1.2: The *admin* username and the new password that you specified during the first sign-in
3. Lesson 2.1: The *gibbs* username and the *123* password
4. Lesson 2.2: The *gibbs* username and the *123* password
5. Lesson 2.3: The *gibbs* username and the *123* password
6. Lesson 3.1: The *gibbs* username and the *123* password
7. Lesson 3.2: The *reece* username and the *123* password
8. Lesson 4.1: The *gibbs* username and the *123* password

Which License You Should Use

For the educational purposes of this course, you use Acumatica ERP under the trial license, which does not require activation and provides all available features. For the production use of this functionality, you have to activate the license your organization has purchased. Each particular feature may be subject to additional licensing; please consult the Acumatica ERP licensing policy for details.

Company Story

This topic explains the organizational structure and operational activity of the company you will work with during this training.

Company Structure

The SweetLife Fruits & Jams company is a midsize company located in New York City. The company consists of the following branches:

- SweetLife Head Office and Wholesale Center: This branch of the company consists of a jam factory and a large warehouse where the company stores fruit (purchased from wholesale vendors) and the jam it produces. Warehouse workers perform warehouse operations by using barcode scanners or mobile devices with barcode scanning support.
- SweetLife Store: This branch has a retail shop with a small warehouse to which the goods to be sold are distributed from the company's main warehouse. This branch is also planning on selling goods via a website created on an e-commerce platform to accept orders online. The e-commerce integration project is underway.
- SweetLife Service and Equipment Sales Center: This branch is a service center with a small warehouse where juicers are stored. This branch assembles, sells, installs, and services juicers, in addition to training customers' employees to operate juicers.

Operational Activity

The company has been operating starting in the 01-2024 financial period. In November 2024, the company started using Acumatica ERP as an ERP and CRM system and migrated all data of the main office and retail store to Acumatica ERP. The equipment center began its operations in 01-2025 in response to the company's growth.

The base currency of the company and its subsidiaries is the US dollar (USD). All amounts in documents and reports are expressed in US dollars unless otherwise indicated.

SweetLife Company Sales and Services

Each SweetLife company's branch has its own business processes, as follows:

- SweetLife Head Office and Wholesale Center: In this branch, jams and fruit are sold to wholesale customers, such as restaurants and cafes. The company also conducts home canning training at the customer's location and webinars on the company's website.
- SweetLife Store: In the store, retail customers purchase fresh fruit, berries, and jams, or pick up the goods they have ordered on the website. Some of the goods listed in the website catalog are not stored in the retail warehouse, such as tropical fruits (which are purchased on demand) and tea (which is drop-shipped from a third-party vendor).
- SweetLife Service and Equipment Sales Center: This branch assembles juicers, sells juicers, provides training on equipment use, and offers equipment installation, including site review and maintenance services. The branch performs short-term service provision.

The company has local and international customers. The ordered items are delivered by drivers using the company's own vehicle. Customers can pay for orders by using various payment methods (cash, checks, or credit cards).

Company Purchases

The company purchases fruits and spices from large fruit vendors for sale and for jam production. For producing jams and packing jams and fruits, the company purchases jars, labels, and paper bags from various vendors. For

the internal needs of the main office and store, the company purchases stationery (printing paper, pens, and pencils), computers, and computer accessories from various vendors.

The company also purchases juicers and juicer parts from large juicer vendors, and it either purchases the installation service for the juicers or provides the installation service on its own, depending on the complexity of the installation.

Part 1: Preparing an Instance for Implementation

In the lessons of this part, you will learn how to prepare an Acumatica ERP instance for implementation.

Preparing an Instance: General Information

When you install a new blank instance of Acumatica ERP, the product features are disabled and the Acumatica ERP instance is in trial mode. To start implementation, you need to activate the instance by enabling the default set of features. Then you apply the license and enable any purchased features that are not in the default set. We also recommend that you configure system-wide security policies and create user accounts for every person who will be involved in further implementation to secure access to the system and track the activities performed by the people who access the system.

Learning Objectives

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

Applicable Scenario

You prepare an instance when you initially implement Acumatica ERP.

Workflow of Instance Preparation

To prepare a new blank instance of Acumatica ERP for further implementation, you perform the following general steps:

1. You sign in to the instance for the first time and enable the standard set of features on the [Enable/Disable Features](#) (CS100000) form. For details, see [Preparing an Instance: Activation and Licensing](#).
2. You apply the license you have obtained by creating a support case through the [Partner Portal](#). For details, see [Preparing an Instance: Activation and Licensing](#).
3. You configure system-wide security policies and create user accounts for people to be involved in the implementation process. For details, see [Preparing an Instance: System-Wide Security Policy](#).

Lesson 1.1: Activating Acumatica ERP and Enabling Features

This lesson explains how to activate a new Acumatica ERP instance and enable features that are included in your license.

Preparing an Instance: Activation and Licensing

To start implementation, you need to activate the instance by enabling the default set of features. Then you apply the license and enable any purchased features that are not in the default set.

In this topic, you will read about the first sign-in to a new blank instance, feature enabling, and the limitations of trial and license modes.

Obtaining a License

In Acumatica ERP, you can request the purchased license by creating a support case through the [Partner Portal](#). You should specify the following settings in the case:

- **Installation ID:** The installation ID is available in the **About** dialog box of the Acumatica ERP application instance. To open this dialog box, on any Acumatica ERP form, select **Tools > About**.
- **Contract ID:** You can find this ID on your Acumatica ERP sales invoice.

After your license request is processed, you will receive a license key. Acumatica uses a licensing server to validate licenses. If the server where you installed the Acumatica ERP instance has no access to the internet, because of the Acumatica security policy, you may request a license file instead of the key.

You apply the key to your instance by clicking **Enter License Key** on the form toolbar of the [Activate License](#) (SM201510) form, enter the license key in the **Activate New License** dialog box, and click **OK**. The system contacts the licensing server and validates the license online. Each license can be used to activate a predetermined number of instances. If you reach the limit for your license, you generally will not be able to use this license. Alternatively, depending on your license settings, the system may bring up a prompt asking if you want to deactivate the license from the oldest instance.



To validate your license, the licensing server requires that port 443 be open on the computer that is running the Acumatica ERP instance where you enter the key. You may have to open port 443 if the computer has a firewall enabled.

To apply the license file, you should click **Upload License File** on the form toolbar of the [Activate License](#) form, and then select and upload the license file by using the **Upload New License File** dialog box. If you use a license file, the system validates the license without contacting the licensing server.

First Sign-In to Acumatica ERP

Preparing an instance is performed under the only active user account (*admin*) that comes with every Acumatica ERP instance. This user has sufficient access rights to perform the instance preparation.

The initial credentials for the default user account are *admin* for the username and *setup* for the password. When you try to sign in for the first time, the system requires you to change the password.

When you sign in to a new Acumatica ERP instance for the first time and attempt to navigate to any form, the system brings up the [Enable/Disable Features](#) (CS100000) form (the only form you can access), which you use to enable the default set of features. After you do this, you can access the [Activate License](#) (SM201510) form, where you can activate your license key if you want to remove the trial mode restrictions. If you want to proceed with the trial mode, you can enable any other features that are available.

Product Features

Acumatica ERP provides scalable core system functionality and offers a range of add-on features. On the [Enable/Disable Features](#) (CS100000) form, you can view and modify the list of enabled features according to your license limitations.

You must enable a feature to cause all feature-related forms and individual elements to appear in Acumatica ERP. Some features may add only additional elements to the available forms, and others may enable a workspace or a set of workspaces with multiple forms. For example, the **Projects** menu item appears on the main menu only if the *Project Accounting* feature is enabled. If you enable the *Tax Entry From GL Module* feature, it only adds additional elements to the [Journal Transactions](#) (GL301000) form, which is available with the default set of features.

The [Enable/Disable Features](#) form also displays (at the top of the form) the state of the currently selected feature set—that is, the set of functionality available in your instance of Acumatica ERP. The following states are possible:

- *Pending Activation:* The system displays this status when you access the form for the first time to enable the standard set of features. Also, the system displays the status after you click **Modify** on the form toolbar to change the selection of features. This status indicates that the current settings on the form do not reflect the actual set of functionality available in Acumatica ERP.
- *Validated:* The system displays this status when you have enabled the features selected on the form by clicking **Enable** on the form toolbar. With this status, the enabled features on the form reflect the actual functionality available in your instance of Acumatica ERP.

Before you start implementing Acumatica ERP, you may find it helpful to become familiar with the functionality to be implemented and the add-on features your organization has included in the license. For details, see [Preparing an Instance: Acumatica ERP Features](#).



You can also use the [Enable/Disable Features](#) form to disable individual features in Acumatica ERP. We recommend that you *not* disable any feature after it has been enabled and used in the live system; this may cause unexpected results, including data loss.

Trial and License Modes

By default, Acumatica ERP is installed in trial mode. Although all features are available in this mode, the mode has the following restrictions:

- You can create no more than 10 tenants per instance.
- All tenants that you create are assigned the *Test Tenant* status. For details, see [Tenants: General Information](#).
- A watermark is added to all printed forms and reports.
- Only two conventional users can concurrently use the system.



Conventional users are users who can sign in by using their usernames and passwords on the Acumatica ERP Sign-In page, through the mobile application, or via the single sign-on page if SSO with Google or Microsoft Account has been set up.

Each time a third conventional user signs in to Acumatica ERP, one of the current users is forcibly signed out. The following message is displayed at the bottom of each form: *Your product is in trial mode. Only two concurrent users are allowed.* The message is followed by the *Activate* link, which you can click to activate a license.

- Only two API users can concurrently use the system. A third API user cannot sign in to Acumatica ERP and receives an error during the sign-in attempt.



API users are users with client applications that can sign in using the contract-based REST API method, the screen-based SOAP API, or the OAuth 2.0 authorization mechanism for applications.

In trial mode, you can enable and use any feature. For a production site, you should activate the full-product license, thus running the system in license mode. After the license activation, the system hides the features that are not included in your license on the [Enable/Disable Features](#) (CS100000) form, and you will not be able to enable these features.

When you obtain the license for using Acumatica ERP and apply this license to an instance, the trial mode restrictions are removed. The license defines the license tier (that is, the level of resources that you can use by using the license) and the set of features you can enable for the instance. For details on license tiers, see [Typical Hardware and Virtual Machine Configurations for PCS and PCP Licenses for the Acumatica ERP Installation](#).



During licensing and activation, the application instance is restarted. When you apply a license to a non-testing environment, make sure that all users of your website are warned about the restart of the site so that they can save all work in progress.

Preparing an Instance: To Enable Features and Activate the License

In the following activity, you will learn how to enable features in Acumatica ERP, activate the license, and review the license information.

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.

Process Overview

To begin using the system after the installation, you will use the [Enable/Disable Features](#) (CS100000) form to enable the standard set of features, which gives you the ability to access the [Activate License](#) (SM201510) form. When you enable the features, you are still in trial mode. To remove the restrictions of the trial mode, you need to activate the license and enable the features that you bought in addition to the standard set.

System Preparation

Before you perform the steps of this activity, make sure that the following tasks have been performed:

1. You have installed an unlicensed Acumatica ERP instance in a tenant without any preloaded dataset (out-of-the-box).
2. You make sure that the port 443 is open on the computer that is running the Acumatica ERP instance. You may have to open port 443 if the computer has a firewall enabled.
3. You have signed in to Acumatica ERP with the following credentials:
 - Username: *admin*
 - Password: *setup* or the one provided to you by the person who did the installation



When you sign in for the first time, the system requires you to change the password.

Step 1: Enabling Features for the First Time

To enable features in Acumatica ERP for the first time, do the following:

1. Open the [Enable/Disable Features](#) (CS100000) form.

Notice that a number of features are selected by default and the activation status is *Pending Activation*, as shown in the following screenshot.

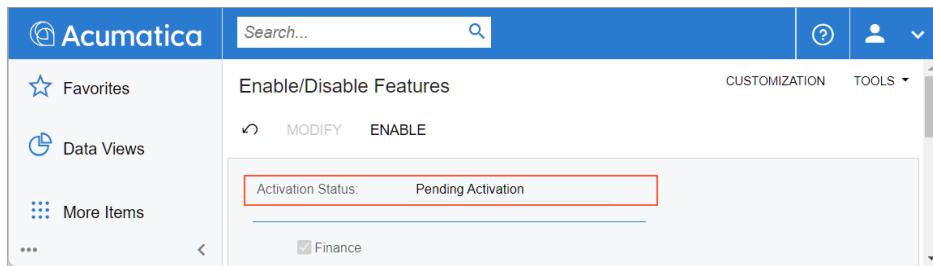


Figure: Activation status of initial features

2. On the toolbar, click **Enable** to activate the selected features.

The activation status of the currently selected set of features is now *Validated*. On the main menu (the panel on the left side of the screen), notice that new workspace menu items (**Time and Expenses**, **Finance**, **Banking**, **Payables**, and **Receivables**) have appeared that correspond to the features you have enabled, as the following screenshot demonstrates. You can now navigate to the forms in these workspaces.

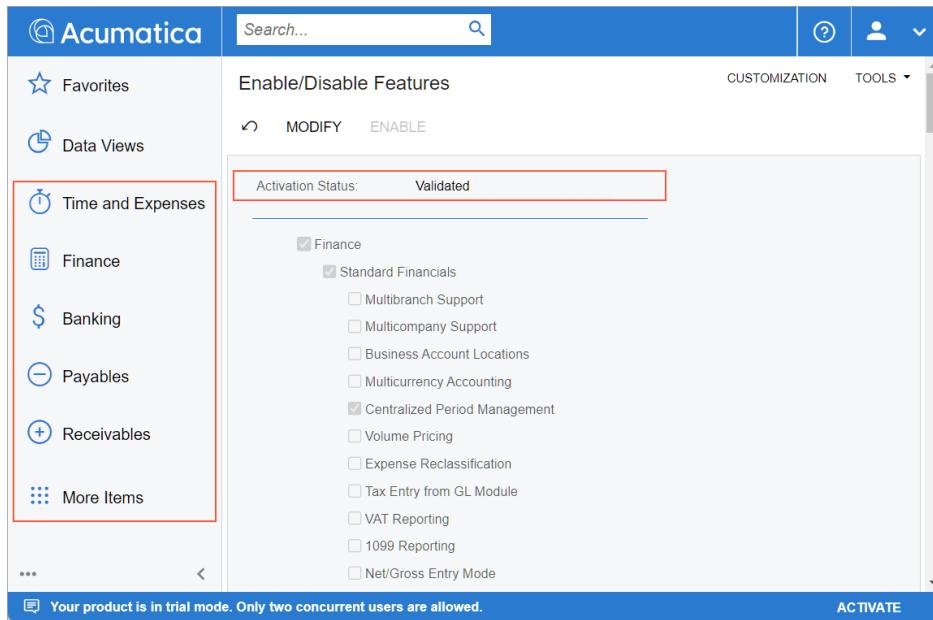


Figure: Activation status of the enabled features

Step 2: Activating the License

To activate the license, do the following:



Before you proceed with license activation on a real website, make sure that all Acumatica ERP users have saved their work and signed out of the system. During license activation, the Acumatica ERP instance will be restarted, and any unsaved work will be lost.

1. Open the [Activate License](#) (SM201510) form and do the following:
 - a. On the form toolbar, click **Enter License Key**.
 - b. In the **Activate New License** dialog box, enter the 918B-A728-0569-7FC6-D058 license key.
 - c. Click **OK** at the bottom of the dialog box.

The system contacts the licensing server and validates the license online.



The license key used in this activity is for training purposes only. The license will be deactivated in 24 hours and the instance will return to the trial mode. The license can be applied to an instance only once.

2. In the **Agree to Proceed** dialog box, which opens, click the link to read the software license agreement, and if you agree to the terms of the agreement, click **Agree** to proceed with activation. The dialog box will close.
3. In the Summary area of the form, review the license status (*Valid*), its validity period, and the number of users and tenants.
4. In the table, review the features that this license supports.



You can use the column filter for the **Activated** column to filter activated features.

5. On the form toolbar, click **Apply License** to activate your license, and the system will restart the instance.

Step 3: Enabling Additional Features

To enable additional features in Acumatica ERP, do the following:

1. Open the [Enable/Disable Features](#) (CS100000) form.
- Notice that the list of features is narrowed to the features allowed by the applied license.
2. On the form toolbar, click **Modify**.
3. In the list of features, select the check box next to the **Inventory and Order Management** feature.
4. On the toolbar, click **Enable** to activate the selected features.

The status of the currently selected feature set is now *Validated*. On the main menu, notice that new workspace menu items (**Sales Orders**, **Purchases**, and **Inventory**) have appeared that correspond to the feature you have enabled. You can now navigate to the forms in these workspaces.

Step 4: Reviewing the License Information

To review the license information—which includes the license status and limitations, statistics about the commercial transactions, warnings, and statistics for constraints—do the following:

1. Open the [License Monitoring Console](#) (SM604000) form.
2. On the **License** tab, which is shown in the screenshot below, review the information about your license.
 - In the **License Status** read-only box, verify that the license status is *Valid*, which means that the instance is licensed and has been activated.
 - In the **License Details** section, review the instance limitations.

- In the **Recommended Maximums** section, notice that the value in the **Concurrent Users** box is set to 3. This means that three users can work in the system at the same time.

The screenshot shows the 'License Monitoring Console' interface. At the top, there are tabs for 'LICENSE', 'STATISTICS', 'WARNINGS', and 'CONSTRAINT HISTORY'. On the right, there are 'CUSTOMIZATION' and 'TOOLS' dropdowns. The main area has sections for 'LICENSE STATUS' (Valid), 'LICENSE TIER' (S1 - Select for General Business), '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), and '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 Lines per Transaction: 1000, Maximum Number of Serial Numbers per Document: 2000, Maximum Number of Employees Paid by Month: 0). The 'Concurrent Users' field is highlighted with a red border and contains the value '3'.

Figure: License Monitoring Console

Lesson 1.2: Configuring System-Wide Security

This lesson explains how to configure your company initial security policy and create user accounts for the people involved in the implementation.

Preparing an Instance: System-Wide Security Policy

Acumatica ERP provides a wide range of tools for security control. You can implement your organization's security regulations by configuring and maintaining system-wide security policies for user accounts, passwords, and security auditing.

In this topic, you will read about the tools we recommend that you use for ensuring that access to your tenant in implementation is secure.

User Accounts for Implementers

Initially, the only active user account (*admin*) is available for signing in to a new instance. We do not recommend using this account for implementation purposes, however. The account should be used only for activating and licensing the instance and configuring secure access for the people involved in the implementation.

The system implementation usually involves third-party implementation consultants as well as people from your company who are assigned to the implementation project. We highly recommend creating user accounts for everyone involved in the process to ensure that access is secure and that only authorized people access the system.

In Acumatica ERP, access to information is controlled primarily by the roles assigned to the user who signs in to the system. Roles generally correspond to particular job assignments or functions of groups of users. When they sign in, the users authenticate themselves by using the appropriate username and password, and the associated roles determine which system resources they may access.

You add user accounts for people involved in the implementation by using the [Users](#) (SM201010) form. For each user, you specify at minimum the username, the initial password (to be changed on the first sign-in), and the email address. Implementers should be able to access all system resources to implement the system. To allow this, you need to assign these users a set of predefined roles that allows access to all system resources.

At this point, a system email account is not configured yet, and you need to find a secure way to pass user credentials (username and initial password) to the people.

System-Wide Password Policies

In Acumatica ERP, you can use the [Security Preferences](#) (SM201060) form to set up the password policies for all user accounts defined in the system.



If your Acumatica ERP instance is integrated with Active Directory, the password policy for domain users is set at the domain level through Active Directory. For more information about the integration of Acumatica ERP with Active Directory, see [Integration with Active Directory](#).

You can set up the system password policy to control the following:

- *Password duration:* For maximum security, we recommend that users change passwords periodically, such as every 90 to 180 days. Shorter ranges can reduce the security of accounts, because users may use simple passwords or struggle to create complex, memorable passwords often, which encourages them to write down these passwords. You use the **Password Expiry Period in Days** check box to specify the change frequency.
- *Password length:* You can set up a minimum required password length. You use the **Minimum Characters in Password** check box to specify the minimum length.
- *Password complexity:* You can enforce password complexity requirements, which means that a new password must include at least three of the following:
 - Latin uppercase letters (A–Z)
 - Latin lowercase letters (a–z)
 - Digits (0 through 9)
 - Special characters (such as +, :, =, and -)

You use the **Password Must Meet Complexity Requirements** check box to enforce complexity requirements.

- *Password validation mask:* You can configure an additional password validation mask to enforce your company's password policy. You can specify a regular expression to enforce additional regulations—for example, to exclude some special characters that are not supported by third-party software (if used).

You can use a validation mask in addition to password length or complexity requirements or use only your validation mask and clear the length or complexity requirements. For example, the following regular expression covers length and complexity requirements and forbids the \$ and ^ symbols: ^ (?=. * [A-Za-z]) (?=. * \d) (?=. * [@ ! % * # ? &]) [A-Za-z \d @ ! % * # ? &] { 10 , } \$. With this validation mask, there is no need to set up password length and complexity settings.

If you use a validation mask, you should provide a custom alert message that explains to users the password policy enforced by the validation mask. Otherwise, the system displays the default message.

You use the **Additional Password Validation Mask** and **Incorrect Password Alert** boxes to configure custom password requirements.

To improve password security, a hashing algorithm is used to process passwords, and only hash values are stored in the database.

System-Wide Account Lockout Policies

You can configure the system to lock out a user account after a particular number of failed sign-in attempts. This configuration option helps to stop an unauthorized person who might be trying to gain system access by guessing a user's password.

On the [Security Preferences](#) (SM201060) form, you can specify the following system-wide parameters:

- The number of failed sign-in attempts that will cause a user account to be locked out

- The duration of the account lockout—that is, the number of minutes the user account remains locked before the system automatically unlocks it
- The time period before the system resets the counter of the failed sign-in attempts.

Preparing an Instance: To Configure Secure Access for Implementers

In the following activity, you will learn how to configure system-wide password and lockout policies and how to create user accounts 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.
- 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

Process Overview

To configure system-wide security policies, you will use the settings on the [Security Preferences](#) (SM201060) form. To meet character exception requirements, you will use a validation mask in addition to the password length and complexity requirements, and set up a custom alert message for incorrect passwords.

Then you will add the requested user accounts on the [Users](#) (SM201010) form. You will use your user account to validate the configured policies.

System Preparation

Before you perform the steps of this activity, make sure that the following tasks have been performed:

1. You have installed an Acumatica ERP instance with a tenant without any preloaded dataset (out-of-the-box).
2. You have signed in to Acumatica ERP with the following credentials:
 - Username: *admin*
 - Password: The new password that you specified during the first sign-in
3. You have enabled the default set of features on the [Enable/Disable Features](#) (CS100000) form, as described in [Preparing an Instance: To Enable Features and Activate the License](#).

Step 1: Configuring the Password Policy

To configure the system-wide password policy, do the following:

1. Open the [Security Preferences](#) (SM201060) form.
2. In the **Password Policy** section of the form, select the **Password Expiry Period in Days** check box, and type 180 into the box next to it.
3. Make sure that the **Password Expiry Period in Days** check box is selected, and type 10 into the box next to it.
4. Make sure that the **Password Must Meet Complexity Requirements** check box is selected, which will force users to use complex passwords with uppercase letters, digits, and special characters.
5. In the **Additional Password Validation Mask** box, type the following regular expression:

```
^(?!.*[$ "]).*$
```

The expression verifies that the entered password has no spaces and does not contain the \$ or " character.

6. In the **Incorrect Password Alert** box, type the following text: 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 ".



The box is expandable; you may want to adjust its size to be able to view the entire message.

7. On the form toolbar, click **Save**.

Step 2: Reviewing Account Lockout Policies

While you are still on the [Security Preferences](#) (SM201060) form, in the **Account Lockout Policy** section, review the following default values inserted by the system and make sure that they match the organization's account lockout policies:

- **Failed Sign-In Attempts Before Account Lockout:** 3
- **Account Lockout Duration (Minutes):** 15
- **Reset Interval for Failed Sign-In Attempts (Minutes):** 10

Step 3: Adding User Accounts

To add user accounts to the system, do the following:

1. On the [Users](#) (SM201010) form, add a new record.
2. In the **Login** box of the Summary area, type gibbs.
3. Clear the **Generate Password** check box.
4. In the **Password** box, type Welcome123.
5. Specify the following user information:
 - **First Name:** Kimberly
 - **Last Name:** Gibbs
 - **Email:** gibbs@sweetlife.com

- **Comment:** Senior system administrator
6. Specify the following settings to configure individual password policy:
 - **Allow Password Recovery:** Cleared
 - **Allow Password Changes:** Selected
 - **Password Never Expires:** Cleared
 - **Force User to Change Password on Next Login:** Selected
 7. On the **Roles** tab, assign the following roles to the user by selecting the check box in the **Selected** column:
 - *Administrator*
 - *Customizer*
 - *Field-Level Audit*
 - *Internal User*
 - *Wiki Admin*
 8. On the form toolbar, click **Save**.
 9. Click **Add New Record** on the form toolbar to add one more user, and specify the following settings in the Summary area:
 - **Login:** prado
 - **Generate Password:** Cleared
 - **Password:** Welcome123
 - **First Name:** Jerry
 - **Last Name:** Prado
 - **Email:** jprado@adaptabiz.com
 - **Comment:** Adaptabiz implementation consultant
 - **Allow Password Recovery:** Cleared
 - **Allow Password Changes:** Selected
 - **Password Never Expires:** Cleared
 - **Force User to Change Password on Next Login:** Selected
 10. On the **Roles** tab, assign the following roles to the user by selecting the check box in the **Selected** column:
 - *Administrator*
 - *Customizer*
 - *Field-Level Audit*
 - *Internal User*
 - *Wiki Admin*
 11. On the form toolbar, click **Save**.

Step 4: Verifying the Password Policy

To verify the configured password policy, do the following:

1. In the top right corner of the screen, click the *admin admin* username, and then select **Sign Out**.
2. On the Sign-In page, enter gibbs as the username and Welcome123 as the password. The system requests that you enter and confirm a new password.
3. Enter welcome"123 as the new password and its confirmation, and click **Sign In**. Because this password contains the prohibited " character, the system clears the entered values and displays the alert message that you configured, as shown in the following screenshot.

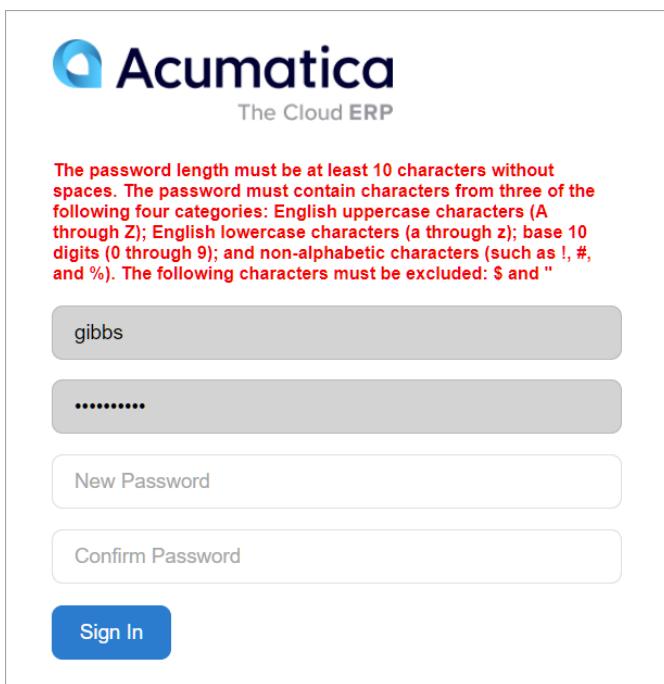


Figure: Custom alert message for incorrect password

4. Enter `123Welcome` as the new password and its confirmation, and click **Sign In**. The expression you entered complies with the password policy requirements and is accepted by the system as your new password.
5. In the top right corner of the screen, click the *Kimberly Gibbs* username, and then select **Sign Out**.

Step 5: Verifying the Lockout Policy

To verify the lockout policy you have configured, do the following:

1. On the Sign-In page, enter `gibbs` as the username and `Welcome123` as the password. The system requests that you enter valid credentials.
2. Again enter the incorrect password three more times. The system warns you that your account is locked out, as shown in the following screenshot.

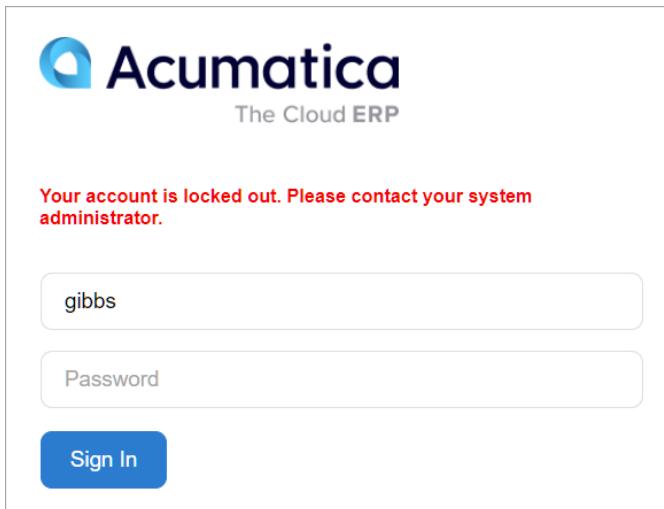


Figure: Account lockout alert message

3. On the Sign-In page, enter `prado` for the username and `Welcome123` as the password. Enter `123Welcome` as the new password and its confirmation, and click **Sign In**. You have successfully signed in as Jerry Prado.
4. Open the [Users](#) (SM201010) form.
5. In the **Login** box, select `gibbs`. In the **Status** box, notice that the user status is *Temporarily Locked*.
6. On the form toolbar, click **Unlock User**. Notice that the user status has changed to *Active*.

Part 2: Securing Access to the System

In the lessons of this part, you will learn how to configure user roles, set up user access, and use digital certificates for encryption.

Lesson 2.1: Configuring User Roles

In Acumatica ERP, you never assign access rights directly to individual users; instead, you use roles to restrict access to the system. A role is a set of access rights to system objects. You assign one role or multiple roles to each user, and based on these roles, the user is then granted the appropriate access rights to system objects.

This lesson provides details about configuring user access in Acumatica ERP.

User Roles: General Information

User roles in Acumatica ERP are sets of access rights to system objects designed for convenient management of access for users with similar responsibilities in the system. In Acumatica ERP, you can set up access rights to such a system object as a particular form, a container of form elements, a form element, or a wiki.



For details about managing access to wikis, see [Wiki Access Management](#).

Learning Objectives

In this lesson, 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

Applicable Scenarios

You create or modify user roles in the following cases:

- You, as an implementation consultant, initially implement Acumatica ERP for your client and the predefined set of roles does not suit your client's needs.
- You, as a system administrator, were notified that the security policy of your company has changed and after a revision of the current set of roles, you need to modify access rights to Acumatica ERP elements.
- You, as a system administrator, were notified about a new position being created in your company, for which the current set of roles does not cover the job description.

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.

The system objects are a particular form, a container of form elements, and a form element. In Acumatica ERP, the system objects are grouped in a tree with nodes, where a tenant is the first-level node with the workspaces nested under it. Each workspace can have multiple forms nested, which can have containers of form elements nested within it; form elements are nested within the containers.

The set of restriction levels available for the system objects depends on the object type. For some objects, you can specify a more granular level; for others, you can either allow or deny the access. For details, see [User Roles: Restriction Level Options](#).

Access Propagation and Inheritance

In Acumatica ERP, as mentioned, the system objects are grouped in a tree with nodes. Each node is a system object that can nest other objects. At each level of nodes, either access rights are propagated to the nested objects or nested objects inherit access rights from their parents. The hierarchy of nesting is the following:

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 the 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.



You can observe the tree of system objects in the left pane of forms related to user access configuration, such as [Access Rights by Screen](#) (SM201020), [Access Rights by Role](#) (SM201025), and [Access Rights by User](#) (SM201055).

The propagation and inheritance mechanism saves time for administrators and simplifies the setting of access rights to system objects. You can change the propagated or inherited rights for any object at any time—that is, change the restriction level received from a parent object. For specifics about the restriction levels of a particular system object, see [User Roles: Restriction Level Options](#).

Predefined Roles

For ease of defining and administering roles, Acumatica ERP provides a set of predefined roles, which is expanded with every major release of Acumatica ERP. We recommend that you use the predefined roles while you configure user access to the system during implementation. For details on the available predefined roles, see [User Roles: Predefined Roles](#).

With every major release of Acumatica ERP multiple new forms are added to the system. Depending on the added functionality, any number of new predefined roles can be supplied, which will provide access to the new forms, or access for existing predefined roles can be modified.

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.

If you have deleted a predefined role, the system will not restore it during the upgrade.



If a predefined role mostly works for you but needs a bit of tweaking, we strongly recommend copying the role and making needed changes to the copied role.

Role Planning

Organizations have different kinds of valuable information that needs protecting, such as financial documents and customer and vendor information. Different employees need access to different subsets of this information to perform their duties. Before you start planning the set of user roles, we recommend that you make sure that job roles and responsibilities in your company are clearly defined. The job responsibilities of a user define the needed levels of access to forms, records, and operations on the records.

While planning the set of roles, take into account the objectives of internal control procedures implemented in your company, like preventing and detecting fraud, maximizing the completeness and accuracy of financial records, safeguarding assets, and preparing financial statements in a timely manner. For example, to minimize the risk of errors and fraud, duties associated with cash handling are often segregated. Also, segregation is recommended for duties related to recording documents and further processing them, as well as conducting reconciliations and preparing financial statements.

We highly recommend that you perform the planning of access configuration when the system is initially implemented and when there have been changes to the security policy of the organization. For detailed recommendations, see [User Roles: Planning of Access Configuration](#).

Role Creation

You use the [User Roles](#) (SM201005) form to create a role. By default, the system automatically sets the access rights for a new role to Revoked for all system objects. The nested objects (containers and elements) have the *Inherited* access level.



We recommend using naming conventions for the user roles that you create or copy from predefined roles.

To set up access rights to multiple system objects for an individual role, you use the [Access Rights by Role](#) (SM201025) form.

To set up access rights to multiple system objects for multiple roles, you use the [Access Rights by Screen](#) (SM201020) form. The form allows you to see the restriction level that other roles have to a system object.

Alternatively, you can use the [Access Rights by Role](#) form to create a copy of a role, give the copied role a new name, and then modify access rights for the copied role.



The process of defining task-based roles requires in-depth knowledge of both the organization's business processes and the Acumatica ERP approach to security.

Role Access Modification

During ongoing maintenance of Acumatica ERP, you may have tasks to change users' access rights to some system objects. To modify a role's access you use either the [Access Rights by Screen](#) (SM201020) form or the [Access Rights by Role](#) (SM201025) form.

You may take different approaches in configuring user access: assigning a single role to a user or assigning a combination of roles to a user. The chosen approach may affect how modification of a role will affect an individual user's access.

If you do not use role combination, the modification of a role will affect access for all users with the role assigned. If you use role combination, the modification of role's access rights can affect users with this role differently. For details, see [User Roles: Calculation of the Restriction Level for a User](#).

Before proceeding to role modification, we recommend collecting detailed information about the role configuration and the users assigned to the role. For details on access management reports, see [User Access: Related Reports and Forms](#).

User Roles: To Configure Roles for Four Access Tiers

In the following activity, you will learn how to create user roles and specify access rights to system objects for the roles.

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.

Process Overview

To configure roles for four access tiers within the general ledger functional area, you will first prepare a spreadsheet with the list of forms of the functional area, and mark the category of each form to understand what this form is used for—configuration, data entry, processing, or reporting. Then you will add roles to the list and indicate the restriction level for each role against the form. For this activity, you will use the [GL_4Tier_Access](#) spreadsheet, which was prepared to these specifications.



The [GL_4Tier_Access](#) spreadsheet contains a limited set of the forms related to the general ledger functional area and can be used for training purposes only.

With the spreadsheet prepared, you will use the [User Roles](#) (SM201005) form to create four roles. You will use the AA prefix for the roles to have them at the top of the list, combined with _GL to indicate the functional area.

With the roles created, you will use the [Access Rights by Screen](#) (SM201020) form to set up the access rights to multiple system objects for multiple roles.

System Preparation

Launch the Acumatica ERP website, and sign in to a company with the U100 dataset preloaded. You should sign in as a system administrator, by using the gibbs username and the 123 password.

Step 1: Creating Roles

To create the needed roles in the system, do the following:

1. On the [User Roles](#) (SM201005) form, add a new record.

2. In the **Role Name** box, type AA_GL_Configurator.
3. In the **Role Description** box, type Role to access GL configuration settings.
4. On the form toolbar, click **Save**.
5. By repeating the actions performed in the previous instructions, add three more roles with the information from the following table.

Name	Description
AA_GL_Manager	Role for working with GL entities and viewing settings
AA_GL_Clerk	Role for entering and editing records
AA_GL_Auditor	Role for viewing records and reports

Step 2: Granting Access to All Forms of a Workspace

To specify the access rights to multiple roles, do the following:

1. Open the [Access Rights by Screen](#) (SM201020) form.
2. In the left pane of the form, select the **Finance** node.
3. In the right pane, locate the four roles you have created. Notice that the roles have the *Revoked* access rights for all forms within the workspace, as all newly created roles do.
4. In the right pane, for the *AA_GL_Manager* role, in the **Access Rights** column, select the *Granted* option. This role is planned to have the highest access level to most forms. To save time, you will grant access to all the forms of the workspace at once.
5. On the form toolbar, click **Save**.

Step 3: Modifying Access to a Form

To modify the roles' restriction levels for a form, do the following:

1. While remaining on the [Access Rights by Screen](#) (SM201020) form, in the left pane, expand the **Finance** node to access the list of the forms, and select the first form, [Account by Period](#) (GL402000), in the list.
2. In the right pane, for the *AA_GL_Auditor* role, in the **Access Rights** column, select *View Only*. (According to the [GL_4Tier_Access](#) spreadsheet, this is the restriction level this role should have for this form.)
3. Verify that the other three roles have the restriction levels planned in the spreadsheet, which are the following:
 - *AA_GL_Configurator: Revoked*
 - *AA_GL_Manager: Delete*
 - *AA_GL_Clerk: Revoked*
4. On the form toolbar, click **Save**.
5. By performing similar actions, modify the access rights for the rest of the forms according to the [GL_4Tier_Access](#) spreadsheet.

You have created and configured roles for four access tiers within the general ledger functional area.

User Roles: To Configure a Role with Granular Access

In the following activity, you will learn how to create a role with granular access to a system object.

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 only the reprinting of checks 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 that are assigned a role that gives this access) can be authorized to reprint checks by being assigned this granular role on request from the CFO.

Process Overview

You will use the [User Roles](#) (SM201005) form to create the *AA_AP_Reprint_Checks* role. You will use the *AA* prefix for the role to have it at the top of the list, combined with *_AP* to indicate the functional area.

You will use the [Access Rights by Screen](#) (SM201020) form to modify access to the *Reprint* and *Reprint With New Number* operations as follows:

1. You will determine roles that also have full access to the [Release Payments](#) (AP505200) form. You can exclude from consideration the roles that have the *View Only* and *Revoked* access to the form, as well as the roles that you are not using for managing user access (for example, predefined roles delivered with Acumatica ERP). In this activity, you can assume that the *Accountant* and *Purchasing Manager* roles meet these criteria. That is, these roles are used for user access management and have a restriction level higher than *View Only*.



To form the list of roles that need modification, you can use filters for the table columns in the right pane of the form or create an advanced filter in the same pane. For details, see [Filtering and Sorting in Acumatica ERP](#).

2. You will modify access rights to a form container for these roles. The *Reprint* and *Reprint With New Number* operations are stored in the *ReleaseChecksFilter* container of the [Release Payments](#) form. Initially, all three roles will have the *Inherited* restriction level set to the container and form elements. Thus, before modifying access rights to the actions, you need to modify access to their parent container.

You will change the restriction level set for the container from *Inherited* to a specific one. In this case, you will revoke access to the container for the newly created role (*AA_AP_Reprint_Checks*), because you need to grant access to only two elements for this role. For the other two roles, you will set the *Delete* level for the container, because you need to restrict access to only two elements and allow access to all others.

After you have modified access to the container, its nested elements will still have the *Inherited* restriction level. (While calculating the restriction level for a user, the system takes into account only the roles for which an explicit level is set.)

3. Because you will use the granular role in combination with other roles, you will explicitly revoke access to the form elements for other two roles and grant access to the *Reprint* and *Reprint With New Number* operations for only the granular role.

The following table summarizes changes that need to be done. For details on how the system calculates a restriction level for a user, see [User Roles: Calculation of the Restriction Level for a User](#).

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	Revoked	Revoked	Inherited	Revoked	Inherited	Edit
Accountant	Delete	Delete	Inherited	Delete	Inherited	Revoked
Purchasing Manager	Delete	Delete	Inherited	Delete	Inherited	Revoked

Step 1: Creating a Role

To create a role, do the following:

1. On the [User Roles](#) (SM201005) form, add a new record.
2. In the **Role Name** box, type AA_AP_Reprint_Checks.
3. In the **Role Description** box, type Role to reprint AP checks.
4. On the form toolbar, click **Save**.

Step 2: Modifying the Access Rights to the Container and Form Elements

To modify the restriction levels for the container and form elements, do the following:

1. Open the [Access Rights by Screen](#) (SM201020) form.
2. In the left pane, expand the **Payables > Release Payments** nodes, and select the **ReleaseChecksFilter** node, which is the container for the reprint operations.
3. In the right pane, do the following:
 - In the **Access Rights** column, select *Revoked* for the AA_AP_Reprint_Checks role.
 - In the **Access Rights** column, select *Delete* for the Accountant and Purchasing Manager roles.
 - On the form toolbar, click **Save**.
4. In the left pane, expand the **ReleaseChecksFilter** node, and select the **Reprint** element.
5. In the right pane, do the following:
 - In the **Access Rights** column, select *Edit* for the AA_AP_Reprint_Checks role.
 - In the **Access Rights** column, select *Revoked* for the Accountant and Purchasing Manager roles.
6. On the form toolbar, click **Save**.
7. By performing similar actions to those in Instructions 3–5 of this step, modify the access rights for the **Reprint With New Number** element. (That is, you need to select the **Reprint With New Number** node and then select *Edit* for the AA_AP_Reprint_Checks role, and select *Revoked* for the Accountant and Purchasing Manager roles.)

You have created and configured a role with access to only one form, and you have restricted the access to two operations on this form for other roles in the system that have access to this form.

Step 3 (Optional): Verifying the Configured Access

To verify the configured access to the actions, do the following:

1. Open the [Access Rights by User](#) (SM201055) form.
2. In the **Login** box, select *pasic*. This user is assigned the **Accountant** role.
3. In the left pane, expand the **Payables > Release Payments** nodes, and select the **ReleaseChecksFilter** node.
4. In the right pane, verify that access to the **Reprint** and **Reprint With New Number** elements is revoked. That is, the *Revoked* option is displayed in the **Access Rights** column.
5. Open the [Users](#) (SM201010) form.
6. In the **Login** box, select *pasic*.
7. On the **Roles** tab, for the row with *AA_AP_Reprint_Checks* in the **Role Name** column, select the check box in the **Selected** column.
8. On the form toolbar, click **Save**.
9. Open the [Access Rights by User](#) form.
10. In the **Login** box, again select *pasic*. You have assigned this user the *AA_AP_Reprint_Checks* role, and before that the user was already assigned the **Accountant** role.
11. In the left pane, expand the **Payables > Release Payments** nodes, and select the **ReleaseChecksFilter** node.
12. In the right pane, verify that the *Edit* option is displayed in the **Access Rights** column for the **Reprint** and **Reprint with New Number** elements. This indicates that the user has access to these elements.
13. In the right pane, select the row with the **Reprint** element, and click **View Roles** on the table toolbar.
14. In the **View Roles** dialog box, which opens, review the list of roles assigned to the selected user and the access rights that each role has to the element, as shown in the following screenshot. The system gives the user the most permissive restriction level to the element (see Item 1 in the screenshot) among the roles with explicitly defined restriction levels (Item 2). The system ignores the roles with the *Inherited* level of access rights.

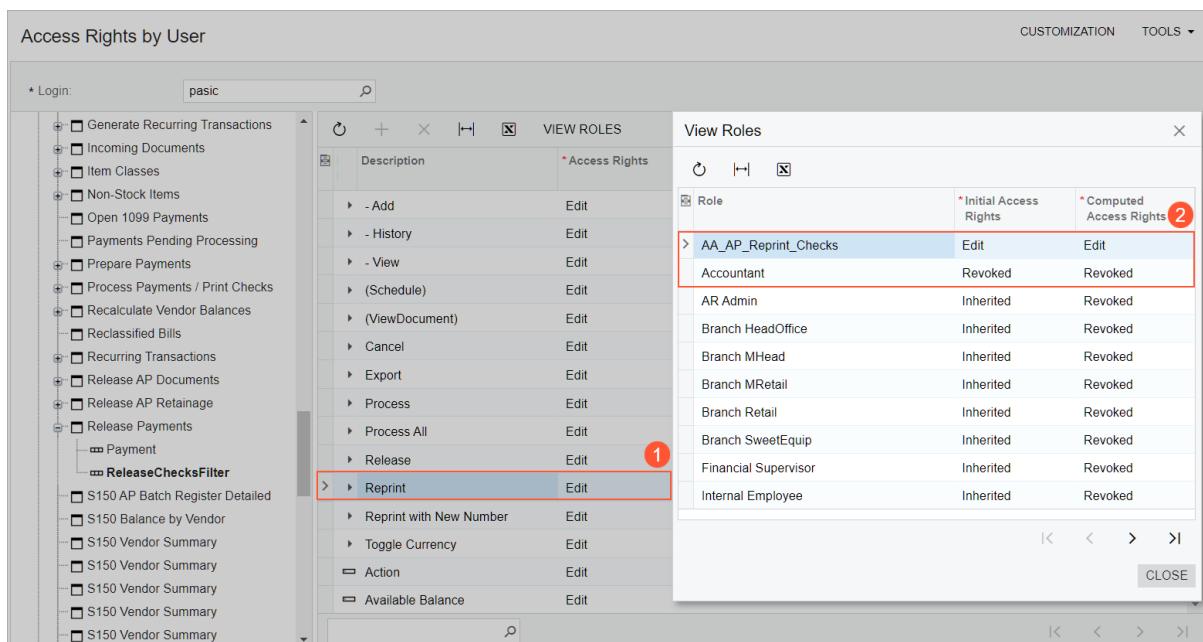


Figure: The list of roles assigned to the selected user that affect the user's access to the Reprint element

User Roles: To Modify Access Rights for a Copied Role

In the following activity, you will learn how to copy an existing role and modify access to system objects for the copied role.

Story

Suppose that you are a system administrator, and because of the company's growth, you 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.

Process Overview

You will use the [Access Rights by Role](#) (SM201025) form to create a copy of a role and then modify access rights for the copied role, which you will name *Junior Administrator*.

You will revoke the access of the *Junior Administrator* role to all workspaces in the system. To allow users with this role to create a user, you will give the role full access to the [Users](#) (SM201010), [Contacts](#) (CR302000), and [Employees](#) (EP203000) forms, which are needed for adding employees to the system. (For details on the creation of user accounts, see [User Access: To Add a User Account](#).) These forms are located in the **User Security**, **Marketing**, and **Configuration** workspaces, to which you have revoked access. The system displays the menu items for restricted workspaces on the main menu, but only links to allowed forms are visible when the user opens one of these workspaces.

Step 1: Copying a Role

To copy an existing role, do the following:

1. Open the [Access Rights by Role](#) (SM201025) form.

2. In the **Role Name** box, select the *Administrator* role.
3. On the form toolbar, click **Copy Role**.
4. In the **New Role** dialog box, which opens, do the following:
 - a. In the **New Role Name** box, type *Junior Administrator*.
 - b. Click **Copy** to copy the role and close the dialog box.
5. On the form toolbar, click **Save**.

Step 2: Modifying Access Rights for the Selected User Role

To modify access rights for the copied role, do the following:

1. While remaining on the [Access Rights by Role](#) (SM201025) form with the copied role selected in the **Role Name** box, in the left pane, select the tenant node (the very first one, whose name is in all caps).
2. In the right pane, for all workspaces in the system, select *Revoked* in the **Access Rights** column.



You can skip workspaces with the functionality that is not included in your license.

3. In the left pane, click the **Configuration** node.
4. In the right pane, for the row with the [Employees](#) (EP203000) form, select *Delete* in the **Access Rights** column.
5. On the form toolbar, click **Save**.
6. By performing actions similar to those in the previous instructions, set the *Delete* access rights to the following forms:
 - The [Contacts](#) (CR302000) form in the **Marketing** node
 - The [Users](#) (SM201010) in the **User Security** node

You have created a new role based on a copy of an existing role and modified the new role's access to suit your needs.

Lesson 2.2: Setting Up User Access

In this lesson, you will find information on user access management in Acumatica ERP.

User Access: General Information

To access Acumatica ERP, an individual must have a user account in the system and a user role assigned to the account. Each account includes a login (that is, a username), a password, and other properties, such as the user's first and last name, email address, password policy options, and the set of roles that control the user's access to the system objects.

Learning Objectives

In this lesson, 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

Applicable Scenarios

You manage user access in the following cases:

- You, as an implementation consultant, initially implement Acumatica ERP for your client and are ready to give access to company employees.
- You, as a system administrator, were notified about a new hire and need to give appropriate access to the system for the new employee.
- You, as a system administrator, were notified about a change of an employee's position and need to change access for this employee according to the new responsibilities.

User Authentication and Authorization

Acumatica ERP requires users to authenticate themselves by using the appropriate username and password. After successful authentication, user membership in roles is checked. Then based on their roles, users may access only the resources and perform only the actions they are authorized to.

A user that has not been assigned any roles has no access to the system. If the user has multiple roles that have different levels of access rights to an entity, the most permissive level applies.

The method of user authentication in Acumatica ERP can be one of the following:

- Local: User accounts are created and managed directly in Acumatica ERP.
- External: If Acumatica ERP is integrated with an external identity management system, then user accounts and roles are created and managed in the integrated system. For details on integration with the supported systems, see [Integration with Active Directory](#), [Integration with AD FS](#), and [Integration with Microsoft Entra ID](#).

To make the authentication process easier for your users, you can configure single sign-on with external identity providers, such as Google and Microsoft Account. For details, see [Integrating Acumatica ERP with OpenID Identity Providers](#).

Also, Acumatica ERP provides two-factor authentication, so that access to the system is granted only after the user successfully presents to the system additional evidence of authentication in addition to the user credentials (that is, the username and password). For details, see [Managing Two-Factor Authentication](#).

User Access Configuration

To configure each user's access to Acumatica ERP, you perform the following steps on the [Users](#) (SM201010) form:

1. You create a user account and specify the username, the password, the user's first and last name, and the email address.
2. If your organization uses specific security policies, you apply them to the user account. For more detailed information on security policies for user accounts, see [User Access: User Access Security](#).
3. You define access to the system objects by assigning a set of roles to the user; these roles correspond to the user's job responsibilities.

Ways to Generate and Share User Credentials

When you create a new user on the [Users](#) (SM201010) form, the system automatically generates a password for the user—that is, inserts the masked password in the **Password** box. You can clear the **Generate Password** check box for the new user and enter a password (which can be generated by any third-party tool) in the **Password** box.

For an existing user, you can click **Reset Password** on the form toolbar. In the dialog box that opens, you enter a new password for this user, confirm the password, and click **OK**.

When you save user settings for the first time, if a default system email account is configured and a corresponding notification template is specified on the [Email Preferences](#) (SM204001) form, the system sends an email with user credentials to the address you have specified in the **Email** box for the user.

If a system email account is not configured or if you do not want to share credentials by using email services, you can share credentials by using third-party services you trust. In this case, you specify passwords manually for the users in Acumatica ERP and share user credentials by using a third-party tool.

Role Assignment

To give a user access to the system objects, you need to assign to this user a role or a combination of roles; roles provide the access necessary to perform job responsibilities. For details on the configuration of user roles, see [User Roles: General Information](#).

To assign multiple roles to a selected user, you use the [Users](#) (SM201010) form. For example, you use this way when you have created a new user account and want to assign existing roles to it.

To assign a selected role to multiple users, you use the [User Roles](#) (SM201005) form. For example, you use this way when you have created a new role and want to assign it to existing users.

Role-Based Access

To access Acumatica ERP, users must pass authentication to confirm their identity (that is, sign in to the system). Then users pass authorization to determine their access rights to the system objects. Users' roles determine which objects they are allowed to use and which actions they are authorized to perform. A user with no role assigned to it has no access to the system.

You may take different approaches in configuring each user's access: assigning a single role to a user or assigning a combination of roles to a user. This may affect how the system calculates an individual user access. A role defines access rights to system objects with a restriction level set for these objects.

The set of restriction levels available for the system objects depends on the object type. For some objects, you can specify a more granular level; for others, you can either allow or deny the access. For details, see [User Roles: Restriction Level Options](#).

If a combination of roles is assigned to a user, some of these roles may have different restriction levels set to the same system object. The way the system calculates the final restriction level depends on a system object for which levels are different among the roles assigned to a user. For details, see [User Roles: Calculation of the Restriction Level for a User](#).

You can view the user access rights to a particular form, container, or form element by using the [Access Rights by User](#) (SM201055) form. For details, see [User Access: Related Reports and Forms](#).

Monitoring of Access Configuration

Access configuration, once established, should be subject to regular review and modification. People in an organization move across roles and projects or leave the company, and new people are hired. Job responsibilities for a particular employee or a whole department can be changed. You should keep the user access configuration in compliance with the company's changed business processes, to make sure that its sensitive data is protected from unwanted access.

We recommend establishing a process of requesting access to particular system objects. Such requests should be justified by changes in the job responsibilities and approved by superiors.

You should be notified each time an employee is leaving the company or a contractor with access to the system has completed their project. You can either deactivate user accounts for these people or clear the list of assigned roles if you need to keep the user account for some reason.

We also recommend regular review of the list of user roles. You can either delete unused roles that are assigned to no users or add some prefix to the descriptions of the roles if you want to keep them for some reason. You should determine the number of roles you can maintain to effectively secure access to the system and try to keep the list within this number.

Also, we recommend that you regularly review the history of users' access to Acumatica ERP forms that contain company data, to identify unexpected or unwanted access behavior.

You can use reports and inquires provided by Acumatica ERP for monitoring access configuration. For details, see [User Access: Related Reports and Forms](#).

User Access: User Access Security

In addition to the system-wide password policy configured on the [Security Preferences](#) (SM201060) form, you can use the following capabilities of Acumatica ERP to apply your organization's security policies to individual user accounts on the [Users](#) (SM201010) form.



We recommend configuring system-wide security policies during the preparation of the Acumatica ERP instance for implementation. For details, see [Preparing an Instance: System-Wide Security Policy](#).

Password Recovery

You can allow a particular user to recover the username and reset the password through email by selecting the **Allow Password Recovery** check box on the [Users](#) (SM201010) form.

If this check box is selected for a particular user, the user can click the *Forgot Your Credentials?* link on the Sign-In page of Acumatica ERP and receive an email with a link to the password reset form. For more information, see [Access to Your Acumatica ERP Instance](#).

Password Change

You can allow a specific user to change the password by selecting the **Allow Password Changes** check box on the [Users](#) (SM201010) form. The user will be able to change the password at any time by clicking **Change Password** on the [User Profile](#) (SM203010) form.

If you have set a system-wide requirement for users to change their passwords periodically by selecting the **Password Expiry Period in Days** check box on the [Security Preferences](#) (SM201060) form, the system forces all users to change their passwords, regardless of whether the **Allow Password Changes** check box is selected for the individual user.

Forced Password Change

You can require a specific user to change the password on the next sign-in by selecting the **Force User to Change Password on Next Login** check box on the [Users](#) (SM201010) form. After the user changes the password, the system clears the check box for this user.

This check box is available only if the **Allow Password Changes** check box is selected.

Password Expiration

You can allow a particular user never to change the password by selecting the **Password Never Expires** check box on the [Users](#) (SM201010) form. Such a user will not be forced to change the password, even if the **Password Expiry Period in Days** check box is selected on the [Security Preferences](#) (SM201060) form to enforce the system-

wide requirement to change a password periodically. The only way to make such a user change their password is to select the **Force User to Change Password on Next Login** check box on the [Users](#) form.

Individual Network Restrictions

You can limit the range of IP addresses from which a specific user can sign in to your Acumatica ERP instance. If the user attempts to access the system from a computer with an IP address that is outside of the specified range, access will be denied. You specify the range of IP addresses on the **IP Filter** tab of the [Users](#) (SM201010) form.

User Account Deactivation

While viewing a particular user on the [Users](#) (SM201010) form, you can deactivate the user account to temporarily prevent the user from signing in to your Acumatica ERP instance by clicking **Disable User** on the form toolbar. For example, suppose that your organization uses a contractor's services from time to time. When the contractor completes a project, you deactivate the contractor's user account until the next project emerges.



You cannot deactivate your own user account.

User Inactivity Timeout

You can specify the time interval (in hours) of user inactivity after which a user will be forced to sign in again. You specify the value on the [Security Preferences](#) (SM201060) form, in the **User Inactivity Timeout** box of the **Timeout Settings** section. This setting will be applied to all tenants of the instance.

You can instead configure the system to use the timeout setting value specified in the `web.config` file. To do this, in the **Timeout Settings** section of the [Security Preferences](#) form, you select the **Use WebConfig Value** check box.

User Access: To Add a User Account

The following activity will walk you through the process of adding 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 a warehouse worker. The request has been justified and approved by the corresponding manager.

Process Overview

You will use the [Users](#) (SM201010) form to add and configure a user account.

Step: Adding the User Account

To add the user account for Sarah Kent, do the following:

1. On the [Users](#) (SM201010) form, add a new record.
2. In the **Login** box of the Summary area, type `kent`.
3. Clear the **Generate Password** check box.
4. In the **Password** box, type `Welcome123`.
5. Specify the following settings for this user:

- **First Name:** Sarah
 - **Last Name:** Kent
 - **Email:** kent@sweetlife.com
 - **Comment:** Warehouse worker
6. Specify the following settings to set this user's individual password policy:
- **Allow Password Recovery:** Selected
 - **Allow Password Changes:** Selected
 - **Password Never Expires:** Cleared
 - **Force User to Change Password on Next Login:** Selected
7. On the **Roles** tab, assign the following roles to the user by selecting the check boxes in the **Selected** column:
- *Branch HeadOffice*
 - *Internal User*
 - *Warehouse Worker*
8. On the form toolbar, click **Save**.

User Access: To Assign a Role to Multiple Users

The following activity will walk you through the process of assigning a role to multiple user accounts.

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*)

Process Overview

You will use the [User Roles](#) (SM201005) form to assign a role to multiple users.

Step: Assigning the Role to Multiple Users

To assign the *BI* role to multiple users, do the following:

1. Open the [User Roles](#) (SM201005) form.
2. In the **Role Name** box of the Summary area, select the *BI* role.
3. On the **Membership** tab, do the following:
 - a. Click **Add Row** on the table toolbar.
 - b. In the **Username** column, select *pick*, which represents the user account of Ian Pick.
4. Repeat the previous instruction to add *owen*, which represents the user account of Bill Owen, to the *BI* role.
5. On the form toolbar, click **Save**.

You have assigned the role to multiple users.

User Access: To Modify Access for a User Account

The following activity will walk you through the process of modifying access for a user.

Story

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

Process Overview

You will use the [Users](#) (SM201010) form to modify the set of roles for a user account.

Step: Modifying Access for the User

To modify access for the user account of Andrew Barber, do the following:

1. Open the [Users](#) (SM201010) form.
2. In the **Login** box of the Summary area, select *barber*.
3. In the **Comment** box, clear the existing text and type Packline operator in the Head Office branch.
4. On the **Roles** tab, do the following:
 - a. For the row with *Warehouse Worker* in the **Role Name** column, clear the check box in the **Selected** column.
 - b. For the row with *Packline Operator* in the **Role Name** column, select the check box in the **Selected** column.
5. On the form toolbar, click **Save**.

You have modified access rights for the user because of a change in his job responsibilities.

Lesson 2.3: Encrypting with Digital Certificates

This lesson provides details on managing encryption certificates and encrypting the database of your Acumatica ERP instance.

Digital Certificates: General Information

Acumatica ERP uses digital certificates to store sensitive information in the database encrypted and to authenticate documents (PDF files) that are shared or sent electronically. These certificates can be purchased from a recognized certification authority. Each certificate has a password that is used to validate the owner of the certificate if you need to reinstall the system or move the database.

Learning Objectives

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

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

Applicable Scenarios

You use digital certificates in the following cases:

- Your company has decided to replace the default encryption algorithm used in Acumatica ERP to encrypt sensitive data stored in the database with some other encryption certificate because of company security policies. You, as a system administrator, have been asked to configure the replacement.
- Your company has decided to use encryption certificates for signing PDF files generated for reports in Acumatica ERP. You, as a system administrator, have been asked to upload the needed certificate and configure the signing of PDF files.

Certificate Registration

To use a certificate, you first need to register it on the [Encryption Certificates](#) (SM200530) form. Only certificates that are added to this form can be used for replacing the database encryption algorithm used in Acumatica ERP or for signing PDF files.

For each certificate, you provide a name and a password. The system uses the password to access the uploaded certificate and use it for data encryption. Then you attach the certificate file to the record.

Database Encryption

The Acumatica ERP database stores sensitive data, such as credit card numbers and passwords, encrypted. If no encryption certificate is loaded, base64 encryption is used. You can find the list of encrypted data on the [Certificate Replacement](#) (SM200535) form.

You can replace the encryption algorithm used in Acumatica ERP with your encryption certificate. If the database of your Acumatica ERP instance is large, encryption may take a lot of time and may cause slowdowns in responses from the database. For large databases, we recommend that you postpone the start of encryption by scheduling it at a time when nobody is using the system (for example, at night).

PDF Signature

You can use encryption certificates to sign PDF files that are generated for reports in the system. A PDF certificate protects the authenticity of a document throughout its life cycle. For example, when a company employee emails the company's digitally signed quarterly financial statements, the recipients of the documents can be sure of the identity of the sender and the integrity of the financial information.

You can specify a certificate that will be used for signing the PDF documents generated by the system. You use the **PDF Signing Certificate** box on [Security Preferences](#) (SM201060) form to specify the default certificate.

Removal of Outdated Certificates

Before you remove a certificate from the system, make sure that the certificate is not being used for the database encryption on the [Certificate Replacement](#) (SM200535) form or for PDF document signing on the [Security Preferences](#) (SM201060) form. If it is used in either of these cases, the certificate cannot be removed.

You remove an outdated certificate from the list on the [Encryption Certificates](#) (SM200530) form by clicking **Delete Row** on the table toolbar.

Digital Certificates: To Encrypt the Database

The following activity will walk you through the process of replacing the default encryption algorithm used in Acumatica ERP with your encryption certificate.

Story

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

Process Overview

You will use the [Encryption Certificates](#) (SM200530) form to register and upload the [AcumaticaTrainingEncryption.pfx](#) digital certificate with the `Aw34esz` password to be used for database encryption.



The provided certificate is for training purposes only; do not use it for the production environment.

On the [Certificate Replacement](#) (SM200535) form, you will specify a certificate in the **New Certificate** box and click **Replace Certificate**. The system will launch the encryption of sensitive data with the new certificate.

Additionally, you will restore the database encryption method to the default one by removing the specified certificate and clicking **Replace Certificate** once again.

System Preparation

Before you start performing the steps of this activity, open the [File Upload Preferences](#) (SM202550) form and verify that `.pfx` is on the list of allowed extensions. Make sure that the check box in the **Forbidden** column is cleared for this extension.

Step 1: To Import a Certificate

To register and upload a certificate, do the following:

1. Open the [Encryption Certificates](#) (SM200530) form.
2. On the table toolbar, click **Add Row**.
3. In the **Name** box, type Training Encryption.
4. In the **Password** box, type the `Aw34esz` password for the certificate. It will be masked after you save your changes.
5. On the form toolbar, click **Save**.
6. Upload the file with the certificate as follows:
 - a. Click the paper clip icon in the **Files** column of the row with the certificate.
 - b. In the **Files** dialog box, click **Browse**, and select the [AcumaticaTrainingEncryption.pfx](#) file with the certificate you want to upload.
 - c. Click **Upload** to import the certificate.
 - d. Close the **Files** dialog box.

Step 2: To Encrypt the Database

To encrypt the database, do the following:

1. Open the [Certificate Replacement](#) (SM200535) form.



In the Selection area, you can see the certificate currently used for database encryption in the **Current Certificate** box. If the box is blank, the default encryption algorithm is being used.

2. In the **New Certificate** box of the Selection area, select the certificate that you imported in the previous step. Its key will be used for encrypting the database.
3. On the form toolbar, click **Replace Certificate**.

This initiates the process of decrypting the data with the previous encryption algorithm and encrypting it by using the new key. The **Processing** dialog box opens.

4. Close the dialog box after the processing completes.

Step 3: To Restore the Default Database Encryption

Perform the following instructions to restore the default database encryption:

1. While remaining on the [Certificate Replacement](#) (SM200535) form, in the Selection area, clear the value of the **New Certificate** box.
2. On the form toolbar, click **Replace Certificate**.

This initiates the process of decrypting the data with the previous certificate and encrypting it by using the default encryption algorithm. The **Processing** dialog box opens.

3. Close the dialog box after the processing completes. Notice that the **Current Certificate** box has become empty.

Part 3: Monitoring User Activities

In the lessons of this part, you will learn how to use system-wide security auditing and field-level auditing.

Lesson 3.1: Using System-Wide Security Auditing

This lesson provides details on the configuration of system-wide security auditing.

System-Wide Security Auditing: General Information

Acumatica ERP can monitor and record events triggered by a user or the system with the security auditing functionality. The system can monitor different types of events, and you set up the time period for which the audit trail—which is a series of records of activities in Acumatica ERP—must be kept.

Learning Objectives

In this lesson, 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

Applicable Scenarios

You use system-wide security auditing in the following cases:

- Your company must comply with auditing regulations and needs to implement the corresponding auditing procedures.
- Your company wants to ensure accountability and the ability to track user actions in the system.

Enabling of Auditing

On the [Security Preferences](#) (SM201060) form, under the **Audit** section of the Summary area, you can select the types of user and system events the system will monitor. Also, you can specify the time period for which the audit trail must be kept by specifying the number of months in the **Audit History Retention Period (Months)** box.

Auditing of User Activities

On the [Security Preferences](#) (SM201060) form, under the **Audit** section of the Summary area, you select the following check boxes to turn on the auditing of system events related to the corresponding user activities:

- **Login:** The system records every successful sign-in of a user.
- **Login Failed:** The system records every unsuccessful sign-in attempt of a user.
- **Logout:** The system records every sign-out of a user.
- **Screen Accessed:** The system records information about a user's access of an Acumatica ERP form.



The event is logged only once for each form during a user session (when the user first opens the form).

- **Session Expired:** The system records every expiration of a user's session.

- **License Exceeded:** The system records every forced user sign-out due to the maximum number of users (as specified in your company's license) being exceeded.

Auditing of Email Processing

On the [Security Preferences](#) (SM201060) form, under the **Audit** section of the Summary area, you select the following check boxes to turn on the auditing of the corresponding system events related to email processing:

- **Send Email Success:** The system records every successful sending of an email from the system email account.
- **Send Email Error:** The system records every failed sending of an email from the system email account.

Auditing of Data Access

On the [Security Preferences](#) (SM201060) form, under the **Audit** section of the Summary area, you select the following check boxes to turn on the auditing of the corresponding system events related to data access:

- **OData Refresh:** The system records the access of Acumatica ERP data through a generic inquiry that has been exposed by using the OData protocol. For more information on support for OData in Acumatica ERP, see [Accessing the Exposed Inquiry Results Through OData](#).
- **Customization Published:** The system records every publication of a customization. For more information, see the Acumatica ERP Customization Guide.

Reviewing Audit Trails

You use the [Access History](#) (SM201045) form to view the audit trails. The audit trail for each event type shows the time when the event took place, the user who performed the operation, the IP address from which the user signed in to the system, and other settings, depending on the event type. You can narrow the range of the listed events by user, date range, and operation type.

System-Wide Security Auditing: Process Activity

The following activity will walk you through the process of specifying system-wide security auditing to meet your needs.

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 because of the maximum number of users (as specified in the license) being exceeded.

Process Overview

To configure system-wide security auditing, you will use the settings on the [Security Preferences](#) (SM201060) form. Then you will review audit trails on the [Access History](#) (SM201045) form.

Step 1: Turning On the System-Wide Security Auditing for Events

To specify your preferences for the auditing of system and user events, do the following:

1. Open the [Security Preferences](#) (SM201060) form.
2. In the **Audit** section, review the check boxes that are selected by default, which are the following:

- **Login**
 - **Login Failed**
 - **Logout**
 - **Screen Accessed**
 - **Session Expired**
 - **Send Email Success**
 - **Send Email Error**
3. In the same section, select the following check boxes (if the check boxes are selected, keep their state as is):
 - **Customization Published**
 - **License Exceeded**
 4. On the form toolbar, click **Save**.

Step 2: Viewing Audit Trails

To view audit trails for system events, do the following:

1. Open the [Access History](#) (SM201045) form.
2. In the **Operation** box of the Selection area, select *Access Screen*. The system displays the list of events registered for this operation.
3. In the **Operation** box, select each of the other available options in succession, and review the list of events.



You can also filter the events by a user account by selecting a user in the **Username** box and by a date range by selecting dates in the **From** and **To** boxes.

Lesson 3.2: Using Field-Level Auditing

This lesson provides details on the field-level auditing functionality, which you can use to configure and manage audit trails that record user changes on the forms.

Field-Level Auditing: General Information

The development of automatic data processing has made it necessary for companies to consider protecting sensitive information. In certain highly regulated industries, these companies must implement auditing to address identity-management concerns related to compliance issues. Regulations such as Sarbanes-Oxley (SOX) Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) all have extensive requirements on the auditing of user identity and access to system resources.

By using the field-level auditing functionality, which provides auditing at the level of actual fields (that is, UI elements) on particular forms for particular records, you can monitor and record user actions on Acumatica ERP forms as they are recorded in the system. The audit trail holds records of every change users have made on the monitored forms, such as changes to documents or transactions and their properties, modifications to customer accounts or employee records, and changes in security policies. You can also see who made the changes and when they took place.



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

Learning Objectives

In this lesson, 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

Applicable Scenarios

You use field-level auditing in the following cases:

- Your company must comply with auditing regulations and needs to implement corresponding auditing procedures.
- Your company wants to ensure accountability and the ability to track user actions in the system.

Configuration of Access to Field-Level Auditing Functionality

User access to field-level auditing should be configured to support business processes without exposing the company to undue risks. The audit trails may contain sensitive information, so only authorized users should have access to this functionality. As you plan the configuration of this access, we recommend that you consider the following user scenarios:

- A user configures, turns on, and turns off auditing of the needed forms. Also, the user periodically views the list of forms for which auditing is configured and checks whether auditing is turned on for each form. To be able to perform these operations, the user should have access to the [Audit](#) (SM205510) form.
- A user views the complete audit trail for all audited forms. To view this audit trail, the user should have access to the [Audit History](#) (SM205530) inquiry form.
- A user views the audit trail for a particular record directly from the audited form, to which the user needs to have access. The predefined *Field-Level Audit* role should be assigned to this user, which causes the **Audit History** command on the **Tools** menu of the form title bar to become available to the user. The user can open any audited form, select a record created by using the form, and click **Tools > Audit History** to view the audit trail for the selected record.



The predefined *Administrator* role has complete access to all of the forms mentioned in these user scenarios.

You can take different approaches in configuring user access to the functionality. For example, you can cover all three scenarios by copying the predefined *Field-Level Audit* role and adding access to the mentioned above forms to the copied role.

Alternatively, you can create a role that will cover only viewing the complete audit trail. You can then use this role in combination with the *Field-Level Audit* role to give a user the ability to view the audit trail from an audited form and the complete audit trail on the [Audit History](#) inquiry form. The configuring and enabling of auditing functionality, with this approach, will be done by a user with the predefined *Administrator* role.

For details on the planning of access configuration, see [User Roles: Planning of Access Configuration](#).

Forms That Support Auditing

Field-level auditing is configured on a per-form basis. A form supports this auditing if the **Audit History** menu command is available on the **Tools** menu of the form title bar, as demonstrated in the following screenshot. If the **Audit History** command is not shown, the selected form does not support field-level auditing.

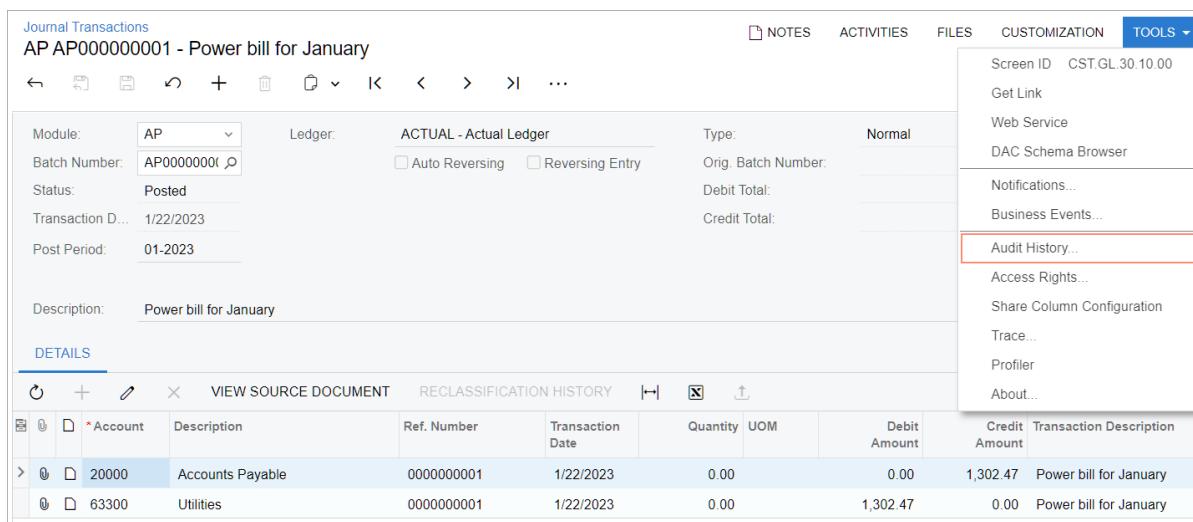


Figure: The available Audit History command for the Journal Transactions form

Setup of Auditing of a Form

You use the [Audit](#) (SM205510) form to configure auditing for a particular form. On this form, you can configure the following levels of auditing granularity:

- Auditing of all fields from all database tables associated with the form: You select the **All Fields** option in the **Show Fields** box on the form and then select all the tables listed in the **Tables** pane.
- Auditing of only the database fields that are available on the user interface from all database tables associated with the form: You select the **UI Fields** option in the **Show Fields** box on the form and then select all the tables listed in the **Tables** pane.
- Auditing of specific database fields from particular tables associated with the form: You select the needed tables from the list on the **Tables** pane, and then for each table, you select the needed fields from the list on the **Fields** pane. You can narrow the list of fields to those that are available on user interface by selecting the **UI Fields** option in the **Show Fields** box.



To view the list of fields for a particular table, you set focus to the line with the table name on the **Tables** pane, and then the system displays the list of table fields in the **Fields** pane. By default, if a table is selected, then all its fields are selected for auditing.

You can view the list of forms for which auditing is configured on the Audit (SM2055PL) form. For any audited form, you can quickly navigate to the [Audit](#) (SM205510) form, where you can turn on or off the auditing of particular database tables and fields associated with the form.

Turning On and Off of Auditing of a Form

After the form auditing is configured, you can turn on and off auditing of the form by selecting or clearing the **Active** check box on the [Audit](#) (SM205510) form.

When you turn on the auditing, every time a user makes changes to a record associated with the form and clicks **Save**, a record is added to the audit trail the system maintains for the form. This record contains the details of the modification, including who modified the document, what changes were made, and when the changes occurred.

When you turn off the auditing of the form, the monitoring of the changes is turned off, but the configuration of the auditing remains without changes.

Viewing of an Audit Trail

When auditing is turned on for a form, you can select a record and view its audit trail—that is, the changes made to the record—directly from the form by clicking **Tools > Audit History** on the form title bar. This opens the *Audit History* (SM205530) form on a new tab, where you can see the audit trail for the selected record. You can click the **Changes** arrow to view the detailed data of the modification. For each change, you can see who modified the record and when, what form was used, when the modification took place, and what changes were made.



You can click **Expand All** to view the details of all modifications or click **Collapse All** to hide these details. Also, you can use the browser functionality to search for a specific word or phrase on the screen or to print the screen.

On the *Audit History* inquiry form, you can view a full audit trail for the records of the form. That is, you can view all the changes made to the records of the audited form since auditing was turned on for the form. You can filter the modifications that you are viewing by user, by database table associated with the form, and by date range.

Viewing of General Information About a Record

If the currently opened form supports field-level auditing but auditing was not configured or is turned off for the form, you can still view some information in the **Update History** dialog box, which opens when the user clicks **Tools > Audit History** on the form title bar. This dialog box does not show an audit trail; it provides only general information about the creation and the last modification of the selected record.

If you have access to the *Audit* (SM205510) form, you will see the **Enable Field Level Audit** button in the **Update History** dialog box. You can click this button to navigate to the *Audit* form, where you can configure and turn on auditing for the currently opened form.

Field-Level Auditing: Implementation Activity

In the following implementation activity, you will learn how to configure and enable auditing for a form.

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.

Configuration Overview

In the *U100* dataset, for the purposes of this activity, the following tasks have been performed:

- On the *Enable/Disable Features* (CS100000) form, the *Field-Level Audit* feature has been enabled.
- On the *User Roles* (SM201005) form, the *Audit History Access* role has been configured. The role provides complete access to the *Audit History* (SM205530) inquiry form. For details on similar configuration of a role, see *User Roles: To Configure a Role with Granular Access*.

Process Overview

You will use the *Audit* (SM205510) form to configure and turn on the auditing of the fields visible on the interface of the *Invoices and Memos* (AR301000) form.

Also, on the Audit (SM2055PL) inquiry form, you will review the list of forms with auditing configured; you will then turn off the auditing for the *Invoices and Memos* form.

Step 1: Configuring and Turning On Auditing for a Form

To configure and turn on audit for the *Invoices and Memos* (AR301000) form, do the following:

1. On the *Audit* (SM205510) form, add a new record.
2. In the **Screen Name** box in the Summary area, select *Invoices and Memos*.
3. In the **Show Fields** box, select the *UI Fields* option.
4. In the **Description** box, type Auditing changes made to invoices and memos.
5. In the **Tables** pane, select the check box in the **Active** column for each table in the list.



The number of tables associated with the form may exceed the capacity of the screen. The actual list of forms may take multiple pages. To navigate between pages, you use the navigation buttons located in the right corner of the table footer.

6. In the Summary area of the form, select the **Active** check box to turn on the auditing of the form.
7. On the form toolbar, click **Save**.



To make sure that the audit configuration has been implemented, sign out of the system and sign in again.

You have configured and activated the auditing for the *Invoices and Memos* form.

Step 2: Providing the User with Access to Audit History

To provide access to audit history for the *gibbs* user account, do the following:

1. Open the *User Roles* (SM201005) form.
2. In the **Role Name** box, select *Audit History Access*.
3. On the **Membership** tab, click **Add Row** and select *gibbs* in the added row.
4. On the form toolbar, click **Save**.

Step 3: Making Changes to Be Audited

To make changes to be audited on the *Invoices and Memos* (AR301000) form, do the following:

1. On the *Invoices and Memos* (AR301000) form, add a new record.
2. In the Summary area, specify the following settings:
 - **Customer:** HMBAKERY
 - **Terms:** 310N30
3. On the **Details** tab, click **Add Row**, and in the added row, specify 311 in the **Ext. Price** column.
4. On the form toolbar, click **Remove Hold**.
5. On the form toolbar, click **Save**.
6. Modify the invoice as follows:
 - a. On the More menu, click **Hold**.
 - b. In the **Ext. Price** column of the only row, type 622.

- c. On the form toolbar, click **Remove Hold**, and then click **Release** to release the invoice.

Step 4: Reviewing User Actions on the Invoices and Memos Form

To review the auditing of changes for the invoice on the *Invoices and Memos* (AR301000) form, do the following:

1. While remaining on the *Invoices and Memos* (AR301000) form, on the form title bar, select **Tools > Audit History**.
2. On the Audit History page, which opens, review the audit history for the invoice (as shown in the following screenshot).

Audit History: AR Invoice/Memo																							
Type: Invoice	Reference Nbr.: 000119	↓ Expand All	↑ Collapse All																				
Created By: gibbs	Last Modified By: gibbs																						
Created Through: AR301000	Last Modified Through: AR301000																						
Created On: 12/5/2025 9:51:01 AM	Last Modified On: 12/5/2025 9:51:22 AM																						
Date: 12/5/2025 9:51:23 AM User: gibbs Screen: AR301000																							
▾ Changes: AR Document Modified <table border="1"> <thead> <tr> <th>Type</th> <th>Reference Nbr.</th> <th>Cash Discount</th> <th>Balance</th> <th>Batch Nbr.</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Invoice</td> <td>000119</td> <td>0.0</td> <td>Balanced</td> <td></td> <td></td> </tr> <tr> <td>Invoice</td> <td>000119</td> <td>18.66</td> <td>AR000192</td> <td></td> <td>Open</td> </tr> </tbody> </table>						Type	Reference Nbr.	Cash Discount	Balance	Batch Nbr.	Status	Invoice	000119	0.0	Balanced			Invoice	000119	18.66	AR000192		Open
Type	Reference Nbr.	Cash Discount	Balance	Batch Nbr.	Status																		
Invoice	000119	0.0	Balanced																				
Invoice	000119	18.66	AR000192		Open																		
Date: 12/5/2025 9:51:22 AM User: gibbs Screen: AR301000																							
▾ Changes: AR Transactions Modified <table border="1"> <thead> <tr> <th>Tran. Type</th> <th>Reference Nbr.</th> <th>Line Nbr.</th> <th>Ext. Price</th> <th>Amount</th> </tr> </thead> <tbody> <tr> <td>INV</td> <td>000119</td> <td>1</td> <td>311</td> <td>311.00</td> </tr> <tr> <td>INV</td> <td>000119</td> <td>1</td> <td>622</td> <td>622.00</td> </tr> </tbody> </table>						Tran. Type	Reference Nbr.	Line Nbr.	Ext. Price	Amount	INV	000119	1	311	311.00	INV	000119	1	622	622.00			
Tran. Type	Reference Nbr.	Line Nbr.	Ext. Price	Amount																			
INV	000119	1	311	311.00																			
INV	000119	1	622	622.00																			
AR Invoice/Memo Modified																							
<table border="1"> <thead> <tr> <th>Type</th> <th>Reference Nbr.</th> <th>Detail Total</th> <th>Misc. Charges</th> <th>Unpaid Balance</th> </tr> </thead> <tbody> <tr> <td>Invoice</td> <td>000119</td> <td>311.00</td> <td>311.00</td> <td>311.00</td> </tr> <tr> <td>Invoice</td> <td>000119</td> <td>622.00</td> <td>622.00</td> <td>622.00</td> </tr> </tbody> </table>						Type	Reference Nbr.	Detail Total	Misc. Charges	Unpaid Balance	Invoice	000119	311.00	311.00	311.00	Invoice	000119	622.00	622.00	622.00			
Type	Reference Nbr.	Detail Total	Misc. Charges	Unpaid Balance																			
Invoice	000119	311.00	311.00	311.00																			
Invoice	000119	622.00	622.00	622.00																			
Date: 12/5/2025 9:51:01 AM User: gibbs Screen: AR301000																							
▶ Changes: 																							

Figure: Audit history for the invoice

Step 5: Turning Off Auditing for a Form

To turn off auditing for the *Invoices and Memos* (AR301000) form, do the following:

1. Open the Audit (SM2055PL) inquiry form.
2. In the list of audited forms, double-click the record with *Invoices and Memos* in the **Screen Name** column.
3. On the *Audit* (SM205510) form, which opens, clear the **Active** check box in the Summary area.
4. On the form toolbar, click **Save**.

You have turned off auditing for the *Invoices and Memos* form.

Field-Level Auditing: Process Activity

The following activity will walk you through the process of reviewing audit trails.

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

In the *U100* dataset, for the purposes of this activity, the following tasks have been performed:

- On the [Enable/Disable Features](#) (CS100000) form, the *Field-Level Audit* feature has been enabled.
- On the [User Roles](#) (SM201005) form, the *Audit History Access* role has been configured. The role provides complete access to the [Audit History](#) (SM205530) inquiry form. For details on similar configuration of a role, see [User Roles: To Configure a Role with Granular Access](#).
- On the [Users](#) (SM201010) form, the *Field-Level Audit* and *Audit History Access* roles have been assigned to Jasmine Reece (with the username *reece*), who is the company's corporate controller.
- Field-level auditing has been configured for the [Purchase Orders](#) (PO301000) form.

Process Overview

You will use the [Purchase Orders](#) (PO301000) form to view the *000026* purchase order. With this document selected on the form, you will click **Tools > Audit History** on the form title bar to open the Audit History page in a new tab, where you can see the list of changes made to the selected document.

Then you will open the [Audit History](#) (SM205530) inquiry form and view the audit trails recorded for the changes made to the documents on the [Purchase Orders](#) (PO301000) form.

Also, you will view general information about a journal transaction by using the **Audit History** command on the [Journal Transactions](#) (GL301000) form, for which auditing has not been configured.

System Preparation

Before you start performing the steps of this activity, sign in to a company with the *U100* dataset preloaded. You should sign in as a corporate controller with the *reece* username and *123* password.

Step 1: Reviewing the Audit History for a Particular Document

To review the audit history for the *000026* purchase order, do the following:

1. Open the [Purchase Orders](#) (PO301000) form.
2. In the **Order Nbr.** box, select the *000026* order.
3. On the form title bar, select **Tools > Audit History**.
4. Review the audit history for the order (shown in the following screenshot) on the Audit History page, which opens. Click **Expand All** to review the details of the changes.

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: 12/31/1899 7:00:00 PM	Last Modified On: 12/31/1899 7:00:00 PM

Date: 10/19/2025 2:17:34 PM User: wiley Screen: PO301000 ▶ Changes:
Date: 10/19/2025 2:17:21 PM User: wiley Screen: PO301000 ▶ Changes:
Date: 10/19/2025 2:17:12 PM User: wiley Screen: PO301000 ▶ Changes:
Date: 10/19/2025 2:16:43 PM User: wiley Screen: PO301000 ▶ Changes:
Date: 10/19/2025 2:16:27 PM User: wiley Screen: PO301000 ▶ Changes:
Date: 10/19/2025 2:16:06 PM User: wiley Screen: PO301000 ▶ Changes:

Version: 25.100.0054 **Customization:** None

Figure: Audit history for the purchase order

You have reviewed the audit history for the particular purchase order.

Step 2: Reviewing the Audit History for Multiple Documents

To review the audit history for changes made to multiple purchase orders, do the following:

1. Open the *Audit History* (SM205530) inquiry form.
2. In the **Screen ID** box, select *PO.30.10.00*.
3. In the **Start Date** and **End Date** boxes, clear the selected dates to view all historical records.
4. In the **Records** table, select a document and review its changes in the **Events** table, as shown in the following screenshot.

The screenshot shows the Audit History screen for a purchase order. The 'Records' section displays a list of purchase orders with columns for Type and Order Nbr. One record, 'Normal 000026', is selected and highlighted with a red box. The 'Events' section displays a list of audit events with columns for Operation, Date and Time, User Name, Branch, Workflow, Vendor, Location, Date, Promised On, Expires On, and Status. Five events are listed, all related to the creation and modification of the purchase order, and they are also highlighted with a red box.

Figure: Audit history for a purchase order

You have reviewed the audit history for multiple purchase orders.

Step 3: Reviewing General Information About a Record

To review general information for a record on a form for which auditing has not been configured, do the following:

1. Open the **Journal Transactions** (GL301000) form. Auditing has not been configured for this form in the *U100* dataset.
2. In the **Batch Number** box, select any batch that is available.
3. On the form title bar, select **Tools > Audit History**.
4. Review general information about the selected batch in the **Update History** dialog box, which opens, as demonstrated in the following screenshot.

The screenshot shows the Journal Transactions form for AP AP00000004 - Power bill for April. The 'DETAILS' section shows a table with rows for 'Branch' (HEADOFFICE), 'Account' (20000 Accounts Payable), and 'Description' (Power bill for April). A modal dialog box titled 'Update History' is open, showing the following details:

Created By:	gibbs	Last Modified By:	gibbs
Created Through:	AP501000	Last Modified Through:	AP501000
Created On:	12/31/1899 7:00:00 PM	Last Modified On:	12/31/1899 7:00:00 PM

At the bottom of the dialog box are buttons for 'ENABLE FIELD LEVEL AUDIT' and 'CANCEL'. The main form shows a table with two rows:

	Debit Amount	Credit Amount	Transaction Description
00-000 00000004	0.00	1,298.17	Power bill for April
00-000 00000004	0.00	1,298.17	Power bill for April

Figure: General information about a document

You have reviewed general information about a document.

Part 4: Using Multifactor Authentication Methods

This part provides details about the configuration and use of two-factor authentication.

General Purpose and Types of Multifactor Authentication

In most cases, multifactor authentication involves two authentication mechanisms. By combining two authentication mechanisms, businesses can achieve two-factor authentication. Most two-factor mechanisms require something you know (such as a password) plus either something you have (a token, mobile phone, or USB) or something that identifies who you are (fingerprint or other biometric information).

Authentication Mechanisms

The following list contains examples of existing authentication mechanisms that can be combined to achieve multifactor authentication:

- Username and password: The most basic authentication mechanism requires users to enter a username and password. Additional options such as IP address validation and strong password requirements can provide additional security.
- Token or key fob: The token displays a code that is regularly updated. The user types the code into the ERP system, which verifies the code. RSA SecurID tokens are an example of this mechanism.
- Mobile devices: An ERP system sends a text message to the user's mobile device. The user types the received code to verify the sign-in directly on the phone or by entering an access code in the application on the device that is used to access the ERP system. Another option is to install a secure application on the phone that behaves like a token.
- Email: During sign-in, the system sends a code to the user's email address. The user enters a code in the email to authenticate themselves.
- Smart card or USB device: Hardware issued by the organization can be configured to grant access when a card is swiped or a USB device or chip is inserted.
- Fingerprint reader or biometric device: Biometric devices work like smart cards. They require an initial setup but cannot be lost or stolen.
- Virtual private networks (VPNs): A VPN has its own authentication mechanism, which provides a layer of security at the communication level. VPNs can be authenticated by using passwords, tokens, MAC addresses, and other methods.

Acumatica ERP offers the ability to configure two-factor authentication without setting up integration with multifactor authentication providers. If the two-factor authentication is enabled, every user will need to present to the system additional evidence (the second factor) of authentication in addition to the user credentials. The second factor is either an access code or sign-in approval sent from the user's mobile device. An access code can be generated by using the web application or mobile device, or it can be sent by email and SMS. For details, see [Two-Factor Authentication: General Information](#).

Adaptive (Smart) Multifactor Authentication

Often there is a trade-off between security and usability. The additional security associated with multifactor authentication comes at the price of users logging in two times instead of one.

To improve usability, some multifactor systems have been configured to select multiple authentication mechanisms only when the risk profile of system entry is high. The risk profile can be set based on the information gathered about the user's environment, such as the machine MAC address, the IP address, browser cookies, the time of day, and other patterns.

Examples of risk profiles include the following:

- Low risk: Sign-in from an office IP address at 9 AM on weekdays by using a browser with a stored cookie
- Medium risk: Sign-in from an unfamiliar IP address or unknown device
- High risk: Sign-in from an unfamiliar IP address after hours by using an unfamiliar device

Based on the risk level, multifactor authentication may not be required. Machine learning can be utilized to analyze failed sign-ins and adjust risk levels.

Lesson 4.1: Configuring Two-Factor Authentication

This lesson explains how to configure two-factor authentication.

Two-Factor Authentication: General Information

Acumatica ERP and the Acumatica mobile app provide mechanisms to support two-factor authentication, so that you can prevent unauthorized system access. Security-conscious businesses require two-factor authentication to verify users' identities before these users can be allowed to access sensitive ERP data.



This functionality is available only if the *Two-Factor Authentication* feature is enabled on the [Enable/Disable Features](#) (CS100000) form.

Learning Objectives

In this lesson, 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

Applicable Scenario

You use two-factor authentication if your company wants (or needs) to verify users' identities before allowing them to access sensitive ERP data.

Configuration of System-Wide Two-Factor Authentication

You use the settings in the **Two-Factor Authentication Policy** section on the [Security Preferences](#) (SM201060) form for setting up system-wide two-factor authentication. The settings in this section affect all of the company's users that do not have individual settings specified in the Summary area (**Two-Factor Authentication** section) of the [Users](#) (SM201010) form.

On the [Security Preferences](#) form, in the **Two-Factor Authentication** box (**Two-Factor Authentication Policy** section), you can select one of the following options:

- *Required:* Two-factor authentication is required for all users of the system who do not have a different option selected on the [Users](#) form, regardless of the specific devices or browsers used to access the web application.

- **Required for Unknown Devices:** Two-factor authentication is required for any user of the system (unless the user has a different option selected on the [Users](#) form) if the user is using a new device or browser to access the web application.



If a user is trying to access the web application by using the *Private* or *Incognito* mode of a browser, the system will require two-factor authentication with *Required for Unknown Devices* selected.

- **None (default):** Two-factor authentication is not in use in the system.

To complete the activation of two-factor authentication, you click **Save** on the form toolbar, and the system displays the **Confirm** dialog box. In the top sections of the dialog box, the system provides the following possible ways you can confirm the activation of two-factor authentication:

- A test access code sent to you by email: In the **Enter access code** box (see Item 1 in the following screenshot), you enter the access code the system has sent to the email address specified on the [Users](#) (SM201010) form for the user account you are currently signed in with.
- A generated access code: In the **Backup Option** section, you click **Generate List of Access Codes** (Item 2). The system generates a PDF document with the list of access codes. You enter an access code to the **Enter access code** box.

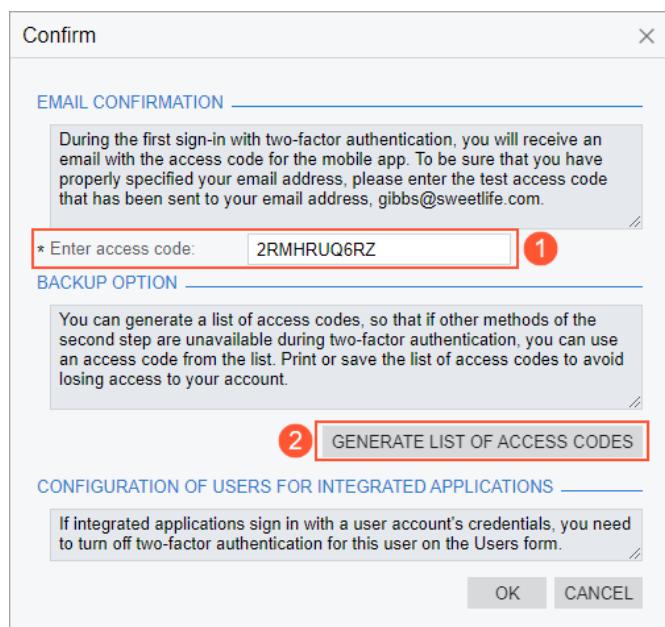


Figure: Confirm dialog box for the activation of two-factor authentication

After the two-factor authentication has been activated by entering the access code and clicking **OK** in the dialog box, every user needs to present to the system additional evidence (the second factor) of authentication in addition to the user credentials.



After the two-factor authentication has been activated system-wide, make sure that at least one user has an access code for the first sign-in to either the web application or the mobile app. Otherwise, no one will be able to sign in to the system, and you will need to contact your Acumatica ERP Support provider to resolve the situation.

Configuration of Individual Authentication

On the [Users](#) (SM201010) form, in the **Two-Factor Authentication** section of the Summary area, you select the **Override Security Preferences** check box in order to override the default system settings and specify the

two-factor authentication mode for the specific selected user. Otherwise, the settings specified on the [Security Preferences](#) (SM201060) form will be used.

Configuration of Users for Integrated Applications

If you activate two-factor authentication system-wide, the settings affect all system users. If there are integrated applications that sign in with some user credentials, you need to turn off the two-factor authentication for these users individually on the [Users](#) (SM201010) form. For each of these users, you select the **Override Security Preferences** check box and then select the *None* option in the **Two-Factor Authentication** box. For details on users for integrated applications, see [Integration Development Guide](#).

Configuration of Authentication Methods

By default, the system recommends the push notification method to authenticate the sign-in operation, as shown in the following screenshot. The push notification method of authentication requires the Acumatica mobile app to be set up on a mobile device.

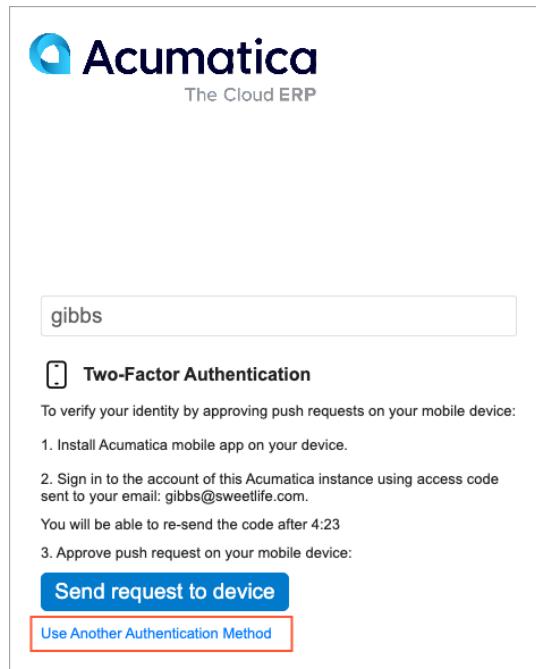


Figure: The default authentication method

If an employee of your company does not have the Acumatica mobile app installed or has turned off push notifications for the app for some reason, they can sign in by providing the system with an access code that can be delivered by email or an SMS message. Also, the list of access codes can be provided by the system administrator or generated by the user using mobile app or web application. (You can see the available authentication methods in the following screenshot.)

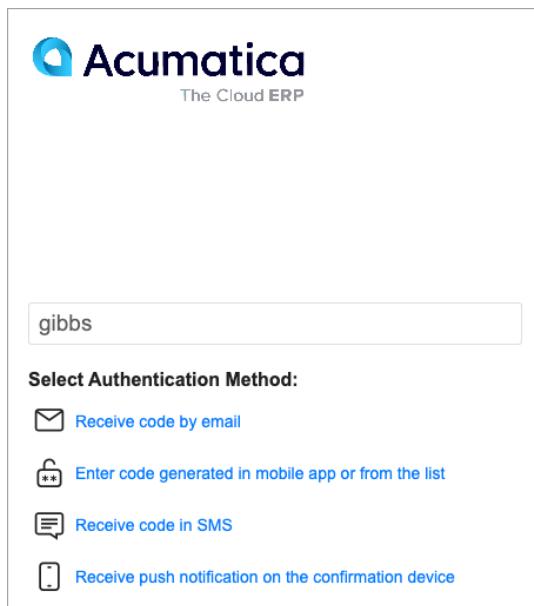


Figure: The available authentication methods



After the two-factor authentication has been activated for a user, the user may use authentication methods that involve the Acumatica app only after the user has passed authorization in the app.

Authentication by Access Code

If a user does not use the Acumatica mobile app or has turned off push notifications for the app, they can provide an access code as the second factor during authorization. There are several ways to receive an access code.

A system administrator can generate a list of access codes for a user for the first sign-in by clicking the **Generate Access Codes** button on the [Users](#) (SM201010) form. The system generates and displays the list of codes that can be exported in PDF or Excel format. Each code can be used only once and has an expiration date. The system administrator shares the list with the user securely. After the first sign-in, the user can generate the individual list of codes by using the **Generate Access Codes** button on the [User Profile](#) (SM203010) form; the user can then save the list securely.

If the receipt of an access code by email or an SMS message is configured, a user can select the corresponding authentication method on the sign-in page and enter the received code.

If a user has installed the Acumatica mobile app and has passed authorization there, the app may be used for generation of an access code. The user can click the **Generate Access Code** command in the account editing menu of the mobile app, as shown in the following screenshot.

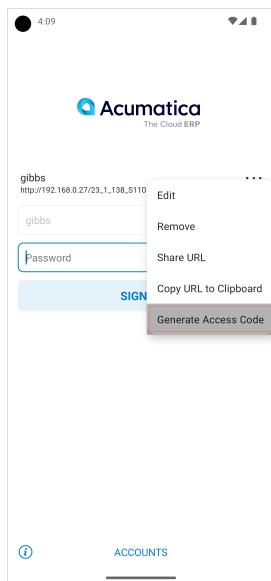


Figure: Generation of an access code by using the mobile app

Authentication by Push Notifications

If a user of the system is using the Acumatica mobile app and has allowed push notifications from the app for the applicable device, the system will send an approval request as a push notification to the mobile device, as the following screenshot demonstrates.

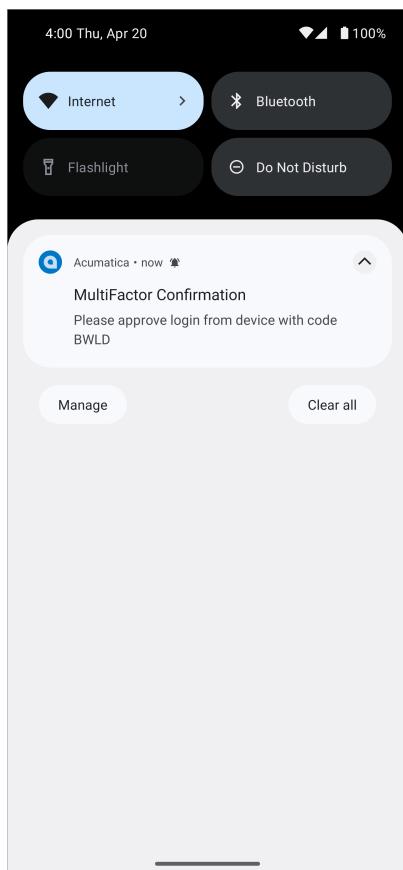


Figure: An approval request sent by the system as a push notification

The user taps **Approve** in the Acumatica mobile app, and the system completes sign-in to the web application (see the following screenshot).

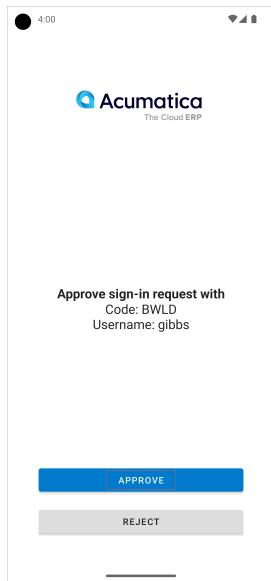


Figure: The Approve button in the Acumatica mobile app

A user can turn push notifications on or off for a registered mobile device on the **Devices** tab of the [User Profile](#) (SM203010) form. The **Send Confirmation Push** column on this tab indicates whether the push notification sign-in request will be sent to each particular device when the user tries to sign in to the web application. For details on user access through a user's mobile device, see [User Access: Mobile Devices](#).

First Sign-In to the Mobile App

If two-factor authentication is required for a particular user, the first time that the user signs in to the Acumatica mobile app, the system will request the security access code. (The following screenshot shows the prompt to enter the access code.) The user should use an access code generated for this user account by a system administrator on the [Users](#) (SM201010) form. The mobile app will also require the user's personal information number (PIN) or biometric verification when the user signs in.

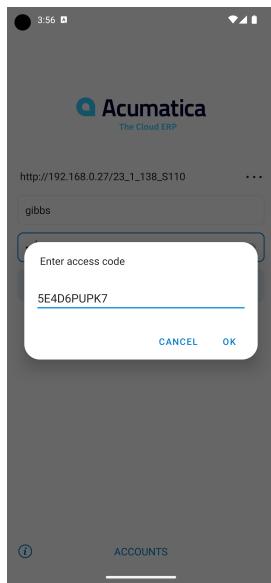


Figure: Access code entered on the first sign-in to the mobile app

Delivery of an Access Code by Email

You make possible the delivery of an access code by email by selecting the **Allow Email** check box on the [Security Preferences](#) (SM201060) form. If you do so, the system suggests this authentication method (by making the *Receive code by email* link available) on the sign-in page. When a user selects this method, the system sends a one-time access code to the email address specified for the user on the [Users](#) (SM201010) form. The following screenshot demonstrates a sample email with the access code.

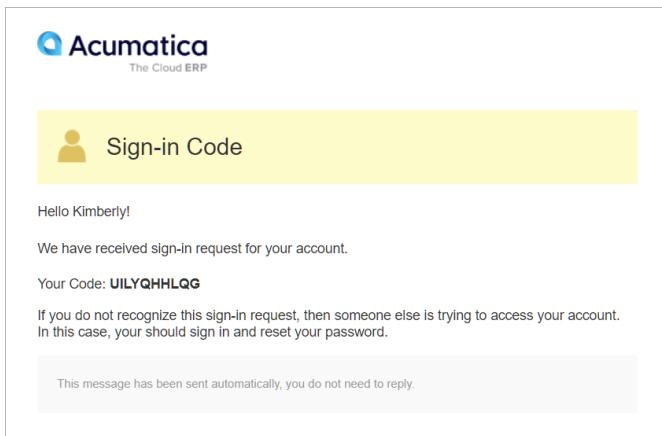


Figure: Sample email with an access code

We recommend that you make sure that all users have email addresses specified on the [Users](#) (SM201010) form, and that all the necessary actions have been performed to make it possible to send and receive emails by schedule. For details, see [Managing Emails](#).

Delivery of an Access Code in SMS

Acumatica ERP provides integration with the Twilio and Amazon SMS providers. To set up the delivery of an access code in SMS, you configure an SMS provider on the [SMS Providers](#) (SM203535) form. Then on the [Security Preferences](#) (SM201060) form, you select the **Allow SMS** check box under the **Two-Factor Authentication Policy** section. With the check box selected, the system suggests this authentication method (by presenting the *Receive code in SMS* link) on the sign-in page. When a user selects this method, the system sends a one-time access code to the phone number specified for the user on the [User Profile](#) (SM203010) form.

We recommend that you test the configuration of the selected SMS provider and make sure that all users have phone numbers specified in the system.

Two-Factor Authentication: Implementation Activity

In the following implementation activity, you will learn how to activate two-factor authentication for an individual user of the system.

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.

Process Overview

In this activity, on the [Users](#) (SM201010) form, you will turn on two-factor authentication for the *gibbs* user and generate the list of access codes there. Then you will turn on the delivery of access codes by email by using the [Security Preferences](#) (SM201060) form.

You will sign out and try to sign in with an access code. Finally, you will use the [All Emails](#) (CO409070) inquiry form to make sure that the system prepared an email with a one-time access code.

System Preparation

Before you start activating two-factor authentication, sign in to a company with the *U100* dataset preloaded. You should sign in as a system administrator with the *gibbs* username and *123* password.

Step 1: Turning On Two-Factor Authentication for a User

To turn on two-factor authentication for a user, do the following:

1. Open the [Users](#) (SM201010) form.
2. In the **Login** box of the Summary area, select *gibbs*.
3. In the **Two-Factor Authentication** section, select the **Override Security Preferences** check box.
4. In the **Two-Factor Authentication** box, select *Required*.
5. On the form toolbar, click **Save**.
6. On the form toolbar, click **Generate Access Codes**. The system opens the [Codes](#) (SM651011) report in a pop-up window.
7. On the report toolbar, click **Export > PDF**. The list of the codes is saved to your computer.

Step 2: Turning On the Delivery of Access Codes by Email

To turn on the delivery of access codes by email, do the following:

1. Open the [Security Preferences](#) (SM201060) form.
2. In the **Two-Factor Authentication Policy** section, select the **Allow Email** check box.
3. On the form toolbar, click **Save**.

Step 3: Signing In with an Access Code

To sign in with an access code, do the following:

1. In the top right corner of the screen, click the *Kimberly Gibbs* username and then select **Sign Out**.
2. On the Sign-In page, enter *gibbs* as the username and *123* as the password, and click **Sign In**. The system provides instructions for two-factor authentication.
3. Click *Use Another Authentication Method*. The system offers the list of other authentication methods available.
4. Click *Receive code by email* to make the system send you the one-time code, which you will later review by using the [All Emails](#) (CO409070) inquiry form.
5. Click *Use Another Authentication Method*, and click *Enter code generated in mobile app or from the list*.
6. Copy the first access code from the saved list of codes and paste it in the empty box.
7. Click **Sign In**.

8. Open the [All Emails](#) (CO409070) inquiry form.
9. In the list of emails, find the one with the *Sign-in Code* summary and open it. Make sure it is addressed to gibbs@sweetlife.com (which is the email address of Kimberly Gibbs) and has an access code inside.

In this activity, you turned on two-factor authentication for a user, generated the list of access codes, and saved it. Then you turned on sending of access codes by email. You verified the configuration by making the system send an access code by email, and then you signed in with a generated access code. You made sure that the system generated an email with an access code upon your request.

Optionally, as a self-guided exercise, if you have the Acumatica mobile app and can connect it to the instance you are using for completing the exercise, you can try to authenticate yourself by using the app.

Additional Materials

This part contains additional materials that are related to the lessons of the course.

The information in these appendixes will not be included in the assessment; it is provided so that you can learn more about subjects that may be useful in your work.

Appendix 1: Preparing an Instance for Implementation

This appendix contains supplemental information related to the lessons of Part 1.

Preparing an Instance: Implementation Checklist

You can use the tables in this topic to quickly check whether the preparation steps are being performed in Acumatica ERP. The following tables cover both mandatory and recommended preparation steps.



The person who performs the initial configuration uses the *admin* username and the initial password only until the accounts for the persons participating in implementation are created (in the last task of initial configuration). We recommend that after initial configuration, the users use their personal usernames and passwords to access the system.

Table: Mandatory Configuration

To ensure that the instance has been implemented properly, make sure that the necessary features have been enabled and the needed entities have been created, as listed in the following table.

Form	Criteria to Check
Enable/Disable Features (CS100000)	The default set of features has been enabled for the instance.
Activate License (SM201510)	A license key has been entered and activated. The license details are correct.

Table: Recommended Configuration

The settings listed in the following table can be specified to secure the process of implementation.

Form	Criteria to Check
Security Preferences (SM201060)	The system-wide security policy has been configured to ensure that access to the tenant in implementation is secure and to track activities performed with the tenant by people involved in the process.

Form	Criteria to Check
Users (SM201010)	<p>User accounts for people involved in the implementation have been created, by using the Users (SM201010) form.</p> <p>For each user, at least the following settings have been specified:</p> <ul style="list-style-type: none"> • Username (login) • Initial password to be changed on the first sign-in • Email address • Set of predefined roles that allow access to all system resources

Appendix 2: Securing Access to the System

This appendix contains supplemental information related to the lessons of Part 2.

User Roles: Restriction Level Options

Users are assigned to roles, and you give these roles the appropriate access rights to system objects—forms, containers of form elements, form elements, and wikis. By defining access rights for a system object, you set the restriction level (that is, the level of access rights) a user will have for this object. With Acumatica ERP, you can control access down to the control of form elements, such as buttons, text boxes, and check boxes.

This topic describes the restriction levels available to different system objects.



You can observe the tree of system objects in the left pane of forms related to user access configuration, such as [Access Rights by Screen](#) (SM201020), [Access Rights by Role](#) (SM201025), and [Access Rights by User](#) (SM201055).

Access to a Workspace

In Acumatica ERP, you do not set up access to a particular workspace itself. Instead, by setting the access rights (that is, restriction level) for the workspace, you set the access for all the nested objects. If you change the access rights to any nested object of a workspace, the system will change the access rights to *Multiple Rights* at the workspace level.

The system displays a workspace with *Multiple Rights* on the main menu. On the workspace dashboard, the system displays only forms for which access is not restricted for a particular user.

Keep in mind that a form may belong to multiple workspaces. For such a form, if you set the access rights to any of these workspaces (that is, to all forms in the workspace), the system will assign this form the restriction level set most recently for one of these workspaces. The system will then change the access rights for other workspaces to which the form belongs to *Multiple Rights*, if these workspaces had different access rights. For example, the [Vendor Details](#) (AP402000) form can be accessed from the **Payables** and **Purchases** workspaces. Suppose that both workspaces have the *Granted* restriction level assigned to the *Purchasing* role. Further suppose that you change the level for the form in the **Payables** workspace to *Revoked*. The system displays the new level for the form in the **Purchases** workspace and changes the access level to *Multiple Rights* for both workspaces.

The following table summarizes the restriction levels that a role can have to a specific workspace—that is, to all forms that belong to a particular workspace of Acumatica ERP.

Restriction Level	Description
<i>Multiple Rights</i>	Means that the role has different restriction levels to the nested objects of the workspace. If you change the level for the workspace from <i>Multiple Rights</i> to some other option, the system will automatically apply the new level to all nested objects.
<i>Revoked</i>	Denies access to all the forms in the workspace for the role. That is, all forms will get the <i>Revoked</i> restriction level. For users with the role, the menu item for the workspace does not appear on the main menu, so they cannot navigate to the workspace and its forms.
<i>Granted</i>	Allows the role complete access to all the forms in the workspace. That is, these forms will get the <i>Delete</i> restriction level. You can, however, limit or revoke access to particular forms within the workspace for the role; if you do, the system will change the access rights for the workspace to <i>Multiple Rights</i> .



You can define access rights to individual forms in the **Hidden** node (which cannot be accessed from the main menu), but not to the node itself.

Access to Reports and Generic Inquiries

A workspace may include multiple reports and inquiries along with the Acumatica ERP forms. Available restriction levels depend on tools used to develop a report or an inquiry as follows:

- Reports built with the Report Designer application and inquiries created using the *Generic Inquiry* (SM208000) form have the same list of available restriction levels that roles can have to workspaces.
- Reports built with the Analytical Report Manager toolkit and inquiries developed using C# have the same list of available restriction levels that roles can have to forms.

Access to a Form

Within each workspace, you can set the access rights that roles have to Acumatica ERP forms, which affects what users with those roles can access. The restriction level to the form is inherited by the entities and records that can be created by using the form.

The following table summarizes the restriction levels that a role can have to a specific form.

Restriction Level	Description
<i>Revoked</i>	Denies access to the form and its functionality for the role.
<i>View Only</i>	Gives the role restricted access to the form and its functionality. This level allows users with the role to view the form and any records associated with the form (in drop-down lists on other forms). This level forbids users with the role from editing details about any record, creating new records or entities of the type, and deleting records.
<i>Edit</i>	Gives the role restricted access to the form and its functionality. This level allows users with the role to view the form, select records, and edit details about any record. This level forbids users with the role from creating new records or entities of the type, and from deleting records. The Clipboard button is available on the form toolbar for users with the role.

Restriction Level	Description
<i>Insert</i>	<p>Gives the role restricted access to the form and its functionality. This level allows users with the role to view the form, select records, edit details about any record, and create new records or entities of the type.</p> <p>This level forbids users with the role from deleting records.</p> <p>The Clipboard and Insert buttons are available on the form toolbar for users with the role.</p>
<i>Delete</i>	<p>Gives the role complete access to the form and its functionality. This level encompasses the capabilities of the <i>View Only</i>, <i>Edit</i>, and <i>Insert</i> levels, while also giving users with the role the ability to delete records.</p> <p>For users with the role, the Clipboard, Insert, and Delete buttons are available on the form toolbar.</p>

Access to Containers of Form Elements

Each form includes containers of elements, such as nested forms, tabs, and grids. Each container includes multiple elements and actions. You can restrict access to any of these containers on the form. The restriction level a role has to the container is inherited by the entities and records created by using the container, if applicable. For example, if you permit access for a user role to a grid, a user with this role can access all records in this grid. By default, containers inherit the restriction level of the form to which they belong.

The following table summarizes the restriction levels that a role can have to a specific container of form elements.

Restriction Level	Description
<i>Inherited</i>	Indicates that the role's access to the container was not explicitly specified and is inherited from its form.
<i>Revoked</i>	Denies access to the container for users with the role and hides it from the form for these users.
<i>View Only</i>	<p>Gives the role restricted access to the container and its functionality. This level allows users with the role to view the container and any records associated with the container (in drop-down lists on other forms), if applicable.</p> <p>The level forbids users with the role from editing details about any record, creating new records or entities of the type, and deleting records, if applicable.</p>
<i>Edit</i>	<p>Gives users with the role restricted access to the container and its functionality. This level allows users with the role to view the container, select records, and edit details about any record, if applicable.</p> <p>The level forbids users with the role from creating new records or entities of the type, and from deleting records, if applicable.</p>
<i>Insert</i>	<p>Gives the role restricted access to the container and its functionality. This level allows users with the role to view the container, select records, edit details about any record, and create new records or entities of the type, if applicable.</p> <p>This level forbids users with the role from deleting records, if applicable.</p>

Restriction Level	Description
<i>Delete</i>	Gives the role complete access to the container and its functionality. This level encompasses the capabilities of the <i>View Only</i> , <i>Edit</i> , and <i>Insert</i> levels, while also giving users with the role the ability to delete records, if applicable.

Access to Form Elements

By default, the restriction level a role has to the form elements and actions is inherited from the container of form elements to which the elements and actions belong. In most cases, a restriction level for a container is not explicitly specified; it is set to *Inherited*. Thus, before changing a restriction level to an element or an action, you should explicitly specify a restriction level for the parent container. Then you can set access to the form elements and actions.

The following table summarizes the restriction levels that a role can have to a specific form element.

Restriction Level	Description
<i>Inherited</i>	Indicates that the role's access to the element was not explicitly specified and is inherited from its container of form elements.
<i>Revoked</i>	Denies the role access to the element and hides the element. A user with the role will not see the element on the form.
<i>View Only</i>	Makes the element read-only for users with the role. A user with the role will see the element on the form but will not be able to use it.
<i>Edit</i>	Allows the use of the element for users with the role.

User Roles: Planning of Access Configuration

Designing system security requires thorough planning and preparation. User access configuration should support business processes without exposing the company to undue risks. That is, a user should have only the access rights necessary to perform typical tasks that are clearly stated in the job description of the user.

In this topic, you will read about the approaches we recommend that you consider while planning user access to the system.

Full Access Role Approach

Small companies usually do not require a complex user access configuration that includes multiple roles and strict segregation by job responsibilities. Employees are usually multitasking, and restricting access to the system configuration is usually enough. In this case, you can design roles individually for a person or for a group of people. For example, for a company with 5 to 10 employees, you might configure two roles as follows:

- *Administrator*: Users with this role have complete access to all system objects in the system, regardless of the functional area.
- *Regular User*: Users with this role have complete access to system objects of multiple functional areas, except for areas related to the system security and user management.

Access Tier Approach

Midsized companies need more complex user access configuration because more people need to access the company's data, but job responsibilities usually are defined and segregated more clearly.

Consider the predefined set of roles that regulates access to finance-related functionality. Roles are grouped by functional areas, such as general ledger, accounts payable, and accounts receivable. Across these areas, in this set, there are three tiers of access for each functional area, which can be referred to as *Admin*, *Clerk*, and *Viewer*. The following table summarizes the different access for these tiers.

Access Tier	Adding and Processing Records	Deleting Records	Configuration Settings	Reports and Inquiries
Admin	Full access	Full access	Full access	Full access
Clerk	Full access	Full access	View only	View only
Viewer	View only	View only	View only	View only

With this configuration, you might consider assigning to each user a set of roles from either the Clerk tier or Admin tier and using roles from the Viewer tier for employees who perform internal or external audits. For example, you could assign to a senior accountant all roles from the Admin tier, thus giving complete access to the whole finance-related functionality. For the assistant accountants, you could assign roles from the Clerk tier according to their responsibilities.

Also, you might consider assigning particular users a combination of roles from different tiers. For example, a user who is doing reconciliation will need to view reports and inquiries from the general ledger and accounts payable functional areas. So in addition to the *CA Admin* role, which allows the user to perform reconciliation, you could assign to the user the *AP Viewer* and *GL Viewer* roles.

Granular Role Approach

In addition to having three tiers of access (Admin, Clerk, and Viewer), we recommend creating roles that allow users to perform granular but sensitive tasks. For example, suppose that a senior accountant with a role from the Admin tier usually reprints checks. During their vacation, the senior accountant passed this responsibility to their assistant, who has a role from the Clerk tier. By defining a role that allows a user to perform only the reprinting of checks, you can temporarily assign this role to the assistant user, instead of giving the user a role from the Admin tier, which would grant more responsibilities than you may want the user to have.

The other solution for securing access to reprinting checks is to create a role specifically for reprinting checks and restrict access to reprinting for all other roles. In this case, you can assign this role to only approved users regardless of their tier of access.

User Roles: Calculation of the Restriction Level for a User

In this topic, you will learn how the system calculates a restriction level to a system object for a user with multiple roles assigned.

Calculation of the Restriction Level to Forms

If a user has multiple roles assigned and the roles have different restriction levels to a system object, the following general rule is used: Acumatica ERP applies the most permissive level among the roles.

For example, suppose that a user is assigned the *Employee* and *Sales Manager* roles. The *Employee* role has the *Revoked* restriction level for the **Inventory** workspace, and the *Sales Manager* role has the *Granted* restriction level for the same workspace. With these settings, the user has the *Granted* restriction level to the forms in the **Inventory** workspace. The following table shows how the system calculates the final restriction level to forms of the workspace.

User Role	Restriction Level	User's Final Level to Forms
<i>Employee</i>	<i>Revoked</i>	<i>Granted</i>
<i>Sales Manager</i>	<i>Granted</i>	

Calculation of the Restriction Level to a Form's Nested Objects with the Inherited Level

If a user has multiple roles assigned and the roles have the *Inherited* restriction level to a particular container or form element, the resulting level is the most permissive level of the system object at a higher level for which a restriction level is specified explicitly—the form (for a container) or the form element container (for a form element).

Suppose that a user is assigned the *Employee* and the *Accountant* user roles. The *Employee* role has the *Revoked* restriction level to the **Customers** (AR303000) form, and the *Accountant* role has the *Edit* level to this form. The restriction level both roles have to the form elements is *Inherited*. The user with these roles, then, has the *Edit* access level to the **Customers** form and its elements. The following table shows how the system calculates the final restriction level to nested objects with the inherited level.

User Role	Restriction Level to a Form	Restriction Level to the Form's Nested Objects	User's Final Level to the Form and its Nested Objects
<i>Employee</i>	<i>Revoked</i>	<i>Inherited</i>	<i>Edit</i>
<i>Accountant</i>	<i>Edit</i>	<i>Inherited</i>	

Calculation of the Restriction Level to a Form's Nested Objects with a Specified Level

If a user has multiple roles assigned and you have explicitly specified a restriction level to a particular form element container or form element for at least one role (while the other roles have the *Inherited* level to this system object), then the resulting level of access rights is the most permissive among the roles with explicitly defined restriction levels. (In making this determination, the system ignores the levels of the roles with the *Inherited* level of access rights.) This algorithm is used to optimize the speed of loading the form.

Suppose that a user is assigned the *Employee*, *Warehouse Worker*, and *Sales Assistant* user roles. All these roles have the *Insert* restriction level to the **Receipts** (IN301000) form. For the **Release** button on this form, the *Employee* role has the *Inherited* restriction level (which the system ignores), the *Warehouse Worker* role has the *Revoked* level, and the *Sales Assistant* role has the *View Only* level. As a result, the user has the *View Only* restriction level (the most permissive level of the two explicitly defined levels) to this button. The following table shows how the system calculates the final restriction level to nested objects with a specified level.

User Roles	Restriction Level to the Form	Restriction Level to a Nested Object	User's Final Level to the Nested Object
<i>Employee</i>	<i>Insert</i>	<i>Inherited</i>	<i>View Only</i>
<i>Warehouse Worker</i>	<i>Insert</i>	<i>Revoked</i>	

User Roles	Restriction Level to the Form	Restriction Level to a Nested Object	User's Final Level to the Nested Object
Sales Assistant	Insert	View Only	

User Roles: Predefined Roles

To ease the process of defining and administering roles, Acumatica ERP provides a set of predefined roles that are stored in the System tenant (for details, see [Tenants: General Information](#)).

Some of these roles grant the users access to a specific functionality, while other roles are used by the system and should not be assigned to users manually.

Service Roles

The following service roles are available in the system:

- *AcumaticaSupport*: The role, which is reserved for the predefined *AcumaticaSupport* user, is used to give support engineers access to a tenant.
- *Anonymous*: This role is reserved for system use.
- *DashboardDesigner*: The system has automatically designated this role as the dashboard owner role for dashboards that were created in previous versions of Acumatica ERP. We recommend that you create specific roles for users who should own particular dashboards. For details, see [Administering Dashboard Forms](#).
- *Guest*: This role is used for backward compatibility.

Administrative Roles

The following administrative roles are available in the system:

- *Administrator*: A user with this role has full access to all system objects, and any access restrictions to system objects are not applied to this role. Therefore, we recommend that you assign users to this role only during initial system setup, so that these users can define roles and enter other users, and then assign the role only in extraordinary cases. We recommend that you create a separate user role for system administrators with access to only Acumatica ERP forms that are used for the configuration and management of the system.



When you add a new form, such as a generic inquiry, to the site map, we strongly recommend that you set the *Granted* level to this form for the *Administrator* role.



A user with the *Administrator* role cannot publish reports or modify original dashboards (which have an owner role other than *Administrator*).

- *BI*: A user with this role can access the *BI Views*—that is, the generic inquiries that are exposed through the OData protocol, meaning that the **Expose via OData** check box is selected for the inquiry on the [Generic Inquiry](#) (SM208000) form. For more information, see [Exposing Inquiry Results by Using OData](#).
- *BusinessDateOverride*: A user with this role can change the business date in the info area of Acumatica ERP. This role appears only if the *Secure Business Date* feature is enabled on the [Enable/Disable Features](#) (CS100000) form. For details, see [User Roles: Restrictions on Changing the Business Date](#).
- *Customizer*: A user with this role can customize Acumatica ERP applications. For details, see [To Assign the Customizer Role to a User Account](#).

- *CS Admin*: Users with this role can access system functions and configuration entities that might be needed by users in financial positions. More specifically, they have administrative permissions to configure most of the common settings, including segmented keys, numbering sequences, tasks, and business process scenarios, as well as to manage business events, notification templates, and document templates. Users with the *CS Admin* role also have full access to row-level security settings and most of the integration functions.
- *Data Privacy Controller*: A user with this role has access to the compliance tools for General Data Protection Regulation. For details, see [Handling Personal Data](#).
- *Field-Level Audit*: A user with this role can view the audit trail directly from an audited form. When you assign this role to a user, the **Audit History** command in the **Tools** menu on the form title bar becomes available to the user. The user can open any audited form, select a document created by using the form, and click **Audit History** to view the audit trail for the selected document. For details, see [Managing Field-Level Auditing](#).
- *OData4 User*: A user with this role can access data exposed through the DAC-based OData interface.



If a user does not have this role, through the DAC-based OData interface, the user has access to the same data that is visible to them via UI according to their access rights.

- *ReportDesigner*: A user with this role can publish reports in Acumatica ERP. Any user can create reports in Report Designer, but for publishing reports in Acumatica ERP, the user needs to be granted this role.
- *Wiki Admin*: A user with this role can set other users' access rights to wikis. For details, see [Wiki Access Management](#).
- *Wiki Author*: A user with this role can create wiki articles. For details, see [Wiki Access Management](#).

User Profile–Related Roles

The following roles that manage access to a user personal settings are available in the system:

- *Internal Employee*: Users with this role have full access to personal settings, tasks, events, email, and time cards, as well as expense receipts and claims. Additionally, these users can view Help.
- *Internal User*: A user with this role can change personal settings and view Help. It is automatically assigned to all user accounts linked with the *Employee* user type.

CRM–Related Roles

The following roles that manage access to CRM functionality are available in the system:

- *CR Marketing Manager*: A user with this role has access to marketing functions and settings.
- *CR Sales & Marketing Admin*: A user with this role has full access to sales and marketing functions and settings.
- *CR Sales Representative*: A user with this role has access to sales functions and settings.
- *CR Support Admin*: A user with this role has full access to support functions and settings.
- *CR Support Representative*: A user with this role has access to support functions and settings.
- *CR Viewer*: A user with this role has view-only access to marketing, sales, and support functions and settings.

Finance–Related Roles

The following roles that manage access to finance functionality are available in the system:

- *AP Admin*: A user with this role has access to functions and settings related to accounts payable, as well as view-only access to general ledger transactions.
- *AP Clerk*: A user with this role has access to accounts payable functions, as well as view-only access to accounts payable settings and general ledger transactions.

- *AP Viewer*: A user with this role has view-only access to accounts payable functions.
- *AR Admin*: A user with this role has access to functions and settings related to accounts receivable, as well as view-only access to general ledger transactions.
- *AR Clerk*: A user with this role has access to accounts receivable functions, as well as view-only access to accounts receivable settings and general ledger transactions.
- *AR Viewer*: A user with this role has view-only access to accounts receivable functions.
- *CA Admin*: A user with this role has access to cash management functions and settings.
- *CA Clerk*: A user with this role has access to cash management functions and view-only access to cash management settings.
- *CA Viewer*: A user with this role has view-only access to cash management functions.
- *CM Admin*: A user with this role has access to functions and settings related to currency management.
- *CM Viewer*: A user with this role has view-only access to currency management functions.
- *DR Admin*: A user with this role has access to functions and settings related to deferred revenue.
- *DR Viewer*: A user with this role has view-only access to deferred revenue functions.
- *FA Admin*: A user with this role has access to functions and settings related to fixed assets.
- *FA Clerk*: A user with this role has access to fixed asset functions, as well as view-only access to fixed asset settings.
- *FA Viewer*: A user with this role has view-only access to fixed asset functions.
- *Financial Supervisor*: When the **Restrict Access to Closed Periods** check box is selected on the [General Ledger Preferences](#) (GL102000) form, a user with this role can post to closed financial periods, while all other users are not able to work with these periods. A financial supervisor can also reopen *Closed* periods and unlock *Locked* periods.
- *GL Admin*: A user with this role has access to functions and settings related to the general ledger.
- *GL Clerk*: A user with this role has access to general ledger functions, as well as view-only access to general ledger settings.
- *GL Viewer*: A user with this role has view-only access to general ledger functions.
- *Project Accountant*: A user with this role can upload and process GL and PM transactions for project tasks with the *Completed*, *Canceled*, or *In Planning* status, while all other users are not able to process transactions for such project tasks.
- *TX Admin*: A user with this role has access to functions and settings related to taxes.
- *TX Viewer*: A user with this role has view-only access to tax-related functions.
- *Customer Data Manager*: A user with this role is responsible for entering master data related to customer profiles.
- *Vendor Data Manager*: A user with this role is responsible for entering master data related to vendor profiles.

Inventory and Order Management-Related Roles

The following roles that manage access to inventory and order management functionality are available in the system:

- *SO Admin*: A user with this role performs the setup of the sales orders functionality and configures the sales processes.
- *SO Manager*: A user with this role creates sales orders, manages customer contracts (such as blanket sales orders), views account receivables invoices and payments, negotiates customer terms, manages approvals, and oversees the sales operations staff and their activities.
- *SO Clerk*: A user with this role enters data of sales orders, creates customer returns, prints and sends order confirmations, and manages customer inquiries.
- *SO Viewer*: A user with this role can view the progress of the sales orders processing but cannot change the orders.

- *PO Admin*: A user with this role performs the setup of the purchase orders functionality and configures the processes of purchasing.
- *PO Manager*: A user with this role creates purchase orders, requisitions, views accounts payable bills and payments, negotiates vendor credit terms, manages vendor returns, manages approvals, and oversees the purchasing staff and their activities.
- *PO Buyer*: A user with this role procures inventory to replenish the warehouse stock levels or to fulfill orders (planning of purchases, creation of purchase orders, linking of purchase orders to fulfill sales orders), reviews seasonality and replenishment settings for optimization and procurement.
- *PO Clerk*: A user with this role enters data of purchase orders, creates vendor returns, and views inquiries and reports.
- *PO Viewer*: A user with this role can view the progress of the purchase orders processing but cannot change the orders.
- *IN Admin*: A user with this role performs the setup of the inventory functionality and configures the inventory processes.
- *IN Manager*: A user with this role analyzes and manages warehouse activities and performance, takes responsibility for the physical movement of goods to and from the warehouse as well as inventory optimization and efficiency within the warehouse, and oversees the warehouse staff and their activities.
- *IN Receiver*: A user with this role receives purchases, inbound transfers, and customer returns, puts away received goods into designated warehouse locations.
- *IN Shipper*: A user with this role picks, packs, and ships customer sales orders, outbound transfers, and vendor returns, and confirms shipments.
- *IN Clerk*: A user with this role performs cycle counts and inventory adjustments and restocks the inventory within the same warehouse according to the warehouse manager's plan.
- *IN Viewer*: A user with this role can view the documents related to the warehouse processes and inventory settings but cannot change orders and settings.
- *Inventory Data Manager*: A user with this role is responsible for entering master data related to inventory item profiles.

Manufacturing-Related Roles

Acumatica ERP also provides a number of predefined roles to manage users' access to manufacturing functionality, including the following:

- *MFG Engineer*: A user with this role has full access to the functions related to bills of material and engineering change control, as well as view-only access to bill of material settings.
- *MFG Engineering MGR*: A user with this role has full access to the functions and settings related to bills of material, except for labor codes, overhead, and shifts.
- *MFG Shop Floor*: A user with this role has view-only access to production orders, full access to clock entry functions, full access to production schedules, and view-only access to production dashboards.
- *MFG Production MGR*: A user with this role has full access to production-related functions, production-related settings, and functions related to the approval of clock entries.
- *MFG Scheduler*: A user with this role has full access to material requirements planning functions, full access to production schedules, and view-only access to material requirements planning settings.
- *MFG Scheduling MGR*: A user with this role has full access to material requirements planning functions, material requirements planning settings, production schedules, and advanced planning and scheduling maintenance.
- *MFG Planner*: A user with this role has full access to master production schedule functions, forecast functions, production schedules, and to some of the material requirements planning functions.
- *MFG Planning MGR*: A user with this role has full access to master production schedule functions and settings, forecast functions, production schedules, and some of the material requirements planning functions.

- *MFG Sales Engineer*: A user with this role has full access to estimating functions.
- *MFG Warehouse*: A user with this role has full access to material transaction functions and to lot- or serial-tracking functions.
- *MFG Viewer*: A user with this role has view-only access to production orders.
- *MFG Admin*: A user with this role has full access to all manufacturing functions and settings.

Payroll-Related Roles

The following roles for managing access to payroll functionality are available in the system:

- *PR Admin*: A user with this role has full access to payroll functions and settings, and view-only access to banking, payables, projects, finance, and configuration settings.
- *PR Clerk*: A user with this role has limited access to payroll functions (such as data entry and internal reporting), view-only access to payroll settings, and view-only access to banking, payables, projects, finance, and configuration settings.
- *PR Manager*: A user with this role has full access to payroll functions, view-only access to payroll settings, and view-only access to banking, payables, projects, finance, and configuration settings.
- *PR Viewer*: A user with this role has view-only access to payroll functions.

Self-Service Portal-Related Roles

The following roles that manage access to Acumatica Self-Service Portal are available in the system:

- *Guest*: This role is used for backward compatibility.
- *Internal Employee*: Users with this role have full access to personal settings, tasks, events, email, and time cards, as well as expense receipts and claims. Additionally, these users can view Help, and they have view-only access to payroll inquiries.
- *Internal User*: A user with this role can change personal settings and view Help. Also, these users have view-only access to payroll inquiries, such as personal pay stubs. This role is automatically assigned to all user accounts linked with the *Employee* user type.
- *Portal Admin*: A user with this role can access the Acumatica Self-Service Portal configuration forms and configure Self-Service Portal. For more information about Acumatica Self-Service Portal, see [Self-Service Portal](#).
- *Portal User*: A user with this role can access Self-Service Portal. You should assign this role only to contacts who must have access to Self-Service Portal. For more information about Acumatica Self-Service Portal, see [Self-Service Portal](#).

User Roles: Restrictions on Changing the Business Date

In Acumatica ERP, the business date is displayed in the info area, which is in the right corner of the top pane. The business date is the date that the system will insert by default into the records that you add to the system. By default, the current date is set as the business date.

Some companies might want to restrict the availability of changing the business date in the system. This can be done to avoid issues with generated documents that have the dates of closed periods inserted into them.

By default, all users can change the business date in the Acumatica ERP system.

Configuring Permissions to Change the Business Date

To restrict the availability to change the business date, you should enable the *Secure Business Date* feature on the [Enable/Disable Features](#) (CS100000) form. This will make the Business Date menu button generally unavailable for

clicking and editing, except to the employees in your company who might need the ability to change the business date in the system.

You can grant these users access rights to change the business date by assigning the *BusinessDateOverride* role to them on the [Users](#) (SM201010) form or the [User Roles](#) (SM201005) form.



This role is available only if the *Secure Business Date* feature is enabled on the [Enable/Disable Features](#) form.

Incrementing the Business Date

The system handles the incrementing of the business date at midnight individually for each user session: The date is automatically incremented at midnight only if you have not modified the business date in any way during your user session.

That is, if you do not change the business date during your user session and your session is active at midnight, the system increments the date. If you have modified the business date, the system will keep the changed date as long as your user session is active.

User Access: Related Reports and Forms

In the following sections, you can find details about the reports and forms you may want to review to gather information about user access configuration.



If you do not see a particular report or form that is described, you may have signed in to the system with a user account that does not have access rights to the report or form. Contact your system administrator to obtain access to any needed reports or forms.

Reviewing a User's Restriction Level to a System Object

You can view the user access rights for a particular form, form container, or form element by using the [Access Rights by User](#) (SM201055) form. In the Summary area of the form, you select the user account for which you want to view the access level. In the left pane, you select the node that contains the nested objects (forms, form containers, or form elements) you are interested in. Then in the right pane, you select the form, form container, or container; you then click **View Roles** on the pane toolbar. The system opens the **View Roles** dialog box, where you can view the access rights of the roles to the selected object in the **Computed Access Rights** column.

Reviewing a Role's Configuration

If you need to modify access to multiple forms for a single role, we recommend that you review the role's configuration by using the [Access Rights by Role](#) (SM651500) report. The report lists the access rights configured for every form in the system for the selected role. You can export the report data to Excel and prepare the list of needed modifications there.

Reviewing Access Rights to a Form

If you need to modify access rights to a single form for multiple roles, we recommend that you review access rights to the form by using the [Access Rights by Screen](#) (SM651700) report. For the form you select, the report lists the access rights configured for every role in the system. You can export the report data to Excel and prepare the list of needed modifications there.

Reviewing the Available Roles

For monitoring access configuration, you can review the list of roles available in the system and the user accounts assigned to each role by using the [Role List](#) (SM651000) report.

Reviewing the Roles Assigned to Users

To ensure that users are assigned only roles that support their current job responsibilities, you can review a list of the user accounts available in the system and the roles assigned to each user account on the [User List](#) (SM650500) report.

Auditing User Activity

If you need to audit the activity of a particular user, you can track the following information on the **Statistics** tab of the [Users](#) (SM201010) form:

- The date and time of the last sign-in
- The most recent date when the account was temporarily locked out
- The date and time of the most recent password change
- The number of unsuccessful attempts the user made to sign in to the account

Reviewing the Access History of Users

On the [Security Preferences](#) (SM201060) form, you can select the types of events the system will monitor and specify the time period for which the audit trail must be kept.

You use the [Access History](#) (SM201045) form to view the audit trails. The audit trail for each event type shows the time when the event took place, the user who performed the operation, the IP address from which the user signed in to the system, and other settings, depending on the event type. You can narrow the range of the listed events by user, date range, and operation type.

User Access: Mobile Devices

Users of the system can use the Acumatica mobile app to perform their job responsibilities. They just need to download the application to a mobile device and enter the connection parameters: the Acumatica ERP website address and the user credentials. The system keeps track of only those devices for which a user has allowed push notifications from the app.

Registering Mobile Devices

If a user of the system is using the Acumatica mobile app and has allowed push notifications from the app for a device, the information about this device is stored in their Acumatica ERP user profile. The details can be viewed on the **Devices** tab of the [User Profile](#) (SM203010) form.

When a user signs in to the mobile app for the first time, the application sends details about the device to Acumatica ERP, and then the information is updated with each subsequent sign-in.

The system administrator can manage the registered devices of a user on the **Devices** tab of the [Users](#) (SM201010) form.

Deleting Mobile Devices

For any user, you can delete any registered device listed on the **Devices** tab of the [Users](#) (SM201010) form by clicking it and clicking the standard **Delete Row** button on the table toolbar, or you can delete all devices for a user by clicking the **Delete All** button on this toolbar.

Enabling Push Notifications

You can control to which devices the system can send push notifications on the **Devices** tab of the [Users](#) (SM201010) form. In the row listing each device, you can use the **Turn On Notifications** check box to selectively allow or disallow these notifications for the device. You can also enable or disable sending push notifications for all of this user's devices by clicking the **Enable All** and **Disable All** buttons, respectively, on the table toolbar.

If push notifications are disabled for a device, the owner of this device will not be able to use the following functionality that uses push notifications:

- Receiving a push notification if a business event occurred. For details, see [Using Business Events](#).
- Uploading images to Acumatica ERP by using a mobile device. For details, see [Managing External Storage for File Attachments](#).
- Using two-factor authentication. For details, see [Managing Two-Factor Authentication](#).

Tracking User Location

In Acumatica ERP, you can view the GPS location coordinates of users that are tracked through their mobile devices. To be able to view a user's coordinates in the system, you have to configure location tracking for each necessary user on the [Users](#) (SM201010) form. You use the **Location Tracking** tab to turn on the tracking functionality for the selected user, specify the time and distance intervals at which the coordinates will be tracked in the system, and specify on which days and during which time periods the system registers the user location. For detailed instructions on how to turn on and configure the location tracking, see [To Turn On Location Tracking of a User](#).



For GPS location coordinates to be tracked, on the user's device, GPS location recording has to be switched on.

You can view the history of the location coordinates of all users that have been tracked in the system on the [Location Tracking History](#) (SM202000) form.

Digital Certificates: Implementation Checklist

The following sections provide details you can use to ensure that the system is configured properly for using digital certificates for database encryption or signing PDF documents generated in Acumatica ERP, and to understand (and change, if needed) the settings that affect the processing workflow.

Implementation Checklist

We recommend that before you use digital certificates, you make sure the needed features have been enabled, settings have been specified, and entities have been created, as summarized in the following checklist.

Form	Criteria to Check
File Upload Preferences (SM202550)	Digital certificates used by Acumatica ERP have the .pfx extension. Before you can import digital certificates into the system, make sure .pfx is on the list of allowed extensions.
Encryption Certificates (SM200530)	Make sure that the list of needed certificates has been uploaded here and passwords are specified for each one. Only certificates that are added to this form can be used for replacing database encryption algorithm used in Acumatica ERP or signing PDF files.
Security Preferences (SM201060)	Make sure that one of the uploaded certificates is specified in the PDF Signing Certificate box. This certificate will be used for PDF files generated for reports in Acumatica ERP.

Other Settings That Affect the Workflow

You can assign the process of replacing the certificate used for database encryption to a schedule by using the **Schedule** menu on the [Certificate Replacement](#) (SM200535) form toolbar. For more information, see [Automated Processing: General Information](#).

Validation of Configuration

To make sure that all configuration has been performed correctly, we recommend that in your system, you perform instructions similar to those described in [Digital Certificates: To Encrypt the Database](#).

Appendix 3: Monitoring User Activities

This appendix contains supplemental information related to the lessons of Part 3.

Field-Level Auditing: Implementation Checklist

The following sections provide details you can use to ensure that the system is configured properly for the use of field-level auditing, and to understand (and change, if needed) the settings that affect the processing workflow.

Implementation Checklist

We recommend that before you initially audit user activity on any form, you make sure the needed features have been enabled, settings have been specified, and entities have been created, as summarized in the following checklist.

Form	Criteria to Check
Enable/Disable Features (CS100000)	The <i>Field-Level Audit</i> feature has been enabled.

Form	Criteria to Check
Multiple forms	The needed access has been configured for the administrators who will use the field-level auditing functionality according to the company's security policy. For details, see User Roles: General Information and User Access: General Information .
Multiple forms that support field-level functionality	Auditing of the forms has been configured and enabled, as demonstrated in the example of Field-Level Auditing: Implementation Activity .

Validation of Configuration

To make sure that all configuration has been performed correctly, we recommend that in your system, you review audit trails by performing instructions similar to those described in [Field-Level Auditing: Process Activity](#).

Appendix 4: Using Multifactor Authentication Methods

This appendix contains supplemental information related to the lessons of Part 4.

Two Factor Authentication: Implementation Checklist

The following sections provide details you can use to ensure that the system is configured properly for using the two-factor authentication functionality, and to understand (and change, if needed) the settings that affect the processing workflow.

Mandatory Configuration

We recommend that before you initially activate two-factor authentication for the users of your system, you make sure the needed feature has been enabled.

Form	Criteria to Check
Enable/Disable Features (CS100000)	The <i>Two-Factor Authentication</i> feature has been enabled.

Recommended Configuration for Authentication by Using the Acumatica Mobile App

The settings listed in the following table should be specified if you want to activate authentication by using the Acumatica mobile app.

Form	Criteria to Check
Activate License (SM201510)	A valid license has been activated for the instance. If a license has not been activated, two-factor authentication by push notifications cannot be used. For more details, see Preparing an Instance: To Enable Features and Activate the License .

Form	Criteria to Check
Web Server IIS	The Acumatica ERP instance has been deployed by using the HTTPS protocol; otherwise, two-factor authentication by push notifications cannot be used. For details, see Preparation for the Acumatica ERP Installation: System Environment .
A mobile device of a user	The Acumatica app has been installed and push notifications have been allowed for the app.

Recommended Configuration for Delivering Access Codes by Email

The settings listed in the following table can be specified to set up the delivery of access codes by email.

Form	Criteria to Check
Email Accounts (SM204002)	A system email account has been configured as described in Configuring Email Accounts .
Send and Receive Email (SM507010)	All the necessary actions for sending and receiving emails by using a schedule have been performed. For details, see To Create a Send and Receive Email Schedule .
Users (SM201010)	Make sure that all users have email addresses specified on this form.
Security Preferences (SM201060)	The Allow Email check box is selected under the Two-Factor Authentication Policy section.

Recommended Configuration for Delivering Access Codes by SMS

The settings listed in the following table should be specified to configure the delivery of access codes by short message service (SMS).

Form	Criteria to Check
SMS Providers (SM203535)	An SMS provider (Twillio or Amazon SMS) has been configured.
User Profile (SM203010)	Make sure that all users have phone numbers specified on this form.
Security Preferences (SM201060)	The Allow SMS check box is selected under the Two-Factor Authentication Policy section.

Validation of Configuration

To make sure that all configuration has been performed correctly, we recommend that in your system, you perform instructions similar to those described in [Two-Factor Authentication: Implementation Activity](#).

Multifactor Authentication in Acumatica ERP

This topic describes possible strategies to use multifactor authentication in Acumatica ERP.

Single Sign-On

The best way to implement multifactor authentication in Acumatica ERP is to take advantage of Acumatica's single sign-on (SSO) capabilities. Currently, Acumatica ERP supports SSO with the following multifactor authentication providers:

- **Microsoft:** Azure multifactor authentication supports phone calls, text messages, mobile app notification, and third-party tokens. For more information, see [How Azure Multi-Factor Authentication works](#).
- **Google:** Google offers two-factor authentication via mobile phone or USB security key. For more information, see [Google 2 Step Verification](#).
- **OneLogin:** A customization project is required for the use of OneLogin. Free and paid two-factor authentication options include a one-time password app, Duo Security, RSA SecurID, and mobile options. For more information, see [OneLogin MultiFactor Authentication](#).

With the use of one of these multifactor authentication providers, users sign in to a provider by using multiple authentication options. The user is then seamlessly signed into Acumatica ERP by using the SSO functionality (see the following screenshot).

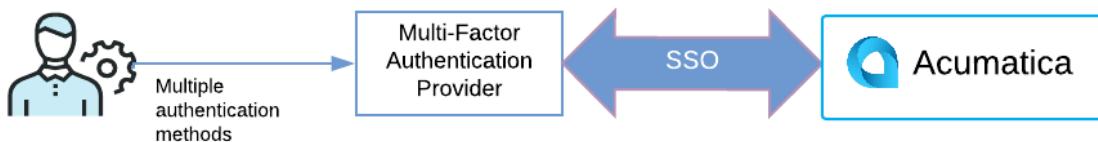


Figure: User sign-in model

Virtual Private Network (VPN)

An alternate strategy involves setting up a virtual private network (VPN). The VPN serves as the first layer of authentication, while the Acumatica ERP username and password act as the second layer.