

# System Administration

---

## S110 System Security

## Training Guide

# Contents

<b>Copyright.....</b>	<b>4</b>
<b>How to Use This Course.....</b>	<b>5</b>
<b>Company Story.....</b>	<b>7</b>
<b>Part 1: Preparing an Instance for Implementation.....</b>	<b>9</b>
Preparing an Instance: General Information.....	9
Lesson 1.1: Activation and Licensing.....	9
Preparing an Instance: Activation and Licensing.....	10
Preparing an Instance: To Enable Features and Activate the License.....	12
Lesson 1.2: Configuring System-Wide Security.....	15
Preparing an Instance: System-Wide Security Policy.....	15
Preparing an Instance: To Configure Secure Access for Implementers.....	17
<b>Part 2: Securing Access to the System.....</b>	<b>23</b>
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.....	32
Lesson 2.2: Setting User Access.....	34
User Access: General Information.....	34
User Access: User Access Security.....	37
User Access: To Add a User Account.....	38
User Access: To Assign a Role to Multiple Users.....	39
User Access: To Modify Access for a User Account.....	40
Lesson 2.3: Encrypting with Digital Certificates.....	41
Digital Certificates: General Information.....	41
Digital Certificates: To Encrypt the Database.....	43
<b>Part 3: Monitoring User Activities.....</b>	<b>45</b>
Lesson 3.1: Using System-Wide Security Auditing.....	45
System-Wide Security Auditing: General Information.....	45
System-Wide Security Auditing: Process Activity .....	46
Lesson 3.2: Using Field-Level Auditing.....	48
Field-Level Auditing: General Information.....	48
Field-Level Auditing: Implementation Activity.....	51
Field-Level Auditing: Process Activity.....	54
<b>Part 4: Using Multifactor Authentication Methods.....</b>	<b>58</b>
General Purpose and Types of Multifactor Authentication.....	58
Lesson 4.1: Configuring Two-Factor Authentication.....	59
Two-Factor Authentication: General Information.....	59
Two-Factor Authentication: Implementation Activity.....	66
<b>Additional Materials.....</b>	<b>68</b>
Appendix 1: Preparing an Instance for Implementation.....	68
Preparing an Instance: Implementation Checklist.....	68

Preparing an Instance: Acumatica ERP Features.....	69
Appendix 2: Securing Access to the System .....	85
User Roles: Restriction Level Options.....	85
User Roles: Planning of Access Configuration.....	89
User Roles: Calculation of the Restriction Level for a User.....	90
User Roles: Predefined Roles.....	91
User Roles: Restrictions on Changing the Business Date.....	95
User Access: Related Reports and Forms.....	96
User Access: Mobile Devices.....	97
Digital Certificates: Implementation Checklist.....	98
Appendix 3: Monitoring User Activities.....	99
Field-Level Auditing: Implementation Checklist.....	99
Appendix 4: Using Multifactor Authentication Methods.....	100
Two Factor Authentication: Implementation Checklist.....	100
Multifactor Authentication in Acumatica ERP.....	101

# Copyright

---

© 2021 Acumatica, Inc. ALL RIGHTS RESERVED.

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

11235 SE 6th Street, Suite 140 Bellevue, WA 98004

## 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: 2021 R1

Last Updated: 05/31/2021

# How to Use This Course

---

This 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. The course consists of lessons that guide you step by step through the examples and explanations of the configuration and business process workflow in Acumatica ERP.

This course must be completed on Acumatica ERP 2021 R1. For this course, you will use the following two 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 pre-configured settings and entities you will need as you complete the course. (You can find detailed instructions on creating a tenant below).

You perform the following general steps to complete the course:

1. You prepare an Acumatica ERP 2021 R1 instance, as described in [How to Create a Tenant with the U100 Dataset](#).
2. You create one more tenant without any preloaded dataset, using the [Tenants](#) (SM203520) form. In this tenant, you complete all the lessons from the Part 1 of the course.
3. In the tenant with the *U100* dataset preloaded, you complete all the lessons from the Part 2, Part 3, and Part 4.
4. At Partner University, you take S110 Certification Test 2021 R1.
5. At Partner University, you complete the course survey to finish the course and get the Partner University certificate of course completion.

## What Is in a Lesson?

Each 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. If additional configuration needs to be performed before you complete a process activity, the lesson also includes an implementation activity that needs to be completed before you start completing the process activity.

Each activity provides a story describing a particular user scenario, an overview of the relevant functionality, a brief overview of the process, and instructions that guide you through the process that should be performed to complete the described scenario.

The lessons of the guide are independent and can be completed in any order. However, depending on the sequence in which you take the course lessons, the values in the screenshots may differ from the values in the system.

## What Is in the Appendices?

The appendices provide additional information related to the lessons. For example, an appendix could include a description of generated transactions, information about reports and inquiry forms that can be used for gathering information related to a described business process, and explanations on how to mass-process documents while a business process is being performed.

## What Are the Documentation Resources

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 to bring up a form-specific Help menu; you can use the links on this menu to quickly access form-related concepts and procedures and to open a reference topic with detailed descriptions of the form elements.

## How to Create a Tenant with the U100 Dataset

To add to an existing Acumatica ERP instance a tenant with the *U100* dataset, which is required for the completion of this course, and prepare the tenant for completing the activities, perform the following instructions:

1. Go to [Amazon Storage](#).
2. Open the folder of your Acumatica ERP instance version.
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**.
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 to the **Snapshots** tab of the [Tenants](#) form.

10. On the form toolbar, click **Restore Snapshot**.
11. If the **Warning** dialog box appears, click **Yes**.
12. 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.

You are now on the Sign-In page, and you can sign in to the tenant you have just created.

## Licensing Information

For educational purposes of this course, you use Acumatica ERP under the trial license that does not require activation and provides all available features. For 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 sales policy for details.

# Company Story

---

This topic explains the organizational structure and operational activity of the company with which you will work 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.
- **Service and Equipment Sales Center:** This branch is a service center with a small warehouse where juicers are stored. This branch assembles juicers, sells juicers, installs juicers, trains customers' employees to operate juicers, and provides juicer servicing.

The ToadGreen Building Group is a subsidiary of the SweetLife Fruits & Jams company. ToadGreen Building Group—which is located in New York—is a general contractor coordinating construction projects for governmental and commercial customers. The company has only one branch, ToadGreen Building Group, in which the corresponding projects are being managed and all construction-related tasks are recorded.

The Muffins & Cakes company is a subsidiary SweetLife Fruits & Jams company. Muffins & Cakes—which is located in Denver, Colorado—consists of the following branches:

- **Muffins Head Office and Wholesale Center:** This branch owns a bakery and a wholesale warehouse where products are stored.
- **Muffins Retail Shop:** This branch, which sells products to retail customers, has a retail shop with a small warehouse.

## Operational Activity

The company has been operating starting in the *01-2020* financial period. In November 2020, 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. Because the company has grown, the equipment center has begun its operations in *01-2021*.

In October 2020, the company received an investment and opened a subsidiary company for construction (ToadGreen). In February 2020, the company started its first construction project.

The Muffins & Cakes company was established in January 2020 and started using Acumatica ERP at the end of the *01-2021* financial period.

## 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 for sale from a large juicer vendor and either purchases the installation service for the juicers or provides the installation service on its own, depending on the complexity of the installation.

The Muffins & Cakes company also purchases stationery (printing paper, pens, and pencils) and advertising services.

## **Company Sales and Services**

Each 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 cafés. 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).
- **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 one-time endeavors as well as complex projects with their own budgets.

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).

The Muffins & Cakes branches have the following business processes:

- **Muffins Head Office & Wholesale Center:** In this branch, baked goods and products for baking are sold to wholesale customers, such as restaurants and cafés. The company also conducts baking classes at customer locations.
- **Muffins Store:** In the store, small retail customers purchase baked goods, or pick the goods ordered on the website.



# Part 1: Preparing an 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 chapter, 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 Scenarios

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: Activation and Licensing

---

## 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.

### License Obtainment

You obtain a license by creating a support case through the [Partner Portal](#). You submit the following information:

- **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 licensing server to validate licenses. If the server where you installed Acumatica ERP instance has no access to internet, due to 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.



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

You apply the license file by clicking **Upload License File** on the form toolbar, and then select and upload the license file by using the **Upload New License File** dialog box.

### 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 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 the default set of features is enabled, you are able to 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 available.

### Product Features

Acumatica ERP provides a 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.

Only after you enable a feature do all feature-related forms and individual elements 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 settings on the form reflect the actual set of 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 in this mode all features are available, the mode has the following restrictions:

- You can create no more than 10 tenants per instance.
- All tenants that you create have the *Test* status. For details on test tenants, see [Support of Multiple Tenants](#) in the Acumatica ERP System Administration Guide.
- Only two conventional users can concurrently use the system. 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, followed by the *Activate* link you can click to activate a license: *Your product is in trial mode. Only two concurrent users are allowed.*
- 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 signing in.

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](#) 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 utilize 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](#).



During licensing and activation, the application instance is restarted. When you apply a license on 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.

If you use Acumatica Self-Service Portal, you have to obtain a license for the Self-Service Portal instance, activate the license, and then activate the required Self-Service Portal features. For details, see [Configuring Acumatica Self-Service Portal](#).

## 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:

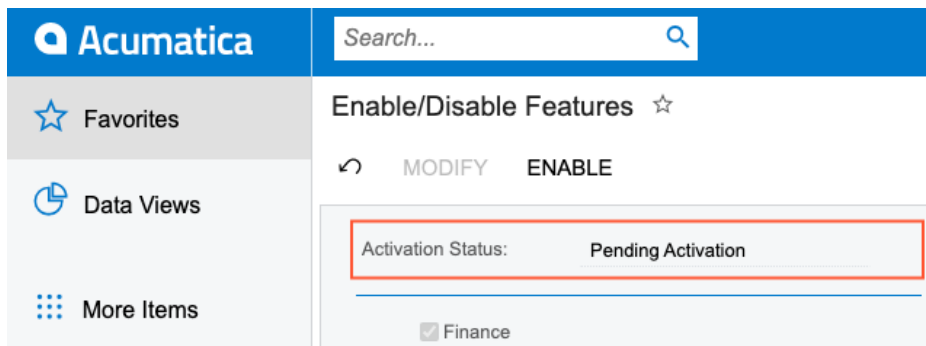
1. You have installed an unlicensed Acumatica ERP instance in a tenant without any preloaded dataset (out-of-the-box).
2. You make sure that the port 443 is opened on the computer running the Acumatica ERP instance. You may have to open port 443 if the computer has a firewall enabled.
3. You have signed 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

### 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.

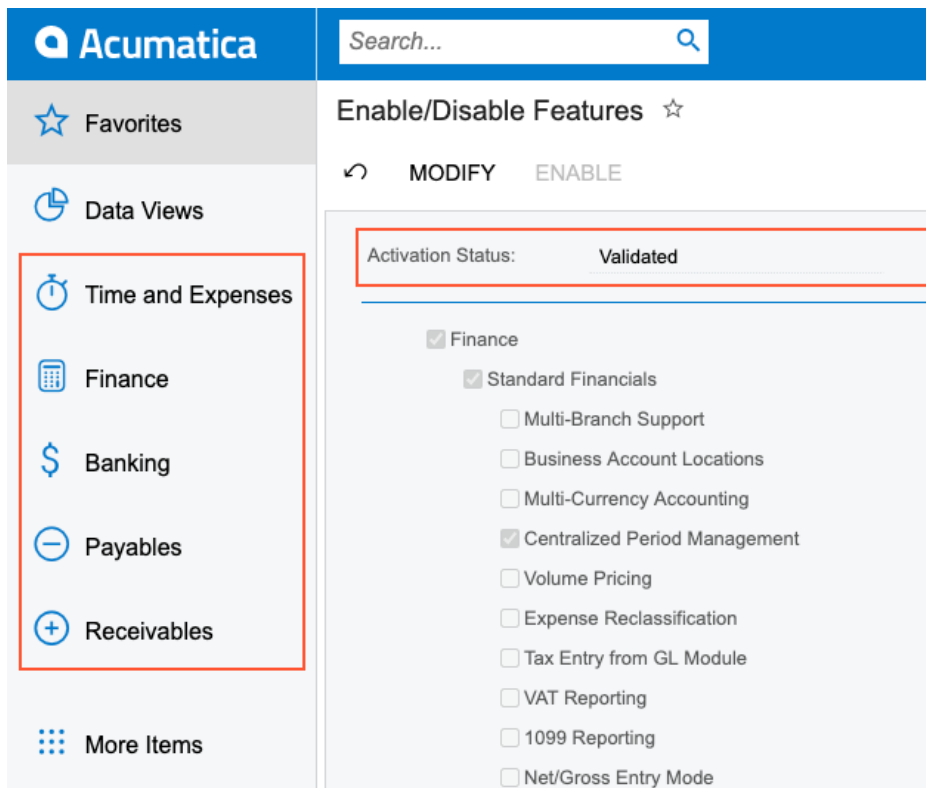
Notice that a number of features are selected by default and the activation status is *Pending Activation*, as shown in the following screenshot.



**Figure: Activation status of initial features**

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

The status of the currently selected feature set 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 any 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.
2. On the form toolbar, click **Enter License Key**; in the **Activate New License** dialog box, enter the 918B-A728-0569-7FC6-D058 license key, and click **OK**. 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.

3. 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, and close the dialog box.
4. In the Summary area, review the license status (*Valid*), its validity period, and the number of users and tenants.
5. In the table, review the features that this license supports, and make sure that the feature list is correct.



You can filter the list of features by the **Activated** column.

6. 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.

License Monitoring Console ☆

LICENSE

STATISTICS

WARNINGS

CONSTRAINT HISTORY

License Status:

Valid

• License Tier:

S Series, Tier 1

LICENSE DETAILS

Monthly Number of Commercial Transactions:

1000

Monthly Number of ERP Transactions:

20000

Database Storage Included (GB):

1

RECOMMENDED MAXIMUMS

Daily Commercial Transactions:

100

Daily ERP Transactions:

2000

Concurrent Users:

3

SYSTEM CONSTRAINTS

Maximum Number of Web Services API Users:

10

Maximum Number of Concurrent Web Services API Requests:

3

Maximum Number of Web Services API Requests per Minute:

50

Maximum Number of Fixed Assets:

1000

Maximum Number of Inventory Items:

50000

Maximum Number of Business Accounts:

50000

Maximum Number of Lines per Transaction:

1000

Maximum Number of Serial Numbers per Document:

2000

Maximum Number of Employees Paid by Month:

0

Figure: License Monitoring Console

## Lesson 1.2: Configuring System-Wide Security

### 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 **Force User to Change Password Every x Days** check box to specify the change frequency.
- *Password length*: You can set up a minimum required password length. You use the **Minimum Password Length x Characters** 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 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 the incorrect passwords.

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

## 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 one that you have entered 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 **Force User to Change Password Every** check box, and type 180 into the **Days** box next to it.
3. Select the **Minimum Password Length** check box, and type 10 into the **Characters** box next to it.

4. Select the **Password Must Meet Complexity Requirements** check box to 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 ".
7. On the form toolbar, click **Save**.

## Step 2: Configuring Account Lockout Policies

To configure the organization's account lockout policies, do the following while you are still on the [Security Preferences](#) (SM201060) form:

1. In the **Account Lockout Policy** section, in the **Lock Account After x Unsuccessful Login Attempts** box, type 3.
2. In the **Lock Account for x Minutes** box, type 15.
3. In the **Reset Lockout Counter After x Minutes** box, type 10.
4. On the form toolbar, click **Save**.

## Step 3: Adding a User Account

To add a user account in the system, do the following:

1. Open the [Users](#) (SM201010) form.
2. On the form toolbar, click **Add New Record**.
3. In the **Login** box of the Summary area, type gibbs.
4. Clear the **Generate Password** check box.
5. In the **Password** box, type Welcome123.
6. Enter the following user settings:
  - **First Name:** Kimberly
  - **Last Name:** Gibbs
  - **Email:** gibbs@sweetlife.com
  - **Comment:** Senior system administrator
7. Enter 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
8. 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*
9. On the form toolbar, click **Save**.
10. Click **Add New Record** on the form toolbar to add one more user, and specify the following settings in the Summary area:
- **Login:** prado
  - **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
11. 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*
12. 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 the 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.



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 ".

gibbs

.....

New Password

Confirm Password

Sign In

**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.



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

**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

---

### Lesson 2.1: Configuring User Roles

---

#### 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, a system object to which access rights can be set up can be 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 chapter, 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:

- When 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
- When you, as a system administrator, were notified that a 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
- When you, as a system administrator, were notified about a new position being added 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.

Acumatica ERP has the *Not Set* restriction level, which is specific for the system. The *Not Set* restriction level indicates that all roles have access to a form, including its nested objects, until at least one role is assigned any other restriction level to this form. All roles with the *Not Set* level are then denied access to the form. For example, suppose that you have created a new generic inquiry and added it to a workspace. By default, all roles in the system will be assigned the *Not Set* restriction level to the inquiry. If you assign any other restriction level to at least one role, users that are not assigned this role will not have access to the inquiry.

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 a container.
5. *Form element*: An element node is on the lowest level of the object hierarchy and inherits its access rights from its parent container.



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 a 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 using 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. 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 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, a newly created role has the *Not Set* restriction level 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.

Because Acumatica ERP is supplied with a set of predefined roles for which access rights have been specified (that is, these roles' restriction levels to different objects were changed from *Not Set* to restriction levels appropriate for each role), a newly created role will be denied access to most system objects.



The *Not Set* restriction level indicates that all roles have access to a form, including its nested objects, until at least one role is assigned any other restriction level to this form. All roles with the *Not Set* level are then denied access to the 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. This information can be useful when you define the access rights to this object for a particular role because it may affect the access rights of other roles if the *Not Set* restriction level is specified for them.

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

Alternatively, you can use the [Access Rights by Role](#) (SM201025) 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](#) or [Access Rights by Role](#) 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 a role may differently affect users with the role assigned. 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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

### 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, we 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

Before you start configuring roles, sign in to a company with the *U100* dataset preloaded. You should sign in as a system administrator with the following credentials:

- Username: *gibbs*
- Password: *123*

## Step 1: Creating Roles

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

1. Open the [User Roles](#) (SM201005) form.
2. On the form toolbar, click **Add New Record**.
3. In the **Role Name** box, type `AA_GL_Configurator`.
4. In the **Role Description** box, type `Role to access GL configuration settings`.
5. On the form toolbar, click **Save**.
6. By repeating the actions performed in the previous instructions, add three more roles with the following settings:
  - **Name:** `AA_GL_Manager`; **Description:** `Role for working with GL entities and viewing settings`
  - **Name:** `AA_GL_Clerk`; **Description:** `Role for entering and editing records`
  - **Name:** `AA_GL_Auditor`; **Description:** `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 *Not Set* 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), from 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*: *Not Set*
  - *AA\_GL\_Manager*: *Delete*
  - *AA\_GL\_Clerk*: *Not Set*
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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

## Story

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

## 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 top of the list, combined with `_AP` to indicate the functional area.

You will use the [Access Rights by Screen](#) (SM201020) form to set the access rights to the [Release Payments](#) (AP505200) form, which contains the *Reprint* and *Reprint With New Number* operations. The new role is to be used only in combination with a role that gives full access to the accounts payable functionality, but you cannot configure access to the actions if an explicit restriction level is not specified for the form. Thus, you will revoke access to the form for the new role, because you need to allow access to only two elements, access to the other functionality of the form will be provided by the accompanying role.

You will use the [Access Rights by Screen](#) 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](#) form. You can exclude from consideration the roles that have the *Not Set*, *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 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
<i>AA_AP_Reprint_Checks</i>	<i>Not Set</i>	<i>Revoked</i>	<i>Inherited</i>	<i>Revoked</i>	<i>Inherited</i>	<i>Edit</i>
<i>Accountant</i>	<i>Delete</i>	<i>Delete</i>	<i>Inherited</i>	<i>Delete</i>	<i>Inherited</i>	<i>Revoked</i>
<i>Purchasing Manager</i>	<i>Delete</i>	<i>Delete</i>	<i>Inherited</i>	<i>Delete</i>	<i>Inherited</i>	<i>Revoked</i>

## 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 system administrator with the following credentials:

- Username: *gibbs*
- Password: *123*

### Step 1: Creating a Role

To create a role, do the following:

1. Open the [User Roles](#) (SM201005) form.
2. On the form toolbar, click **Add New Record**.
3. In the **Role Name** box, type *AA\_AP\_Reprint\_Checks*.
4. In the **Role Description** box, type *Role to reprint AP checks*.
5. On the form toolbar, click **Save**.

### Step 2: Setting the Access Rights to the Form

To set the new role's restriction level to the form, do the following:

1. Open the [Access Rights by Screen](#) (SM201020) form.
2. In the left pane, expand the **Payables** node and select the **Release Payments** node.
3. In the right pane, for the *AA\_AP\_Reprint\_Checks* role, in the **Access Rights** column, select *Revoked*.
4. On the form toolbar, click **Save**.

### Step 3: 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. While remaining on the [Access Rights by Screen](#) (SM201020) form, in the left pane, expand the **Release Payments** node, and select the **ReleaseChecksFilter** node, which is the container for the reprint operations.
2. 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**.
3. In the left pane, expand the **ReleaseChecksFilter** node, and select the **Reprint** element.
4. 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.
5. On the form toolbar, click **Save**.
6. Modify the access rights for the **Reprint With New Number** element in the same way.

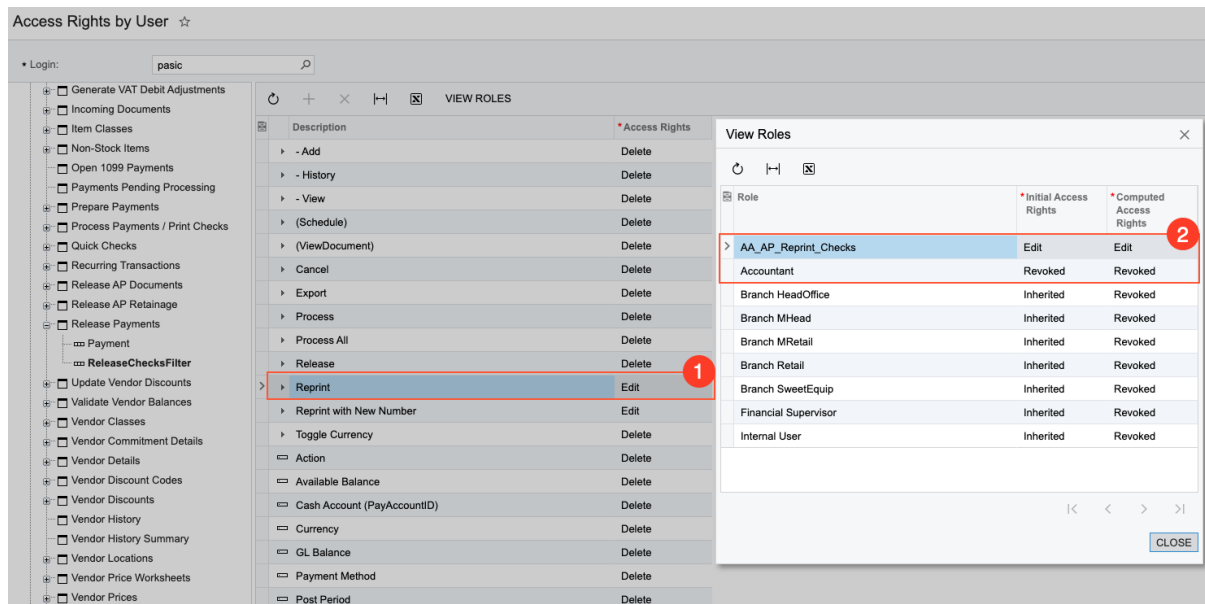
You have created and configured a role with access to only one form, and you have restricted the access to two operations on this form for other roles in the system that have access to this form.

### 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 to 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](#) (SM201055) form.

10. In the **Login** box, again select *pasic*. You have assigned this user to the *AA\_AP\_Reprint\_Checks* role, and it was already assigned to 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 access to the **Reprint** and **Reprint With New Number** elements is allowed.
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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.



## Story

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

## 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 workspace.

## System Preparation

Before you start modifying a copied role, sign in to a company with the *U100* dataset preloaded. You should sign in as a system administrator with the following credentials:

- Username: *gibbs*
- Password: *123*

## 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. In the **Role Description** box, add *Junior* to the copied description.
6. 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 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* 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 User Access

---

### 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 chapter, 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:

- When you, as an implementation consultant, initially implement Acumatica ERP for your client and are ready to give access to company employees
- When you, as a system administrator, were notified about a new hire and need to give appropriate access to the system for the new employee

- When 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 to which no roles have been assigned 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 Azure Active Directory](#).

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 [Single Sign-On with Google](#) and [Single Sign-On with Microsoft Account](#).

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 Account Creation

When you configure access for users 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, fills in the **Password** box with the masked password. 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 companies data, to identify unexpected or unwanted access behavior.

You can use reports and inquiries 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 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 user name 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 at will 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 **Force User to Change Password Every x 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 **Force User to Change Password Every x 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](#) (SM201010) 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.

## User Access: To Add a User Account

The following activity will walk you through the process of adding a user account.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

## Story

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

## Process Overview

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

## System Preparation

Before you start performing the step of this activity, you should sign in to a company with the *U100* dataset preloaded. Sign in as a system administrator with the following credentials:

- Username: *gibbs*
- Password: *123*

## Step: Adding the User Account

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

1. Open the [Users](#) (SM201010) form.
2. On the form toolbar, click **Add New Record**.
3. In the **Login** box of the Summary area, type `kent`.
4. Clear the **Generate Password** check box.
5. In the **Password** box, type `Welcome123`.
6. Specify the following settings for this user:
  - **First Name:** `Sarah`
  - **Last Name:** `Kent`
  - **Email:** `kent@sweetlife.com`
  - **Comment:** `Warehouse worker`
7. 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
8. On the **Roles** tab, assign the following roles to the user by selecting the check box in the **Selected** column:
  - *Branch HeadOffice*
  - *Internal User*
  - *Warehouse Worker*
9. 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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

## 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.

## System Preparation

Before you start performing the step of this activity, you should sign in to a company with the *U100* dataset preloaded. Sign in as a system administrator with the following credentials:

- Username: *gibbs*
- Password: *123*

## 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.





The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

## Story

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

## Process Overview

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

## System Preparation

Before you start performing the step of this activity, you should sign in to a company with the *U100* dataset preloaded. Sign in as a system administrator with the following credentials:

- Username: *gibbs*
- Password: *123*

## 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, 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 due to a change in his job responsibilities.

# Lesson 2.3: Encrypting with Digital Certificates

---

## 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 default encryption method used for Acumatica ERP database with a certificate of your choice.
- Configure signing of PDF files generated for reports in the system.

## Applicable Scenarios

You use digital certificates in the following cases:

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

## Certificates 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 signing PDF files.

For each certificate you provide a name and 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

Acumatica ERP database stores sensitive data, such as credit card numbers and passwords, encrypted. If no encryption certificate is loaded, the 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 uses the system (for example, at night).

## PDF Signature

You can use encryption certificates to sign PDF files 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 a 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). Otherwise, 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 default encryption algorithm used in Acumatica ERP with your encryption certificate.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

### Story

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

### Process Overview

You 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 production.

Then, on the [Certificate Replacement](#) (SM200535) form, you specify a certificate in the **New Certificate** box and click **Replace Certificate**. The system launches 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

Do the following:

1. Launch the Acumatica ERP website with the *U100* dataset preloaded, and sign in as a system administrator by using the `gibbs` username and the `123` password.

2. Open the [File Upload Preferences](#) (SM202550) form and verify that `.pfx` is on the list of allowed extensions.

### 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 the certificate name that will be used in the system.
4. In the **Password** box, type the `Aw34esz` password for the certificate. It will be hidden 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 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

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 Selection area, in the **New Certificate** box, select the certificate whose 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.

### Step 3: To Restore the Default Database Encryption

1. Open the [Certificate Replacement](#) (SM200535) form.
2. In the Selection area, clear the value of the **New Certificate** box.
3. 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.

# Part 3: Monitoring User Activities

---

## Lesson 3.1: Using 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 chapter, 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 **Keep Audit History for x 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 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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

## Story

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

## 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.

## System Preparation

Before you start configuring security auditing, 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 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 of the Summary area, 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:
  - **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 *Login Failed*. The system displays the list of events registered for this operation, which should be similar to the one shown in the following screenshot.

Access History ☆ CUSTOMIZATION TOOLS ▾

↶ < > DELETE HISTORY

Username:

From:  To:

Operation: **Login Failed**

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

**Figure: List of Login Failed events**

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

### 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 chapter, 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) and [Audit](#) (SM205520) forms.
- 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 document created by using the form, and click **Tools > Audit History** to view the audit trail for the selected document.



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](#) (SM205530) 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 doesn't support field-level auditing.

**Journal Transactions**

NOTES ACTIVITIES FILES BUSINESS EVENTS CUSTOMIZATION **TOOLS**

← SAVE & CLOSE ↻ + ✖ ⏮ ⏪ ⏩ ⏭ RELEASE ACTIC

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

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

VIEW SOURCE DOCUMENT RECLASSIFICATION HISTORY

	*Branc	*Ac	Description	Project/Cr	Project Task	Ref. Number	Tran Date	Quan	UC	Debit Amot	Credi Amot	Transaction Description	Not Bill
>	HEA...	20...	Accounts Paya...	X		000001	12/11/2	0.00		0.00	239.00	Logo labels	<input checked="" type="checkbox"/>
	HEA...	81...	Other Expenses	X		000001	12/11/2	0.00		239.00	0.00	Logo labels	<input type="checkbox"/>

**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](#) (SM205520) 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 is left intact.

## Viewing of an Audit Trail

When auditing is turned on for a form, you can select a document and view the changes made to the document directly from the form by clicking **Tools > Audit History** on the form title bar. This opens the Audit History page on a new tab, where you can see the list of changes made to the selected document. You can click the **Changes** arrow to view the detailed data of the modification. For each change, you can see who modified the document 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](#) (SM205530) inquiry form, 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 general information about the creation and the last modification of the selected record in the **Update History** dialog box, which is opened when the user clicks **Tools > Audit History** on the form title bar.

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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

## 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 *Field-Level Audit* feature has been enabled in the system.

## 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](#) (SM205520) 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.

## System Preparation

Before you start configuring auditing of a form, 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: 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. Open the [Audit](#) (SM205510) form.
2. In the **Screen Name** box of 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 of 18 tables 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: Reviewing User Actions on the Invoices and Memos Form

To review the auditing of changes for a record on the [Invoices and Memos](#) (AR301000) form 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**.
5. On the [Invoices and Memos](#) (AR301000) form, click **Add New Record** and create a new invoice with the following settings:

6. On the **Document Details** tab, click **Add Row** and specify the following settings in the added row:
  - **Branch:** *HEADOFFICE*
  - **Ext. Price:** *311*
7. On the form toolbar, click **Remove Hold**, and then click **Release** to release the invoice.
8. While remaining on the *Invoices and Memos* (AR301000) form, click **Actions > Reverse** to create a credit memo.
9. On the form toolbar, click **Remove Hold**, and then click **Release** to release the credit memo.
10. On the *Invoices and Memos* form, select the invoice you created and select **Tools > Audit History** on the form title bar.
11. On the Audit History page, which opens, review the audit history for the invoice (as shown in the following screenshot).

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

3. In the [Audit](#) (SM205510) form, which opens, clear the **Active** check box in the Summary area.
4. On the form toolbar, save the current record and close the screen.
5. On the [Audit](#) (SM205520) inquiry form, verify that the check box in the **Active** column is cleared for the record with *Invoices and Memos* in the **Audited Screen Name** column, as shown in the following screenshot.

[Audit](#) ☆ CUSTOMIZATION TOOLS ▾

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

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

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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

### 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.

<

**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 the 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.

Audit History ☆ TOOLS ▾

↶ MANAGE

Screen ID: PO.30.10.00 - Purchase Orders 🔍

Table Name: Purchase Order 🔍

User: 🔍

Start Date:

End Date:

**Records**

🔄 |🔍| ☒

All Records ▾ 🔍

Type	Order Nbr.
> Normal	000026

🔍

🔄 |🔍| ☒

All Records ▾ 🔍

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

**Figure: Audit history for a purchase order**

You have reviewed the audit history for all purchase orders.

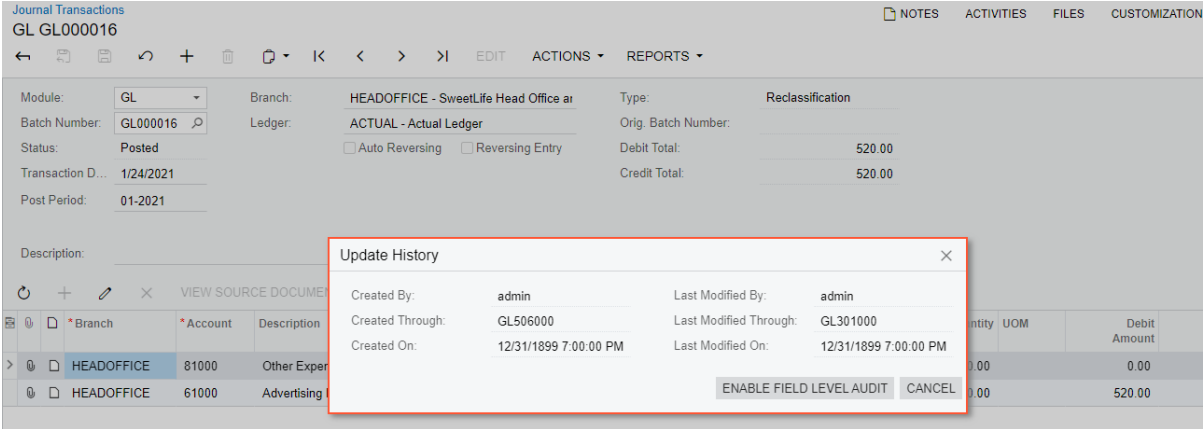
**Step 3: Reviewing General Information About a Record**

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.



**Figure: General information about a document**

You have reviewed general information about a document.

## Part 4: Using Multifactor Authentication Methods

---

### 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).

#### 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 a 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.

Some 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

---

### 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 chapter, 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 Scenarios

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 of 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 (shown in the following screenshot), 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, 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**. The system generates a PDF document with the list of access codes. You enter an access code to the **Enter access code** box.

The screenshot shows a 'Confirm' dialog box with a close button (X) in the top right corner. It contains three main sections:

- EMAIL CONFIRMATION:** A text box with the message: "During first login with two-factor authentication you will receive an access code for mobile application by email. To be sure that you have properly specified your email address, please enter the test access code which has been sent to your email gibbs@sweetlife.com". Below this is a text input field labeled "\* Enter access code:" containing the code "2RMHRUQ6RZ".
- BACKUP OPTION:** A text box with the message: "You can generate a list of access codes so that if other methods of the second step during two-factor authentication are unavailable you can use an access code from the list. Print or save the list of access codes not to lose access to your account." Below this is a button labeled "GENERATE LIST OF ACCESS CODES".
- CONFIGURATION OF USERS FOR INTEGRATED APPLICATIONS:** A text box with the message: "If there are integrated applications that log in with some user's credentials you need to turn off two-factor authentication for this user on the Users form." Below this are two buttons: "OK" and "CANCEL".

**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.



gibbs

**Two-Factor Authentication**

To verify your identity by approving push requests on your mobile device:

1. Install Acumatica mobile app on your device.
2. Sign in to the account of this Acumatica instance using access code sent to your email: gibbs@sweetlife.com.  
You will be able to re-send the code after 4:23
3. Approve push request on your mobile device:

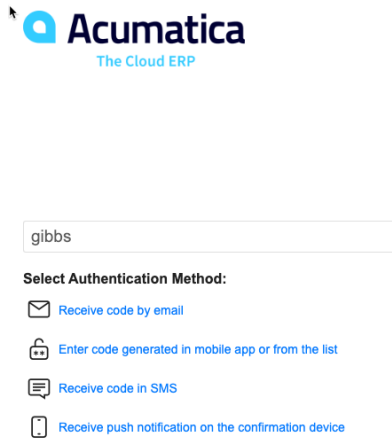
[Send request to device](#)

[Use Another Authentication Method](#)





**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.)



The screenshot shows the Acumatica login page. At the top left is the Acumatica logo with the tagline 'The Cloud ERP'. Below the logo is a text input field containing the username 'gibbs'. Underneath the input field is the heading 'Select Authentication Method:' followed by four options, each with a small icon and a blue link text:

-  [Receive code by email](#)
-  [Enter code generated in mobile app or from the list](#)
-  [Receive code in SMS](#)
-  [Receive push notification on the confirmation device](#)

**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.

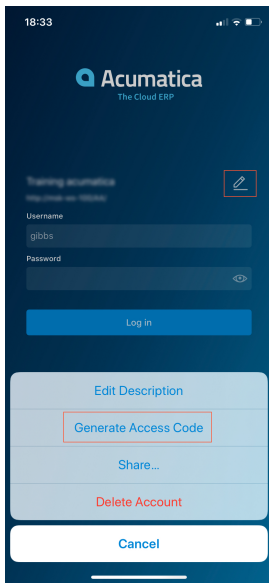
## Authentication by Access Code

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.

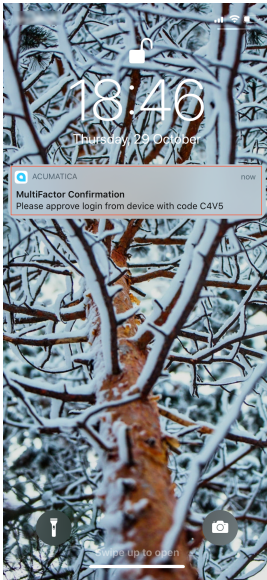
If a user has installed the Acumatica mobile app and has passed authorization there, the app may be used for generation of an access code. The user can click the **Generate Access Code** command in the account editing menu of the mobile app, as shown in the following screenshot.



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

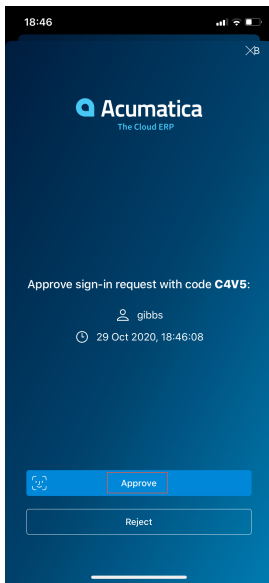
## Authentication by Push Notifications

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).



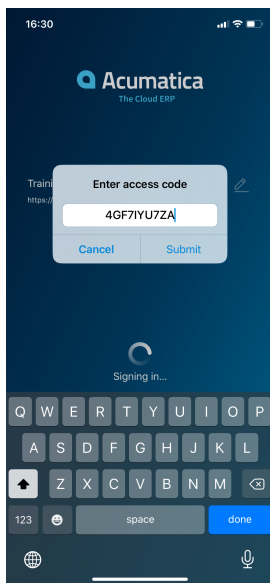
**Figure: The Approve button in the Acumatica mobile app**

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 user signs in to the Acumatica mobile app, the system will request the security access code, which will be sent to the user's email address that is specified on the [Users](#) (SM201010) form. (The following screenshot shows the prompt to enter the access code.) Alternatively, the user may 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.

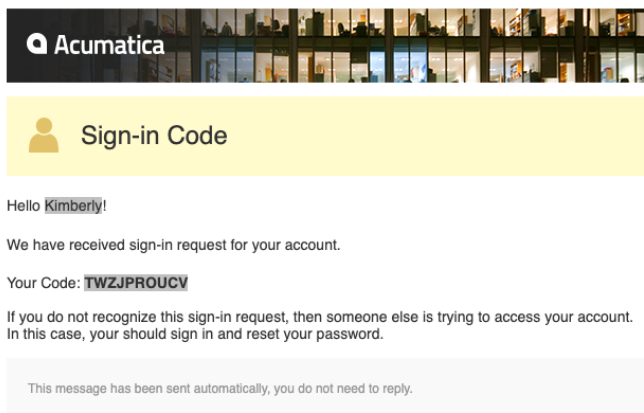




**Figure: Access code entered on the first sign-in to the mobile app**

## 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, 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.



The following activity is based on the *U100* dataset. If you are using another dataset, or if any system settings have been changed in *U100*, these changes can affect the workflow of the activity and the results of the processing. To avoid any issues, restore the *U100* dataset to its initial state.

### 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

You will use the [Users](#) (SM201010) form to 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 using the [Security Preferences](#) (SM201060) form.

You will sign out and try to sign in with an access code. Then, you will use the [All Emails](#) (CO409070) inquiry 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 the *Required* option.
5. On the form toolbar, click **Save**.

6. Click **Generate Access Codes** on the form toolbar. The system opens the Codes (SM651011) report in a pop-up window.
7. On the report toolbar, click **Export > PDF**, and save the list of the codes 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 Kimberly 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

## Appendix 1: Preparing an Instance for Implementation

### 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
<a href="#">Enable/Disable Features</a> (CS100000)	The default set of features has been enabled for the instance.
<a href="#">Activate License</a> (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
<a href="#">Security Preferences</a> (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
<a href="#">Users</a> (SM201010)	<p>User accounts for people involved in the implementation have been created, by using the <a href="#">Users</a> (SM201010) form.</p> <p>For each user, at least the following settings have been specified:</p> <ul style="list-style-type: none"> <li>• Username (login)</li> <li>• Initial password to be changed on the first sign-in</li> <li>• Email address</li> <li>• Set of predefined roles that allow access to all system resources</li> </ul>

## Preparing an Instance: Acumatica ERP Features

Acumatica ERP provides a scalable core system functionality and includes a range of add-on features, which can be enabled and disabled on the [Enable/Disable Features](#) (CS100000) form.

### Finance Group of Features


Feature	Related Feature	Overview
<b>Standard Financials</b>		This group of features is available in all editions of Acumatica ERP. You can enable any of the features in this group—they are included in any license.
	<b>Multi-Branch Support</b>	<p>Provides support for multiple branches. Branches can be configured for points of sale (locations) as well as for separate legal entities within your organization, to ensure better visibility into various layers of financial operations. For details, see <a href="#">Multiple Branch Support</a> and <a href="#">Basic Models for Multi-branch Organization</a>.</p> <p>If this feature is disabled, users can create only one company without branches.</p>
	<b>Business Account Locations</b>	Supports multiple locations for vendor and customer accounts.
	<b>Multicurrency Accounting</b>	Adds forms related to the currency management functionality and support of the following: multiple currencies across the modules; automatic calculation of the realized gains and losses and rounding amounts on foreign currency transactions; revaluation of foreign currency accounts; and translation of the base currency accounts into any foreign currency for reporting. For more information, see <a href="#">Currency Management</a> .

Feature	Related Feature	Overview
	<b>Centralized Period Management</b>	<p>Makes it possible to manage financial periods on the tenant level only; the status of each financial period is the same in all companies. This feature is enabled by default.</p> <p>You can enable the <i>Centralized Period Management</i> feature if the <i>Multiple Calendar Support</i> feature is disabled.</p> <p>You can disable the <i>Centralized Period Management</i> feature if the <i>Multi-Branch Support</i> feature is enabled. Disabling the <i>Centralized Period Management</i> feature makes it possible to open, close, and lock a particular financial period separately for each company within the tenant.</p> <p>For more information, see <a href="#">Generating Financial Calendars</a>.</p>
	<b>Volume Pricing</b>	Gives you the ability to define price tiers for item quantities.
	<b>Expense Reclassification</b>	<p>Supports the two-stage release of AP documents: <i>pre-release</i>, when a data entry clerk enters a bill or a quick check; and <i>release</i>, when an authorized accountant reviews a pre-released document, specifies the correct expense accounts (and subaccounts), and releases the document. For details, see <a href="#">Configuring Reclassification of Expenses</a>.</p>
	<b>Tax Entry From GL Module</b>	Gives users the ability to specify taxes for documents entered on the <a href="#">Journal Transactions</a> (GL301000) form.
	<b>VAT Reporting</b>	<p>Provides accounting and reporting for any value-added tax (VAT) in the system. The feature makes the VAT tax type option available on the <a href="#">Taxes</a> (TX205000) form, and adds UI elements that can be used for automatic calculation of tax amounts and for VAT reporting to the <a href="#">Invoices and Memos</a> (AR301000) and <a href="#">Bills and Adjustments</a> (AP301000) forms. For details, see <a href="#">Value-Added Tax and Its Variations</a>.</p>
	<b>1099 Reporting</b>	<p>Provides support for configuring 1099 vendors and filing the 1099 MISC form and adds the corresponding forms, reports, and UI elements. For details, see <a href="#">Filing the 1099-MISC Form</a>.</p>
	<b>Net/Gross Entry Mode</b>	<p>Gives users the ability to specify the tax calculation mode, which the system will use for computing a tax amount in a document, when you enter a document in the system manually. Depending on the specified mode, you can enter either tax-inclusive amounts at the line level or the document level, or tax-exclusive amounts at the line level or the document level. You will also be able to activate the tax amount validation functionality in a document that you enter.</p> <p>For details, see <a href="#">Managing Taxable Documents</a>.</p>
	<b>Invoice Rounding</b>	Provides automatic rounding of bill and invoice amounts. For details, see <a href="#">Rounding of Document Amounts</a> .
	<b>Expense Management</b>	<p>Allows company employees to file their claims for reimbursement of expenses.</p> <p>For details, see <a href="#">Processing Expense Claims</a>.</p>

Feature	Related Feature	Overview
<b>Advanced Financials</b>		This group of features is not available in the standard edition of Acumatica ERP. You can enable any of the features in this group if the group of features is available in your license.
	<b>Subaccounts</b>	Gives you the ability to use subaccounts in addition to accounts. Subaccounts, which are configured on the <a href="#">Subaccounts</a> (GL203000) form, are used to detail account balances, for more granular financial analysis. For details, see <a href="#">Subaccounts: General Information</a> .
	<b>General Ledger Allocation Templates</b>	Makes possible the creation and maintenance of allocation templates (which define how the allocations are to be performed) and the automatic application of allocations according to your definitions.
	<b>Inter-Branch Transactions</b>	<p>Makes possible the automatic generation of balancing entries for transactions between different companies of one tenant, branches of different companies of one tenant, and branches that belong to one company and require balancing. For details, see <a href="#">Configuring Interbranch Account Mapping</a>.</p> <p>Also, enabling this feature gives you the ability to process sales transactions between legal entities implemented as companies or branches in the same tenant. For details, see <a href="#">Intercompany Sales Setup: General Information</a>.</p> <p>If this feature is disabled, users can enter transactions only between branches that belong to one company and do not require balancing.</p>
	<b>Customer and Vendor Visibility Restriction</b>	<p>A check box that you use to select the <i>Customer and Vendor Visibility Restriction</i> feature for enabling. Enabling this feature gives you the ability to limit access to particular customer and vendor records for employees of a particular company, company group, or branch.</p> <p>For details, see <a href="#">Customer Visibility: General Information</a>, <a href="#">Vendor Visibility: General Information</a>, and <a href="#">Company Groups: General Information</a>.</p>
	<b>Multiple Calendar Support</b>	<p>Provides the ability to configure companies with different fiscal calendars within one tenant. For details, see <a href="#">Multiple Calendar Support</a>.</p> <p>The <i>Multiple Calendar Support</i> feature can be enabled if the <i>Centralized Period Management</i> feature (under <b>Standard Financials</b>) is disabled.</p>
	<b>General Ledger Consolidation</b>	Provides consolidation of data from specific branches of subsidiaries (or consolidation units) into a specific branch of the parent company. You can configure which data should be consolidated and how exactly the data should be consolidated. After that, you can consolidate the data as often as you need to within each financial period.
	<b>Translation of Financial Statements</b>	Gives you the ability to translate amounts from the base currency to another currency at the account balance level. Translation can be used for reporting purposes in any foreign currency. For details, see <a href="#">Translation of Financial Statements: General Information</a> .

Feature	Related Feature	Overview
	<b>Customer Discounts</b>	<p>Gives you the ability to maintain customer discounts in your system: import them or enter them manually, and update them. The system automatically applies the customer discounts to sales orders (or invoices if the <i>Inventory and Order Management</i> group of features is not enabled) when a user saves the document.</p> <p>When the feature is disabled, you can enter the discount percent or amount on a line and document level on data entry forms, but the discount amounts are not posted separately to a discount account.</p> <p>For more information, see <a href="#">Customer Discounts: General Information</a>.</p>
	<b>Vendor Discounts</b>	<p>Gives you the ability to maintain vendor discounts in your system: import them or enter them manually, and update them. The system automatically applies the vendor discounts to purchase orders (or bills if the <i>Inventory and Order Management</i> group of features is not enabled) when a user saves the document.</p> <p>When the feature is disabled, you can enter the discount percent or amount on a line and document level on data entry forms, but the discount amounts are not posted separately to a discount account.</p> <p>For more information, see <a href="#">Configuring Vendor Discounts</a>.</p>
	<b>Commissions</b>	<p>Makes it possible to configure commission calculations that support your company's policies.</p>
	<b>Overdue Charges</b>	<p>Gives you the ability to configure additional charges to be applied to the outstanding balances of customers who are paying too late or not paying in full.</p>
	<b>Dunning Letter Management</b>	<p>Provides you with the ability to generate dunning letters to notify customers about their overdue documents. You can select how you want to manage a level of dunning letter: by customer or by overdue document. For details, see <a href="#">Managing Dunning Letters</a>.</p>
	<b>Deferred Revenue Management</b>	<p>Adds forms and UI elements related to the deferred revenue functionality and integrates it with accounts payable and accounts receivable, so that users can assign various documents to deferral schedules for recognizing portions of the deferred amounts. For more information, see <a href="#">Deferred Revenue</a>.</p>
	<b>Revenue Recognition by IFRS 15/ASC 606</b>	<p>Allows recognition of the revenue of each component in AR documents according to the <i>IFRS 15</i> or <i>ASC 606</i> standard (based on the fair value price).</p> <p>For more information, see <a href="#">Recognition of Revenue from Customer Contracts</a>.</p>
	<b>Parent-Child Customer Relationship</b>	<p>Makes it possible to configure parent-child relationships between business accounts of the <i>Customer</i> and <i>Customer &amp; Vendor</i> types. A parent-child relationship includes the ability for the parent account to pay invoices of the child account, to generate consolidated statements and reports, and to view a consolidated balance for a parent account that includes the balances of its child accounts. The relationship can be removed at any time. For details, see <a href="#">Managing Parent-Child Relationships</a>.</p>



Feature	Related Feature	Overview
	<b>Retainage Support</b>	<p>Makes it possible to create documents of the <i>Invoice</i> and <i>Bills</i> type with retained amounts that will be paid later. Multiple documents are created in the system to process a retainage: the original document (which has retainage withheld) and the retainage document or documents (which reflect the retainage amount to be paid).</p> <p>If the <i>Standard Inventory</i> feature is enabled in addition to this feature, you can also create purchase orders with retained amounts. For each purchase order, you then create an AP bill in which the system specifies the retainage settings based on the purchase order settings.</p> <p>If the <i>Project Accounting</i> feature is enabled in your system in addition to this feature, you can also create pro forma invoices with retained amounts. For each pro forma invoice, you then create an AR invoice in which the system specifies the retainage settings based on the pro forma invoice settings.</p>
	<b>Payment Application by Line</b>	<p>Allows individual lines of accounts payable documents to be paid. When you add lines to AP documents, for each line, you specify the inventory ID, project, project task, and cost code (if the <i>Cost Codes</i> feature has been enabled).</p> <p>This feature can be used in the AR subledger only with the Construction Edition.</p> <p>For more information, see <a href="#">Applying Payments to Particular Lines of AP Documents</a>.</p> <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;">  For documents paid by line, the functionality of the <i>Invoice Rounding</i> feature, if it is enabled, is not applied. However, in documents that are not paid by lines, invoice amounts are rounded. </div>
	<b>Contract Management</b>	<p>This feature provides the support of contracts, including case processing and contract billing. It makes available forms related to contract processing and provides integration with the accounts receivable and tracking of time and expenses functionality. For more information, see <a href="#">Managing Contracts</a>.</p>
	<b>Fixed Asset Management</b>	<p>This feature adds the forms related to fixed asset management, which can be used to create and manage fixed assets through their useful life, from acquisition to disposal. The fixed asset functionality integrates with the requisition and purchase order functionality to facilitate converting purchases into fixed assets without users needing to re-enter data. For more information, see <a href="#">Fixed Assets</a>.</p>

## Inventory and Order Management Group of Features

The Inventory and Order Management group of features, once enabled, includes basic functionality related to the following:

- **Inventory:** The basic functionality includes only non-stock items that can be processed in the with sales orders and purchase orders. For more information, see [Inventory Management](#).

- Sales orders: The basic functionality includes predefined order types, flexible order processing workflows (which include sending orders by email or printing them and sending them by postal mail), generation of pick lists, and shipment processing. For more information, see [Order Management](#).
- Purchase orders: The basic functionality includes purchase orders of multiple types, vendor catalogs, default prices that are updated from current documents, landed cost tracking, and barcode support.

The purchase requisitions functionality is made available by a separate feature of the Inventory and Order Management group of features, *Purchase Requisitions*. The other features of the Inventory and Order Management group of features are divided into two groups, *Standard Inventory* and *Advanced Inventory*.

All of the Inventory and Order Management features are briefly described below.

Feature	Related Feature	Overview
<b>Inventory and Order Management</b>		This group of features includes the features associated with the standard functionality of inventory and order management. You can enable any of the features in this group and disable the features that will not be used in your implementation if this group is included in your license.
	<b>Inventory</b>	<p>Gives you the ability to maintain stock items using forms related to the inventory functionality and use the inventory and order management functionality for creating and processing documents that include stock items.</p> <p>If this feature is not included in your license, you can use the forms that provide the inventory and order management functionality for creating and processing documents that include only non-stock items and services.</p> <p>The <i>Inventory</i> and <i>Purchase Receipts Without Inventory</i> features are mutually exclusive. That is, you cannot enable one of these features if the other is enabled; if you attempt to select the check box on the <a href="#">Enable/Disable Features</a> form corresponding to one of these features and the check box corresponding to the other feature is selected, the system displays an error indicating that you must disable the other feature first.</p>
	<b>Multiple Units of Measure</b>	For each stock item, gives you the ability to define multiple units of measure (UOMs) and the rules for conversion between them. With this feature not enabled, for each stock item, you can define only the base unit of measure, which is used for purchasing the item, selling it, and calculating its available quantity. For more information, see <a href="#">Units of Measure: General Information</a> .
	<b>Lot and Serial Tracking</b>	Gives you the ability to track stock items by lot or serial numbers and by expiration dates. Acumatica ERP provides flexible numbering schemes for lot and serial numbers and the ability to track different products differently. For more information, see <a href="#">Items with Lot and Serial Numbers: General Information</a> .

Feature	Related Feature	Overview
	<b>Blanket and Standard Purchase Orders</b>	Makes possible the processing of blanket purchase orders—orders that can be fulfilled through multiple normal orders. This feature also makes possible the processing of standard purchase orders—orders with products that are purchased regularly in the same quantities and that can be processed repeatedly. For more information, see <a href="#">Blanket and Standard Purchase Orders</a> .
	<b>Purchase Receipts Without Inventory</b>	<p>Provides you with the ability to process non-stock items by using purchase receipts and purchase returns when the <i>Inventory</i> feature is disabled on the <a href="#">Enable/Disable Features</a> (CS100000) form.</p> <p>The <i>Purchase Receipts Without Inventory</i> and <i>Inventory</i> features are mutually exclusive. That is, you cannot enable one of these features if the other is enabled; if you attempt to select the check box on the <a href="#">Enable/Disable Features</a> form corresponding to one of these features and the check box corresponding to the other feature is selected, the system displays an error indicating that you must disable the other feature first.</p>
	<b>Drop Shipments</b>	Gives you the ability to create and track orders for goods that should be delivered directly to a customer location. For more information, see <a href="#">Sales with Drop Shipment: General Information</a> .
	<b>Multiple Warehouses</b>	Adds the ability to configure multiple warehouses. For more information, see <a href="#">Warehouses: General Information</a> .
	<b>Multiple Warehouse Locations</b>	Supports multiple locations for each warehouse. Some of these locations can be reserved for specific inventory transactions, such as receipts, issues, and returns. For more information, see <a href="#">Warehouse Locations and Single-Step Transfers: General Information</a> .
	<b>Inventory Replenishment</b>	Automates the generation of purchase and transfer orders for the replenishment of stock items for your warehouse or warehouses. This feature can be enabled only if the <i>Multiple Warehouses</i> feature is enabled. For more information, see <a href="#">Automated Replenishment</a> .
	<b>Matrix Items</b>	Makes available the functionality of creating and using matrix items in the system. For details, see <a href="#">Matrix Items: General Information</a> .
	<b>Inventory Subitems</b>	Makes possible the use of subitems in your system. With this feature enabled, under the same inventory ID, there can be a number of products that share all the settings of the inventory item record but have additional properties that differ, such as size, color, and material. For details, see <a href="#">Inventory Subitems</a> .
	<b>Automatic Packaging</b>	Makes it possible for the system to calculate the optimal set of boxes for each sales order or a consolidated shipment. The system selects the boxes (based on the list of carrier boxes), the item packaging options, and the item quantities in the document. If the items will be shipped through an integrated carrier, the system calculates the shipping costs for each carrier, so that you can select the best shipping option. For more information, see <a href="#">Automatic Packaging for Integrated Carriers</a> .
	<b>Kit Assembly</b>	Makes possible the creation of kit specifications and kit assembly and disassembly according to your specifications. For more information on kits, see <a href="#">Inventory Item Kits</a> .

Feature	Related Feature	Overview
	<b>Advanced Physical Count</b>	Supports physical counts by inventory IDs, item classes, user-defined cycles, movement classes, or ABC codes. For information, see <a href="#">Configuration of Physical Inventory</a> .
	<b>Sales Order to Purchase Order Link</b>	Supports sales order fulfillment through purchasing. For details, see <a href="#">Purchases for Sale: General Information</a> .
	<b>Custom Order Types</b>	Provides the ability to create custom types of sales orders. For more information, see <a href="#">Custom Sales Order Types</a> .
	<b>Purchase Requisitions</b>	Makes available forms and UI elements related to the purchase requisition functionality in the system. You can use these forms to create requisition requests and requisitions, perform bidding to find the best prices, and control budget compliance. For more information, see <a href="#">Processing Purchase Requisitions</a> .
	<b>Advanced SO Invoices</b>	Gives you the ability to add stock items directly to SO invoices without creating and processing an associated sales order and shipment. For more information, see <a href="#">Direct Sales: General Information</a> and <a href="#">Direct Returns: General Information</a> .
	<b>Vendor Relations</b>	Gives you the ability to configure and manage vendor relations. For more information, see <a href="#">Managing Vendor Relations</a> .
	<b>Warehouse Management</b>	Gives you the ability to perform warehouse operations by using barcode scanners or mobile devices.
	<b>Fulfillment</b>	Gives you the ability to perform fulfillment operations—such as picking, packing, and shipping items—by using barcode scanners or mobile devices.
	<b>Advanced Picking</b>	Gives you the ability to fulfill sales orders by using advanced picking processes, such as wave picking and batch picking.
	<b>Receiving</b>	Supports receiving operations, such as receiving and putting away items, by using barcode scanners or mobile devices.
	<b>Inventory Operations</b>	Supports inventory operations—such as issuing, receiving, transferring, and counting items—by using barcode scanners or mobile devices.
	<b>Cart Tracking</b>	Makes available the capability to configure carts and track them when performing warehouse operations by using barcode scanners or mobile devices.

## Customer Management Group of Features

This group of features makes available the forms and UI elements related to the customer management functionality: lead and customer tracking, business opportunities, case management, marketing lists, and campaign management.

For more information, see [CRM: General Information](#).

Feature	Overview
<b>Case Management</b>	Gives you the ability to enter, assign, and resolve cases. For details, see <a href="#">Managing Cases</a> .
<b>Lead/Contact Duplicate Validation</b>	Provides functionality you can use to configure and perform the automatic validation of lead and contact records for duplicates. For more information, see <a href="#">Validating Records for Duplicates</a> .
<b>Sales Quotes</b>	Gives you the ability to create opportunity-based sales quotes, send them to customers for review, and create sales orders and invoices based on these quotes. For more information, see <a href="#">Managing Opportunities: Sales Quotes</a> .
<b>Address Lookup Integration</b>	Gives you the ability to use the address enrichment functionality. With this feature enabled, integration with a web map service can be set up, and you can add new addresses, update existing addresses, and fill in the missing address information on the forms that have address information. For more information, see <a href="#">Integration with Web Map Services</a> .

## Projects Group of Features

These features are available as add-on features.

Feature	Related Features	
<b>Projects</b>		This group of features adds the forms and UI elements related to the project accounting functionality, which can be integrated with other functional areas of the system. For more information, see <a href="#">Projects</a> .
	<b>Project Accounting</b>	Adds the forms and UI elements related to the project accounting functionality, which can be integrated with the other functional areas. For more information, see <a href="#">Overview of Projects Accounting</a> .
	<b>Change Orders</b>	Gives you the ability to control changes to the project's budgeted and committed values, and to control the profitability of every change initiated by a customer. For more information, see <a href="#">Single-Tier Change Management: General Information</a> .
	<b>Change Requests</b>	Gives you the ability to set up two-tier change management for change orders. In the first tier, you create change requests, and in the second tier, you group multiple change requests into a single change order. This feature can be enabled only if the <i>Change Orders</i> feature is enabled. For more information, see <a href="#">Change Requests: General Information</a> .

Feature	Related Features	
	<b>Budget Forecast</b>	<p>Gives you the ability to prepare a budget forecast for long-term projects, which allows you to break down the structure of the project budget by financial periods.</p> <p>For more information, see <a href="#">Project Budget Forecasts: General Information</a>.</p>
	<b>Cost Codes</b>	<p>Gives you the functionality of cost codes, which represent an additional classification level for project revenues and costs, as subaccounts do for accounts in the general ledger.</p> <p>This feature can be used only if the <i>Projects</i> and <i>Construction</i> features are enabled.</p>
	<b>Project Quotes</b>	<p>Allows you to create project quotes and convert the winning quote to a project when you reach an agreement with the customer on the terms of this project quote.</p> <p>This feature can be enabled only if the <i>Projects</i> feature is enabled.</p> <p>For more information, see <a href="#">Processing Project Quotes</a>.</p>
	<b>Multicurrency Projects</b>	<p>Allows tracking of projects in the project currency, which can differ from the base currency.</p> <p>This feature can be enabled only if the <i>Multicurrency Accounting</i> feature is enabled.</p> <p>For more information, see <a href="#">Multicurrency Project Accounting</a>.</p>
	<b>Construction</b>	<p>Enhances progress billing of pro forma invoices to support the inclusion of the material stored amount in the amount to be invoiced.</p> <p>This feature also makes available construction-specific functionality, which is distributed as a separate customization package. Once the package has been installed and the feature is included in the license that is applied to an Acumatica ERP instance, the following functionality becomes available in the system: subcontracts, compliance tracking, and support for multiple bids on opportunities.</p> <p>This feature can be enabled only if the <i>Projects</i> feature is enabled.</p> <p>For more information, see the Construction Edition guide.</p>
	<b>Construction Project Management</b>	<p>Provides construction-specific project management functionality, which is distributed as a separate customization package.</p> <p>This feature can be enabled only if the <i>Projects</i> feature is enabled.</p> <p>For more information, see the Construction Edition guide.</p>

## Customer Portal Group of Features

Feature	Related Feature	Overview
<b>Customer Portal</b>		<p>The Acumatica Self-Service Portal provides a solution for you to more efficiently work and communicate with your customers. Self-Service Portal is specifically designed to be the site where your customers can view all the relevant information about their interactions with you as a vendor and perform needed activities.</p> <p>Self-Service Portal is an additional application that can be installed separately. For more information, see <a href="#">Overview of Acumatica Self-Service Portal</a>.</p>
	<b>B2B Ordering</b>	<p>Makes it possible for your customers to view the online catalog and place orders themselves through Self-Service Portal.</p> <p>For more information, see <a href="#">Managing Online Orders</a>.</p>
	<b>Case Management on Portal</b>	<p>Gives your customers the ability to add cases and track case processing through Self-Service Portal.</p> <p>This feature can be enabled only if the <i>Case Management</i> feature is enabled.</p> <p>For more information, see <a href="#">Managing Cases with Self-Service Portal</a>.</p>
	<b>Financials on Portal</b>	<p>Provides a means for your customers to view the documents associated with their company accounts in Acumatica ERP.</p>

## Service Management Group of Features

Feature	Related Feature	Overview
<b>Service Management</b>		<p>This group of features includes the features associated with the service management functionality. You can enable or disable features related to the service management if this group is included in your license.</p>
	<b>Equipment Management</b>	<p>This feature makes available the forms and UI elements related to the equipment management functionality. You can enable this feature if it is included in your license.</p>
	<b>Route Management</b>	<p>This feature makes available the forms and UI elements related to the route management functionality. You can enable this feature if it is included in your license.</p>




## Payroll Functionality

Feature	Overview
<b>Payroll</b>	<p>Adds the forms and UI elements related to the payroll functionality, which can be integrated with the other functional areas.</p>

## Platform Group of Features

Feature	Related Feature	Overview
<b>Monitoring and Automation</b>		The features in this group make possible the monitoring of user activities and the automation of workflows. This group of features is not available in the standard edition of Acumatica ERP.
	<b>Time Reporting on Activity</b>	Extends the functionality of the functionality for tracking time and expenses by making it possible to track the time your organization's employees spend on activities that can be included in time cards. For details, see <a href="#">Time Activities</a> .
	<b>Approval Workflow</b>	Provides the ability to configure and use approval maps for the automatic assignment of various documents to particular employees for approval. If this feature is not enabled, approval maps cannot be used in the system, but the approval for expense claims still can be configured and performed by using a different method. For details, see <a href="#">Approving Documents</a> and <a href="#">Expense Claim Approval</a> .
	<b>Field-Level Audit</b>	Gives your organization the ability to track user activities in the system. This feature, which is configured on the <a href="#">Audit</a> (SM205510) form, provides complete information on who did what and when on the form. For more information, see <a href="#">Field-Level Auditing: General Information</a> .
	<b>Row-Level Security</b>	Adds forms and UI elements, which provides the management and administration of user access (through restriction groups) to particular system records and objects to which users have access based on their roles. For details, see <a href="#">Restriction Groups in Acumatica ERP</a> .
	<b>Scheduled Processing</b>	Makes it possible for you to configure the automatic processing of documents that require significant time and system resources. You can define a schedule for this automatic processing—for instance, at times when there are no employees at work, such as weekends or nights. For more information, see <a href="#">Scheduled Processing</a> .
	<b>Workflow Automation</b>	Provides the ability to customize workflows by means of automation steps, and gives you the ability to back up and store automation definitions that include all the automation steps defined in the application. For more information, see <a href="#">Automation Maintenance</a> .
	<b>DeviceHub</b>	Provides the ability to connect hardware devices, such as printers, scanners and digital scales, by using the DeviceHub application. For instructions on configuring printers by using DeviceHub, see <a href="#">Configuring Hardware Devices in DeviceHub</a> .
	<b>GDPR Compliance Tools</b>	Gives you the ability to protect personal data and restrict its processing by using compliance tools for General Data Protection Regulation (GDPR). For more information about GDPR compliance tools, see <a href="#">Compliance Tools for General Data Protection Regulation</a> .




Feature	Related Feature	Overview
	<b>Secure Business Date</b>	Restricts the ability to change the business date, so that this task cannot be performed by all users in the system. To permit the change of the business date for specific users, you assign the <i>BusinessDateOverride</i> role to these users. For more information about restricting the ability to change the date, see <a href="#">User Roles: Restrictions on Changing the Business Date</a> .
<b>Image Recognition for Expense Receipts</b>		<p>Makes available the recognition of expense receipts in the Acumatica mobile app.</p> <div>  <p>The feature is not available in trial mode and can be enabled only if it is included in the license that is applied to the Acumatica ERP instance.</p> </div>
<b>Image Recognition for Business Cards</b>		<p>Makes available the recognition of business cards in the Acumatica mobile app.</p> <div>  <p>The feature is not available in trial mode and can be enabled only if it is included in the license that is applied to the Acumatica ERP instance.</p> </div>
<b>AP Document Recognition Service</b>		<p>Allows you to configure the system to automatically recognize invoices attached to incoming emails so that users can create AP bills from those recognized documents with a single click.</p> <p>With this feature enabled, the <i>Incoming Documents (AP3011PL)</i> and <i>Incoming Documents (AP301100)</i> forms can be used. Also, the following elements become available in the system:</p> <ul style="list-style-type: none"> <li>• The <b>Submit to Incoming Documents</b> check box on the <b>Incoming Mail Processing</b> tab of the <i>System Email Accounts (SM204002)</i> form</li> <li>• The <b>Create AP Document</b> button in the Acumatica add-in for Outlook, which is available only for emails with PDF attachments</li> </ul> <div>  <p>The feature is not available in trial mode and can be enabled only if it is included in the license that is applied to the Acumatica ERP instance.</p> </div> <p>For more information, see <a href="#">Recognizing AP Documents From PDFs</a>.</p>
<b>Authentication</b>		The features in the <i>Authentication</i> group of features are available for all the editions by default.
	<b>Two-Factor Authentication</b>	Provides the ability to configure 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 <a href="#">Managing Two-Factor Authentication</a> .

Feature	Related Feature	Overview
	<b>Google and Microsoft SSO</b>	Gives you the ability to integrate Acumatica ERP with Google or Microsoft Account by using the OAuth 2.0 standard for providing single sign-on (SSO). This reduces the number of usernames and passwords the users have to remember, thus reducing the risk of identity theft.
	<b>Active Directory and Other External SSO</b>	Gives you the ability to integrate Acumatica ERP with Microsoft Active Directory (AD), Microsoft Active Directory Federation Services (AD FS), or Microsoft Azure Active Directory (Azure AD).
	<b>OpenID Connect</b>	Provides the ability to configure integration with OpenID identity providers. A system administrator can configure integration with multiple OpenID providers for a system tenant or multiple tenants.

### Third Party Integrations Group of Features

The features in the *Third Party Integrations* group of features are available for all editions of Acumatica ERP, although the number of features is different in different editions.

Feature	Related Feature	Overview
<b>Commerce Integration</b>		This group of features activates Acumatica ERP Retail-Commerce Edition, which supports integration with external shopping carts and marketplaces for omni-channel sales and fulfillment.
	<b>BigCommerce Connector</b>	Enables the integration with the BigCommerce automated shopping cart software. For details, see <a href="#">Integration with BigCommerce</a> .
	<b>Shopify Connector</b>	Enables the integration with the Shopify e-commerce platform. For details, see <a href="#">Integration with Shopify</a> .
	<b>Shopify POS</b>	Gives you the ability to import and process point-of-sale (POS) orders from Shopify to Acumatica ERP. This feature can be enabled only if the <i>Shopify Connector</i> feature is enabled.
<b>Shipping Carrier Integration</b>		<p>Makes it possible for you to configure integration with carriers, such as FedEx or UPS. With this integration, you can apply real-time rates to shipments and track their delivery.</p> <div style="border: 1px solid orange; border-radius: 10px; padding: 10px; margin: 10px 0;">  Integration with any of the carriers does not support international shipments. </div> <p>For details, see <a href="#">Integration with Carriers</a>.</p>
<b>Exchange Integration</b>		<p>Gives you the ability to integrate Acumatica ERP with Microsoft Exchange Server. You will be able to configure synchronization, and then synchronize users' contacts, emails, tasks, and events in Acumatica ERP with their Exchange mailboxes.</p> <p>For more information, see <a href="#">Synchronizing Acumatica ERP with Microsoft Exchange Server</a>.</p>

Feature	Related Feature	Overview
<b>External Tax Calculation Integration</b>		<p>Provides integration with the AvaTax service by Avalara, Vertex Tax Calculation, or another tax provider for the automatic calculation of sales and use taxes online.</p> <p>For details, see <a href="#">Integrating Acumatica ERP with External Tax Providers</a>.</p>
<b>Address Validation Integration</b>		<p>Provides validation of customer addresses through integrated specialized services, such as AvaTax by Avalara. The feature can be used with the <i>External Tax Calculation Integration</i> feature or without it. For details, see <a href="#">Integrating Acumatica ERP with Address Validation Providers</a>.</p>
<b>Salesforce Integration</b>		<p>Supports bi-directional real-time synchronization of data between Acumatica ERP and Salesforce, so users can work simultaneously in both systems with changes in one system being reflected in the other. For details, see <a href="#">Synchronization with Salesforce</a>.</p>
<b>HubSpot Integration</b>		<p>Gives users the ability to transfer marketing data into Acumatica ERP from HubSpot and to transfer relevant data back to HubSpot from Acumatica ERP. For details, see <a href="#">Configuring Integration with HubSpot</a>.</p>
<b>Procore Integration</b>		<p>Adds the forms and UI elements related to the Procore Integration solution, which is distributed as a separate customization package. Once the package is installed and the feature is included in the license that is applied to an Acumatica ERP instance, the functionality becomes available in the system.</p>

Feature	Related Feature	Overview
<b>Outlook Integration</b>		<p>Gives you the ability to use the Acumatica add-in for Outlook. With this feature enabled, you can create and view contacts, log an activity from an email, and attach an activity to a contact.</p> <p>Enabling both this feature and the <i>Customer Management</i> feature gives you the ability to do the following:</p> <ul style="list-style-type: none"> <li>• Create and view a lead, and attach the logged activity to the lead</li> <li>• Create and view an opportunity, and attach the logged activity to the opportunity</li> </ul> <p>Enabling both this feature and the <i>Case Management</i> feature gives you the ability to create and view a case and attach the logged activity to the case.</p> <p>Enabling both this feature and the <i>Document Recognition Service</i> feature gives you the ability to do the following:</p> <ul style="list-style-type: none"> <li>• Submit email attachments to the recognition service</li> <li>• View documents processed by the recognition service</li> </ul> <p>Enabling both this feature and the <i>Projects</i> feature gives you the ability to attach the logged activity to a project.</p> <p>Enabling both this feature and the <i>Construction Project Management</i> feature gives you the ability to do the following:</p> <ul style="list-style-type: none"> <li>• Create a project issue and attach the logged activity to the project issue</li> <li>• Create a request for information (RFI) and attach the logged activity to the RFI</li> </ul> <p>For more information, see <a href="#">Acumatica Add-In for Outlook</a>.</p>
<b>WorkWave Route Optimization</b>		<p>Provides integration with WorkWave to give users the ability to automatically optimize appointment schedules in field services. For details, see <a href="#">Schedule Optimization by WorkWave</a>.</p>

## Manufacturing Group of Features

Feature		Overview
<b>Manufacturing</b>		This group of features activates Acumatica ERP Manufacturing Edition, which provides the functionality related to item production.
	<b>Material Requirements Planning</b>	Makes available forms and UI elements related to the functionality of material requirements planning. For details, see <a href="#">Material Requirements Planning: General Information</a> .

Feature		Overview
	<b>Product Configurator</b>	Makes available forms and UI elements related to the functionality of product configurator. For more information, see <a href="#">Product Configurator: General Information</a> .
	<b>Estimating</b>	Makes available forms and UI elements related to the functionality of estimations. For details, see <a href="#">Estimating: General Information</a> .
	<b>Advanced Planning and Scheduling</b>	Makes available forms and UI elements related to advanced planning and scheduling. For more information, see <a href="#">Advanced Planning and Scheduling: General Information</a> .
	<b>Engineering Change Control</b>	Makes available forms and UI elements related to the functionality of engineering change control. For details, see <a href="#">Engineering Change Control: General Information</a> .
	<b>Manufacturing Data Collection</b>	Enables the ability to perform production operations by using barcode scanners or mobile devices. For more information, see <a href="#">Manufacturing Data Collection</a> .

## Advanced Authentication Group of Features

The features in the *Advanced Authentication* group of features are available for all the editions by default.

Feature	Overview
<b>Two-Factor Authentication</b>	Provides the ability to configure 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 <a href="#">Managing Two-Factor Authentication</a> .
<b>Google and Microsoft SSO</b>	Gives you the ability to integrate Acumatica ERP with Google or Microsoft Account by using the OAuth 2.0 standard for providing single sign-on (SSO). This reduces the number of usernames and passwords the users have to remember, thus reducing the risk of identity theft.
<b>Active Directory and Other External SSO</b>	Gives you the ability to integrate Acumatica ERP with Microsoft Active Directory (AD), Microsoft Active Directory Federation Services (AD FS), or Microsoft Azure Active Directory (Azure AD).

## Appendix 2: Securing Access to the System

---

### 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.

## 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>Not Set</i>	When this level is assigned to all roles, allows all roles to have access to all forms in a workspace until the <i>Revoked</i> or <i>Granted</i> level is set to the workspace for at least one role. After that, a role with the <i>Not Set</i> level is denied access to the forms in the workspace.
<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>Not Set</i>	When this level is assigned to all roles, allows all roles to have access to the form until the restriction level is changed to any other level for at least one role. After at least one role has been assigned another level, access to the form is denied for a role with the <i>Not Set</i> level.
<i>Revoked</i>	Denies access to the form and its functionality for the role.
<i>View Only</i>	<p>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).</p> <p>This level forbids users with the role from editing details about any record, creating new records or entities of the type, and deleting records.</p>
<i>Edit</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, and edit details about any record.</p> <p>This level forbids users with the role from creating new records or entities of the type, and from deleting records.</p> <p>The <b>Clipboard</b> button is available on the form toolbar for users with the role.</p>
<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 <b>Clipboard</b> and <b>Insert</b> 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 <b>Clipboard</b>, <b>Insert</b>, and <b>Delete</b> 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>
<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. See the following table for an illustration of this example.

**Table: Calculation of 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>	



The *Not Set* restriction level indicates that all roles have access to a form, including its nested objects, until at least one role is assigned any other restriction level to this form. All roles with the *Not Set* level are then denied access to the form.

## 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. See the following table for an illustration of this example.

**Table: Calculation of 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. See the following table for an illustration of the example.

**Table: Calculation of 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>	
<i>Sales Assistant</i>	<i>Insert</i>	<i>View Only</i>	

## 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 [Support of Multiple Tenants](#)).

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 [Managing Dashboards](#).
- *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 an Inquiry 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 OData Version 4 protocol.
- *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 read-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 read-only access to general ledger transactions.

- *AP Clerk*: A user with this role has access to accounts payable functions, as well as read-only access to accounts payable settings and general ledger transactions.
- *AP Viewer*: A user with this role has read-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 read-only access to general ledger transactions.
- *AR Clerk*: A user with this role has access to accounts receivable functions, as well as read-only access to accounts receivable settings and general ledger transactions.
- *AR Viewer*: A user with this role has read-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 read-only access to cash management settings.
- *CA Viewer*: A user with this role has read-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 read-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 read-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 read-only access to fixed asset settings.
- *FA Viewer*: A user with this role has read-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 read-only access to general ledger settings.
- *GL Viewer*: A user with this role has read-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 read-only access to tax-related functions.

## 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 read-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), read-only access to payroll settings, and read-only access to banking, payables, projects, finance, and configuration settings.
- *PR Manager*: A user with this role has full access to payroll functions, read-only access to payroll settings, and read-only access to banking, payables, projects, finance, and configuration settings.
- *PR Viewer*: A user with this role has read-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 read-only access to payroll inquiries.
- *Internal User*: A user with this role can change personal settings and view Help. Also, these users have read-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 user's access rights of the user 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 File External Storage](#).
- 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 announce the ability of using 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
<a href="#">File Upload Preferences</a> (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.

Form	Criteria to Check
<a href="#">Encryption Certificates</a> (SM200530)	<p>Make sure that the list of needed certificates has been uploaded here and passwords are specified for each one.</p> <p>Only certificates that are added to this form can be used for replacing database encryption algorithm used in Acumatica ERP or signing PDF files.</p>
<a href="#">Security Preferences</a> (SM201060)	<p>Make sure that one of the uploaded certificates is specified in the <b>PDF Signing Certificate</b> box. This certificate will be used for PDF files generated for reports in Acumatica ERP.</p>

### 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 [Scheduled Processing](#).

### 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

---

### 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
<a href="#">Enable/Disable Features</a> (CS100000)	The <i>Field-Level Audit</i> feature has been enabled.
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 <a href="#">User Roles: General Information</a> and <a href="#">User Access: General Information</a> .
Multiple forms that support field-level functionality	Auditing of the forms has been configured and enabled, as demonstrated in the example of <a href="#">Field-Level Auditing: Implementation Activity</a> .

## 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

## 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
<a href="#">Enable/Disable Features</a> (CS100000)	The <i>Two-Factor Authentication</i> feature has been enabled.

### Recommended Configuration for Authentication by Using the Acumatica App

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

Form	Criteria to Check
<a href="#">Activate License</a> (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 <a href="#">Preparing an Instance: To Enable Features and Activate the License</a> .
Web Server IIS	<p>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 <a href="#">Setting Up an HTTPS Service in Web Server (IIS)</a>.</p> <div>  <p>If your site works with the HTTP protocol, add the following key to the <code>web.config</code> file: <code>&lt;add key="identityServer:allowHttp" value="true" /&gt;</code>.</p> </div>
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
<a href="#">System Email Accounts</a> (SM204002)	A system email account has been configured as described in <a href="#">Configuring Email Accounts</a> .
<a href="#">Send and Receive Email</a> (SM507010)	All the necessary actions for sending and receiving emails by using a schedule have been performed. For details, see <a href="#">To Create a Send and Receive Email Schedule</a> .
<a href="#">Users</a> (SM201010)	Make sure that all users have email addresses specified on this form.
<a href="#">Security Preferences</a> (SM201060)	The <b>Allow Email</b> check box is selected under the <b>Two-Factor Authentication Policy</b> 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
<a href="#">SMS Providers</a> (SM203535)	An SMS provider (Twilio or Amazon SMS) has been configured.
<a href="#">User Profile</a> (SM203010)	Make sure that all users have phone numbers specified on this form.
<a href="#">Security Preferences</a> (SM201060)	The <b>Allow SMS</b> check box is selected under the <b>Two-Factor Authentication Policy</b> 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.



**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.