Auditor

With E-Sign

For Dynamics GP October 2023 Release (18.6)
Documentation dated July 9, 2025

rockton SOFTWARE

Copyright

Manual copyright © 2004-2025 Rockton Software, Inc.

Printed in U.S.A.

All rights reserved.

No part of this document may be reproduced, stored or transmitted in any form or by any means without prior written permission of Rockton Software, Inc.

Unless otherwise noted, all names of companies, products and persons contained herein are fictitious and are used solely for documentation of this product.

Trademarks

Rockton Software® is a trademark of Rockton Software, Inc.

Dynamics GP® and associated products are trademarks of Microsoft® Corporation, Inc.

Great Plains® and associated products are trademarks of Microsoft® Corporation, Inc.

Windows® versions are trademarks of Microsoft® Corporation, Inc.

Other company or product names mentioned may be trademarks or registered trademarks of their respective holders.

Limitation of Liability

Information in this document is subject to change without notice. Neither Rockton Software nor anyone involved in the creation, production or delivery of this documentation shall be liable for any indirect, incidental or consequential damages, including but not limited to any loss of anticipated profit resulting from the use of this documentation.

License Agreement

Use of this product is covered by a license agreement provided by Rockton Software, Inc.

SOFTWARE LICENSE AGREEMENT

Carefully read all the terms and conditions of this Agreement prior to installing software. Do not activate this software until you have read this entire Agreement. Installing this software indicates your acceptance of these terms and conditions.

If you do not agree to these terms and conditions, then return the software and other components of the software package of this product to the place of purchase and your money will be refunded. If you downloaded this software in its demonstration form and you do not agree to the terms of the license, you may retain the software only in its demonstration form solely for the purpose of passing on the demonstration software to another prospective buyer. No refunds will be given for products downloaded off of the Internet that have been registered and activated.

1. LICENSE: You are granted a personal, nontransferable, and nonexclusive, license to use the enclosed software, under the terms stated in this Agreement. Title, copyright and ownership of the software and any and all related documentation remains with Rockton Software, Inc. (Rockton Software). This software and related programs may be used only on a single site licensed for use of Microsoft Dynamics GP, for the number of concurrent users as provided for in the original Microsoft Dynamics GP registration and purchase. Registration keys can be obtained directly from Rockton Software, if applicable. You may not distribute copies of the registered and activated software or any of the associated documentation to others. The demonstration version of the software may be distributed freely. You may not modify, reverse engineer, de-compile, disassemble or translate the software or related documentation without the prior written consent of Rockton Software.
2. BACKUP: You may make backup copies of this software solely for your own use. You must reproduce and include the copyright notice on the backup copies. If all or any portion of this software is included in other software packages, then the copyright notice must appear on these other materials.
3. TRANSFER: You may not transfer this software to any other party. There are no provisions whatsoever for any other transfer, operation, or use of the software by any other party whatsoever except for the original buyer of the product, which has been registered with the Rockton Software at the time of original purchase and software activation.
4. LIMITED WARRANTY: Rockton Software warrants for a period of thirty days (30 days) from the date of receipt that the software covered by this agreement will perform substantially in accordance with the accompanying written documentation. You assume the entire risk as to the results and performance of the software. This warranty gives you specific legal rights and you may also have other rights that vary from state to state. Rockton Software makes no claim in regard to the merchantability or suitability for any specific purpose of this or any other software product.
5. ACKNOWLEDGMENT: By activating, and using this product you acknowledge that you have read this agreement, understand it, and agree to be bound by its terms and conditions. You also agree that this agreement is the complete and exclusive statement of agreement between the parties and supersedes all proposals or prior agreements, verbal or written, and any other communications between the parties relating to the subject matter of this agreement.
6. REMEDIES: Rockton Software's entire liability and your exclusive remedy shall be at the option of Rockton Software, either (a) return of price paid or (b) repair or replacement of the software that does not meet the limited warranty and is returned to Rockton Software. If you have need of service or help regarding this software, you should contact the dealer through which the software was originally purchased. There is no obligation to render assistance to you if you are not the owner under which the software is registered, or if the registered user has not purchased a recognized support plan from the vendor of this product. The laws of the State of Colorado will govern this Agreement.

Table of Contents

General Information 6
- Introduction 7
- What's in This Manual 8
- Customer Technical Support 9
- System Requirements 10
- Backup and Restore 11
- Customization 11

Installation 12
- Installation 13
- Navigation 16
- Auditor Security Settings 17
- Auditor Administrators 17
- Newer Rockton Software Builds are Available window 18
- Removing Auditor with E-Sign 19

Setup 20
- Auditor Setup window 21
- Auditor Registration window 23
- Rockton Software Registration Issues window 25

Enter Contact Information window 27
- Auditor System Settings window 28
  - Auditor Options window 29
  - Auditor Advanced Options window 31
  - Security Auditor Options window 34
- Please Wait dialog 35
- Reason Codes window 36

Creating Audits 37
- Overview of Auditor and Auditing 38
  - Performance Issues with Auditing 38
  - Audit Types 39
- Group Maintenance window 40
- Auditor Form Maintenance window 44
- Field Options window 46
  - Conditional Auditing 47
- Auditor Table Maintenance window 50
- Auditor SQL Table Maintenance window 52
- Audit sa User window 55
- Auditor Note Maintenance window 58
- Security Audit Note Maintenance window 60
- Auditor Message Center window 61

Inquiry 63
- Audit Reporting using Smartlist 64
- Journal Voucher Roadmap window 65
- Transaction Lifecycle window 66
- Audit Startup Issues Inquiry 68
- View Related Audits 69
  - View Related Audits window 69
  - Related Audit Rules Setup window 70
  - Rule Setup window 71
  - Window Field Relationship Setup window 72
  - Field List Setup window 73
  - Related Audit Rules List window 74

Table of Contents (cont.)

Segregation of Duties 75
Segregation of Duties Group Maintenance window 76
E-Sign 78
Overview 79
E-Sign Signature Definition Maintenance window 82
E-Sign Signature Assignment window 84
E-Sign Signature Assignment Wizard window 85
E-Sign Approval Needed window 92
E-Sign Signature Needed window 94
E-Sign Pending Approval Requests window 95
E-Sign Request Status window 96
E-Sign Queued Approval Requests window 98
E-Sign Approvals window 99
Maintenance 100
Auditor Table Archive/Purge window 101
Query Builder 104
Auditor Reconcile window 105
Auditor Rebuild window 106
Auditor Import / Export window 106
Rockton Support and Troubleshooting 109
About Auditor window 110
Rockton Software Support window 111
Rockton Software Preferences window 112
Enable or Disable Script Logging window 113
Appendix A 113
Audit Group Export File Format 114
Appendix B 115
Typical Archive XML Format 115
Audit Log Archive XML Format 115
Approval Log Archive XML Format 115
Appendix C 116
Example: Setting Up Related Audits 116

General Information

Introduction

Rockton Software is pleased to bring Auditor with E-Sign to the Microsoft Dynamics GP community.

Auditor is a system management tool that will track data changes in your Dynamics GP accounting system. Auditor answers Who changed What, When, Where, and optionally, Why. Auditor can be configured to track field-level specific changes, when new records are added, and when information is deleted from your system.

E-Sign gives you the ability to require approval for changes made to sensitive fields. The User making the change and the Approver "sign" that change by entering their Dynamics GP password. Optionally, changes can be set to require a User's signature without requiring approval.

Auditor with E-Sign also works with all 3rd party installed products which integrate with Dynamics GP, as long as the products are Dexterity based.

What's in This Manual

This manual contains the basic instructions needed for the installation and use of Rockton Software's Auditor with E-Sign. You will find instructions for:

- Installation
- Navigation
- Setting up Auditor

If you do not find the information you need in the following documentation, please contact Rockton Software (see the following page).

Symbols and Conventions

To help you use this documentation more effectively, we have included the following symbols to highlight important information:

This symbol points out suggestions and important notes that assist you in installing and using Auditor.

The warning symbol alerts you to situations in which you should proceed with caution. Notes highlighted with a warning symbol relate to information that affects your entire system—please read carefully!

- Keyboard keys, specific buttons, file names and menu paths are shown in bold print, such as the **Move Right** button, the **OK** key or the **setup.exe** program.

- Window titles and captions are shown in quotes, such as the "Maintenance" window.

Customer Technical Support

Technical support from Rockton Software is simple. With an active maintenance agreement, support is unlimited and available to Resellers and Customers alike. We can communicate via telephone, fax, email, web conference, or other means if possible. Beyond FAQs and product manuals available on our website, we prefer for all customers to utilize their Reseller for support, as it is usually most efficient and the customer's Reseller is more familiar with all third party products on site and the specifics of the customer's needs. However, we will also provide direct support as requested. Without an active maintenance agreement, no technical support is offered.

Please see the Support section for windows that may be useful when you are communicating with Rockton Support.

As always, user input into improving this product, constructive feedback or technical ideas are always appreciated and highly encouraged. At Rockton, we want to hear your input. So drop us a line whenever you feel like it.

You can reach us by contacting technical support from Rockton Software by phone at (877) 476-2586 or e-mail support@rocktonsoftware.com. You can also visit www.rocktonsoftware.com for more information on Rockton products, including a Frequently Asked Questions section.

Enjoy!

System Requirements

The system requirements for installing and using Auditor follow those of Microsoft Dynamics GP. The following table lists the specific hardware and software requirements that pertain to Auditor:

Server Operating System	One of the following: X64 • Microsoft Windows Server 2019 Essentials, Standard, or Datacenter Edition • Microsoft Windows Server 2016 Essentials, Standard, or Datacenter Edition • Microsoft Windows Server 2012 Essentials, Standard, or Datacenter Edition • Microsoft Windows Server 2012 R2 Essentials, Standard, or Datacenter Edition
Client Operating System	One of the following: • Microsoft Windows 10 Professional or Enterprise Editions • Microsoft Windows 8 or 8.1 Professional, Ultimate, or Enterprise Editions • Microsoft Windows 7 Professional, Ultimate, or Enterprise Editions
Available hard disk space	5 MB in the Dynamics GP install folder; 5 MB in the DYNAMICS database
Minimum available RAM	2 GB (more recommended)
Microsoft SQL Server	One of the following: • SQL Server 2019 Enterprise, Standard or Express Editions • SQL Server 2016 Enterprise, Standard or Express Editions • SQL Server 2014 Enterprise, Standard or Express Editions
Microsoft Dynamics GP	One of the following: • Version 2018.2
Adobe Acrobat Reader	Adobe XI, X, 9.0, 8.0, 7.0, or 6.0

Backup and Restore

All Auditor data is stored in the DYNAMICS database. Therefore, performing the process normally used to backup this database should also backup all Auditor data. Similarly, restoring this database will restore Auditor data as well.

In addition to the Setup data, there may be some SQL Triggers on other databases. These would only be present if you have chosen to define SQL Table Audits on tables in databases other than the DYNAMICS database. If you have chosen to do this, then you should backup those databases as well.

Customization

Auditor with E-Sign has been built using Microsoft Dexterity. Therefore, you can use the tools typically available to a Dexterity developer (Modifier, Report Writer, etc.) to customize and extend Auditor. Refer to the Microsoft documentation on these tools for more information.

Installation

Installation

Please read these instructions in their entirety before installing this software.

Workstation Installation Instructions

1. Extract **all of the files and folders** in the zip file you downloaded to a folder where you can access it from all workstations that you are going to install.
2. From each computer on which you wish to install Auditor, right-click the Auditor setup file (**AuditorSetup.exe)** and choose *Run as administrator*.

   It is recommended that you are not running any other Windows programs when installing this program
3. Select the folder where Dynamics GP is installed.

   Important! *Install Auditor to the same directory where Dynamics GP is installed. If the default directory on the Auditor Installation Wizard is not the same as the Dynamics GP installation directory, modify the default directory.* ***If you enter this incorrectly, Auditor will not function!***
4. Click the Install button. This will copy **Audit.cnk** and any other files as appropriate. It will also install any other components that are necessary to run Auditor. On some installations, you may have to reboot your system.
5. Verify that the Status shows "Installed Successfully." for each item listed. Then click the Exit button on the setup window.
6. Include the new chunk file code into Dynamics GP by launching Dynamics GP. Be sure to right-click the Dynamics GP icon, choose More, then choose *Run as administrator*.

   The following message may appear: "New code must be included in the DYNAMICS.SET dictionary. Do you wish to include new code now?" Click **Yes**.

   This process will modify your DYNAMICS.SET file to include information relating to Auditor, and the **Audit.cnk** file will create an **AUDIT.DIC** file.
7. You will be prompted to exit GP. Log out of GP and log back in.

You should now exit Dynamics GP to complete the installation process for each workstation. If this is the first workstation in your network on which you are installing Auditor, continue with the following section.

First Workstation Instructions

If this is the first workstation on which you are installing, complete the following steps.

You will need to complete these steps only once for your system. You do not need to perform these steps in each company.

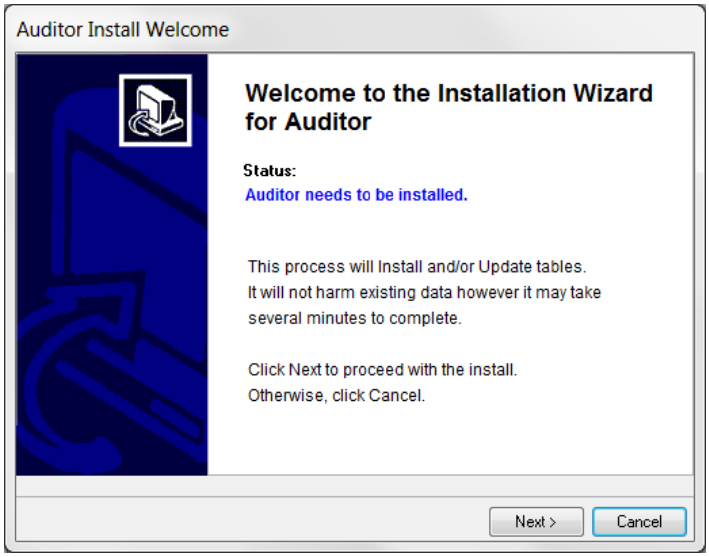
1. First, complete steps 1 thru 6 from the previous section.
2. Log in as any User that has sufficient SQL Server rights to be able to create Tables and Triggers**.** This user must either be in the 'sysadmin' fixed server role or the 'db_owner' role for the DYNAMICS database and any database for which there are SQL Table audits defined. In addition, this User must be either in the AUDITOR ADMIN or POWERUSER Security Role.

   If this is a new installation of Auditor (not an upgrade from a previous build or version), you will need to log in as a User that is in the POWERUSER Security Role. This is because the AUDITOR ADMIN role has not yet been created.

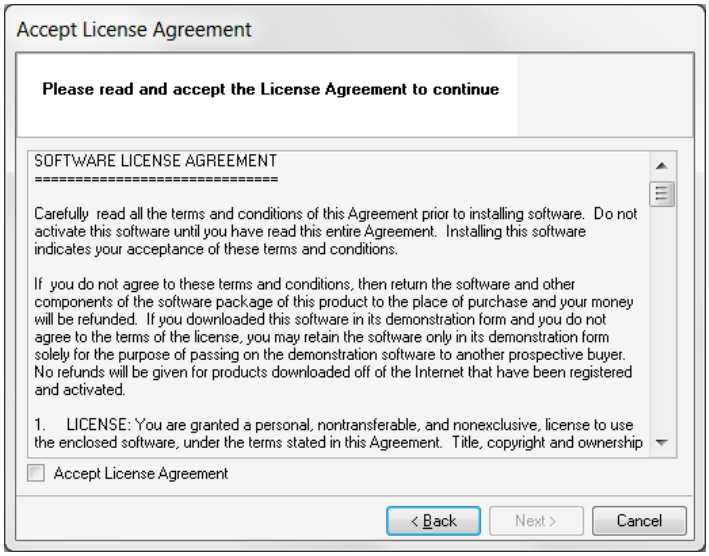
3. Log into any company. Since Auditor maintains data at the system level, it is only necessary to install the software in one company. If you have not received a product registration file, we recommend that you log into the Dynamics GP lesson company.

If you are evaluating the software and have not yet received a product registration file, this product will only work in the Dynamics GP lesson company. To register, contact Rockton Software or your authorized reseller.

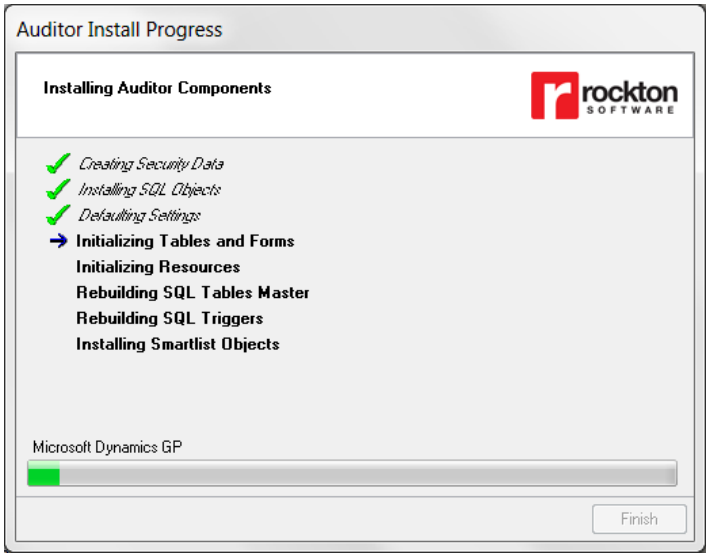
4. Next, the Auditor Install Welcome window will open. Note the status message. This indicates whether you will be installing from scratch or upgrading from an earlier build.



5. Click the Next button to review the License Agreement.



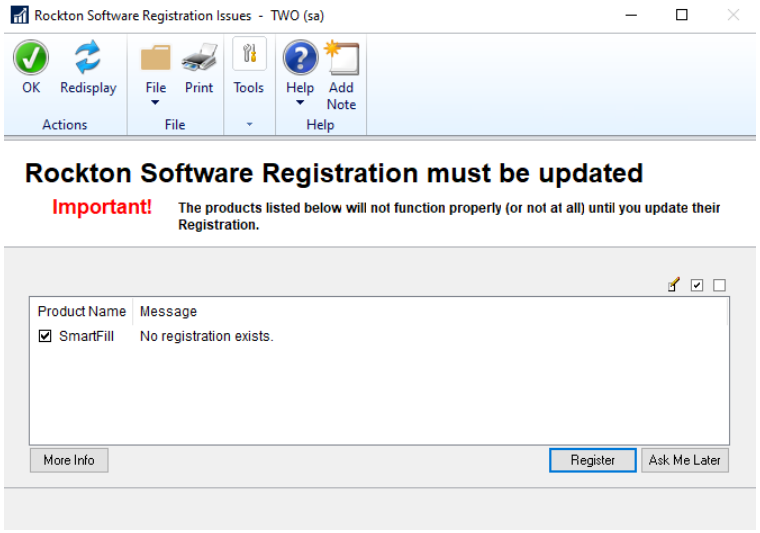
6. Mark the **Accept License Agreement** check box, then click the Next button to launch the Install Progress dialog. You may see some informational messages as the installation continues. Take note of these and click OK or respond to them as necessary.



7. If you have Security Auditor installed and have Security Audits logged or you have created Segregation of Duties Groups, you will be allowed to Import from Security Auditor into Auditor at the end of the install.

8. When the installation has completed, press the Finish button. The Auditor Install Status window will open. Take note of any messages on the Install Status window and click OK.

9. If you have not previously registered your software, the following window will open:



This will show any Rockton products not currently registered. If you wish, you can click the Register button to have your registration loaded automatically.

To register the product manually, choose Registration on the Auditor Setup window to open the Auditor Registration window. Click Import Registration and import the registration file you received previously.

For subscription products that are registered, a periodic check is done to verify their registrations are valid. Administrators may see a progress dialog when logging in during this check while non-admin. users will not. We recommend an administrator log in periodically to verify your subscription status for each product. If issues are found during the process, you will see a message relating to the issue.

If you are using Auditor to audit database changes at the SQL level (SQL Table Audits), then all of the SQL Logins that will be performing those changes must have EXECUTE permission to the stored procedure rsaLogAudit if they are not in the DYNGRP role.

10. Log out of Dynamics GP and log back in.

Verify the Installation

Test at least one audit of each type (Form, Table, and SQL Table) using different user types (POWERUSER, Auditor Administrator, regular user, etc., as appropriate) in a company other than Fabrikam.

This completes the installation process for the first workstation.

Navigation

An Auditor menu is added to the Setup menu in Dynamics GP. You will be able to access all of Auditor's functionality from this menu.

However, you may find it more convenient to use the Auditor Toolbar. The toolbar includes these three buttons:

- Auditor Setup menu
- Auditor Message Center
- Audit Groups

You can also add Auditor windows to the Navigation Pane as follows:

- Go to the Home Page.
- Right-click in the Navigation Pane, anywhere above the Navigation Buttons. From the context menu, choose **Add** and then **Add Window…**.
- Double-click Auditor in the Add Window Shortcut window. Navigate to the window that you want to access and then press the **Add** button.
- Press the **Done** button.

Because Auditor with E-Sign is designed to be an administrative tool, Auditor windows will only appear on the Dynamics GP menus and on the Dynamics GP toolbar if you are logged in as a user in the AUDITOR ADMIN Security Role or the POWERUSER Security Role.

Auditor Security Settings

Security in Auditor can be administered via the following Security Items:

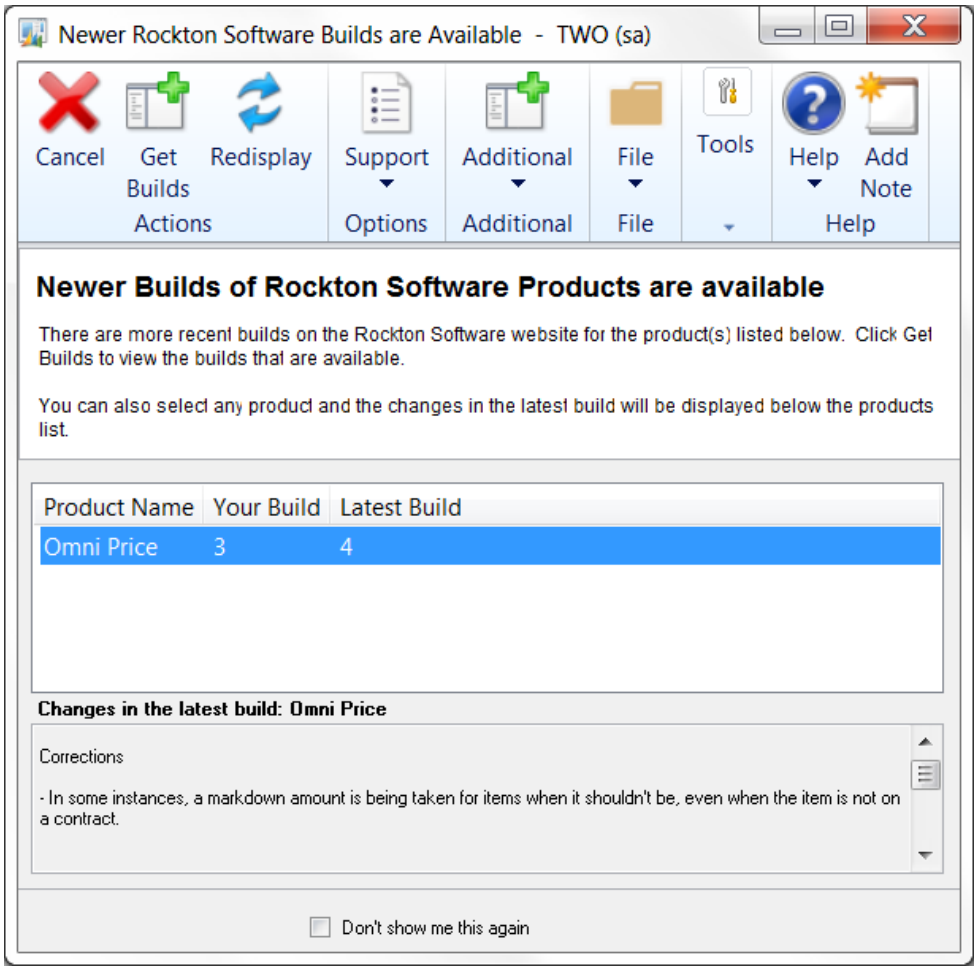
Name	Role or Task	Description
AUDITOR ADMIN	Role	Used to set access to an Administrator of Auditor.
AUDITOR AUDITORS	Role	Used to set access to an auditor that will be reviewing audits and Auditor setup, but not making changes to Auditor setup.
AUDITOR INQUIRY	Role	Used to set access for users that need to see Auditor Smartlists, but are not allowed to add or make changes to any Favorites that have been set up for them.
ADMIN_AUDITOR_01	Task	Contains all windows necessary to setup and administer Auditor. Typical Users do not need to have access to these windows.
ADMIN_AUDITOR_02	Task	Contains all windows necessary for auditors to use Auditor.
ADMIN_AUDITOR_03	Task	Contains only Auditor Smartlist objects.
DEFAULTUSER	Task	Contains all the windows that are required for the average User to be able to use Auditor. No setup or administration windows are included.

Auditor Administrators

Certain users of this software will have the ability to perform functions that the average user cannot. These functions may include but are not limited to installation, setup, and configuration of advanced features. We will call these users “Auditor Administrators”.

Auditor Administrators are selected on the System Settings window in Auditor.

Newer Rockton Software Builds are Available window



This window opens automatically when an Auditor Administrator logs in if any Rockton products are found to have newer builds available for download on www.rocktonsoftware.com.

Description

Whenever an Auditor Administrator logs in, the system will check to see if any of the installed Rockton products have updates available on the Rockton Software website. If all products are up-to-date, then this window will not open. Otherwise, the products that have updates available will be listed here.

You will see the build that you currently have installed, as well as the Latest Build available on our website. If you select any of the products listed, you will see the changes for that build in the box at the bottom of the window.

If you want to download any of the latest builds, click the Get Builds button and your Internet browser will open to the Downloads page on our website. Here you will see all of the latest builds for each of our products and each version of Dynamics GP for which they are available. If you don't want to download at this time, click the Cancel button.

If you don't want to be notified of new builds any more, mark the "Don't show me this again" check box and you won't be notified of a new build again until the next time you install a Rockton product.

Removing Auditor with E-Sign

These steps will completely remove Auditor with E-Sign from workstation and server:

1. Log in to Dynamics GP as any User that is either in the 'sysadmin' fixed server role or the 'db_owner' role for the DYNAMICS database.
2. Open the Auditor Setup window and select the Uninstall Tab. Then select the Complete Uninstall task to completely uninstall from the server, or select Workstation Uninstall to simply remove it from the current workstation.
3. Click OK on the message to close Dynamics GP.
4. Delete the following files from the Dynamics GP install folder (you may not find all of them):

AUDIT.DIC	AUDIT.VBA	Audit.cnk
Auditor Manual.pdf	Auditor Whats New.pdf	Auditor ReadMe.txt
AUDITOR SETUP.auditor	E-SIGN SETUP.auditor	Audit.chm

   Any files that start with RSA_BACKUP and have an extension of .xml
5. Delete the following files from the Dynamics GP Data folder (you may not find all of them):

FRMS2704.DIC	RPTS2704.DIC

6. If you chose Complete Uninstall in step 2, then log into Dynamics GP as a User that has access to the Security windows. Remove the AUDITOR ADMIN Security Role and the ADMIN_AUDITOR_01 Security Task.

Manually uninstalling

The following steps can also be used to manually remove Auditor with E-Sign:

Manually uninstalling from a Workstation

Perform this process on each workstation where you want to remove Auditor with E-Sign.

1. Edit the Dynamics.set file (located in the Dynamics GP installation directory) to remove the Auditor entries. There are three steps to this:
   a. The first line in the file should be a number. Subtract 1 from this number.
   b. Remove these two lines:
      2704
      Auditor
   c. The bottom part of the file contains several path names. Remove the ones that reference the following dictionaries: AUDIT.DIC, FRMS2704.DIC and RPTS2704.DIC.
2. Delete the following files from the Dynamics GP install folder (you may not find all of them):

AUDIT.DIC	AUDIT.VBA	Audit.cnk
Auditor Manual.pdf	Auditor Whats New.pdf	Auditor ReadMe.txt
AUDITOR SETUP.auditor	E-SIGN SETUP.auditor	Audit.chm

   Any files that start with RSA_BACKUP and have an extension of .xml
3. Delete the following files from the Dynamics GP Data folder (you may not find all of them):

FRMS2704.DIC	RPTS2704.DIC

Manually uninstalling from the Server

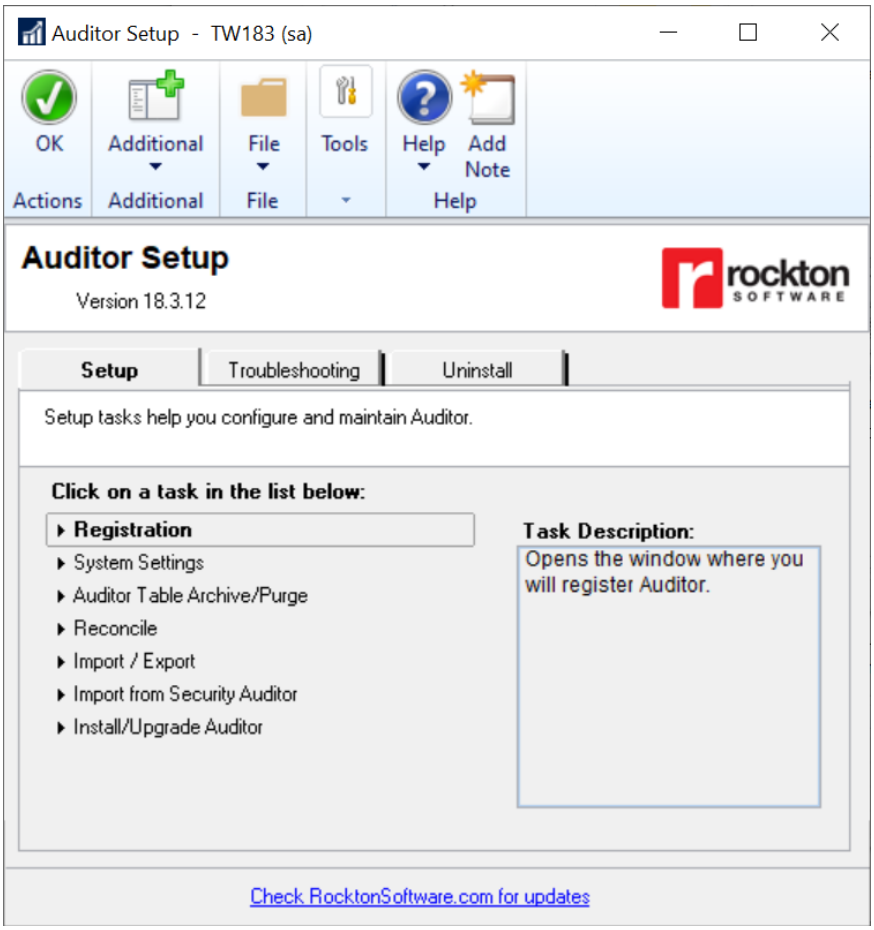
Perform this process to completely remove Auditor with E-Sign from the system.

1. Open SQL Enterprise Manager.
2. Drop all tables in the DYNAMICS database that are named RSAxx, (xx is the table number).
3. Drop all stored procedures in the DYNAMICS database whose names start with zDP_RSAxxYYY (where xx is the table number and YYY is one of 11 possible suffixes).
4. Drop these stored procedures, which are located in the DYNAMICS database:
   rsaLogAudit, rsaUpdateMessageCenter, and rsaFindSODConflicts
5. Drop these scalar functions, which are located in the DYNAMICS database:
   rsaDatabaseTableID and rsaHasSecurityAccess
6. Log into Dynamics GP as a User that has access to the Security windows. Remove the ADMIN_AUDITOR_01 Security Task and the AUDITOR ADMIN Security Role.

Setup

Auditor Setup window

The Auditor Setup window allows you to perform setup and maintenance tasks.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > Auditor Setup.

Description

The Auditor Setup window gives you access to all of the tasks you will need to configure and maintain the system. It contains three tabs:

- Setup
- Troubleshooting
- Uninstall

You can see a brief description of each task by moving your cursor over any of the tasks in the list. To select a task, simply click on the task name.

Clicking the “Check RocktonSoftware.com for updates” link will take you to the Downloads web page for this product. Here you can verify that you are installing the latest build.

The tasks available for each tab are described in the following tables:

Setup tab

Setup tasks help you configure and maintain Auditor.

Task	Description
Registration	Opens the window where you will enter a registration key.
System Settings	Opens the Auditor System Settings window. This is where you can configure various options for Auditor.
Auditor Table Archive/Purge	Opens the Auditor Table Archive/Purge window. This is where you can purge or archive the Audit Log and E-Sign Approval Log tables.
Reconcile	Opens the Auditor Reconcile window where you can run the process to ensure the integrity of your audit setups. A report will inform you of any discrepancies.
Import / Export	Opens the Import / Export window. This will allow you to save and restore values from Auditor tables.
Import from Security Auditor	Opens the Import from Security Auditor window where you can bring over the Security Audit Log and any Segregation of Duties Groups that you created in Rockton's Security Auditor product into Auditor.
Install/Upgrade Auditor	Installs the software, or upgrades it from a previous version. This may take several minutes. It will also set table permissions to all users in the system database. You can perform this task multiple times without causing any problems. **Note:** you must be logged in as a User that is in the 'sysadmin' fixed server role or the 'db_owner' role for the DYNAMICS database and any database for which there are SQL Table audits defined.

Troubleshooting tab

These tasks are for troubleshooting only. You may be asked to use them by Rockton Support.

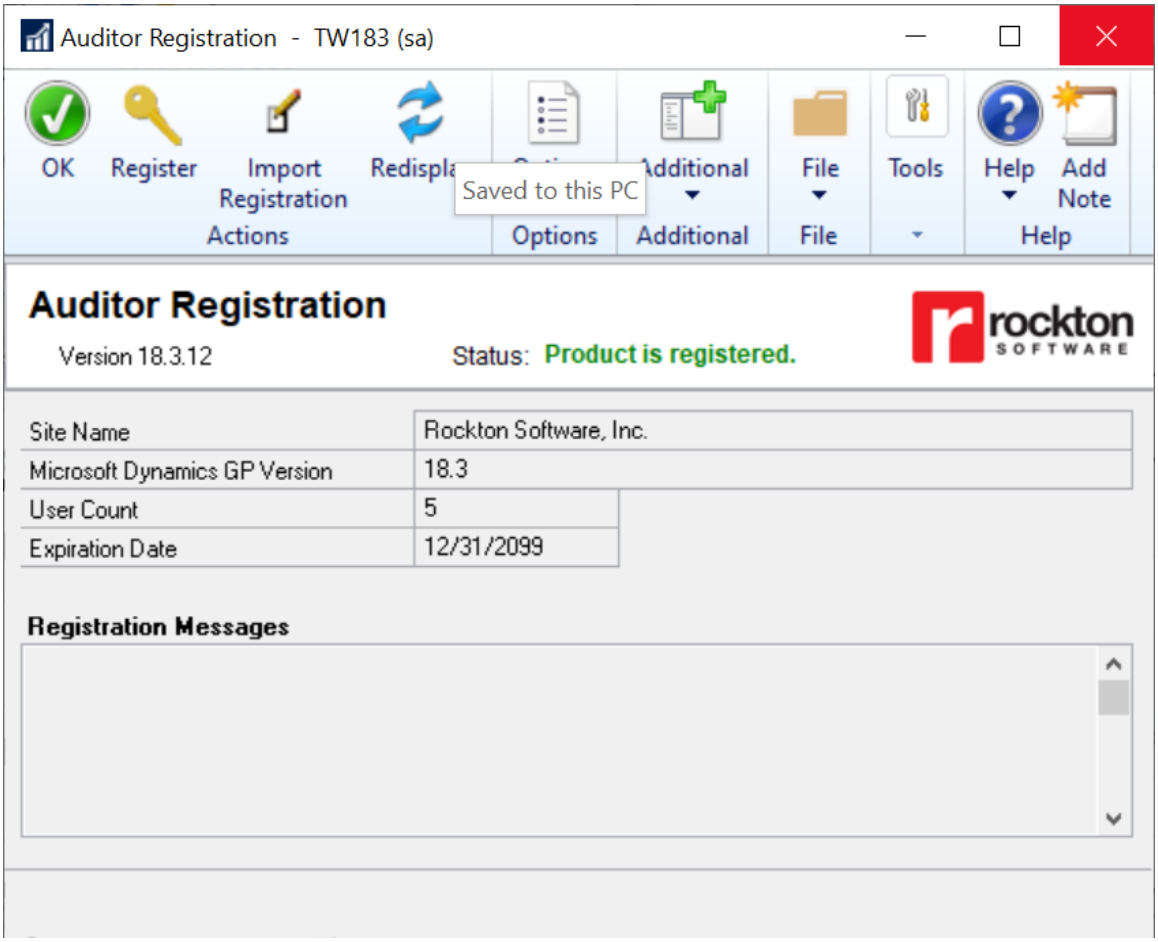
Task	Description
Add or Remove Smartlist Objects	Adds or removes the Audits and E-sign Approvals objects from Smartlist.
Rebuild	Opens the Auditor Rebuild window where you can rebuild system tables or SQL objects.
Re-add Security Data	Adds Security Roles and Tasks for Auditor, if they have been deleted. **Note:** you must be logged in as a User that has access to run the Install/Upgrade option (as described above) or a User that has Security access to both the Security Role Setup and Security Task Setup windows in order to use this option.
Rebuild Toolbars	Removes and recreates default toolbar items for this product.
Move to First Position	Moves Auditor to the first position in the launch file after Dynamics GP.
Remove from Launch File	Removes Auditor from the launch file.
Rebuild Menus	Rebuilds menu navigation for Auditor by first removing all menus from the Menu Master table. To complete the process you must log in again to see the rebuilt menus.
Enable Script Logging	Enables script logging, beginning with the next time you log into Dynamics GP from this workstation.
Diagnostics Mode	This option may gather diagnostics, create log files, open the Code window, or other things that may be helpful to Rockton Support.

Uninstall tab

These tasks can be used to uninstall Auditor from the system or just from this workstation.

Task	Description
Workstation Uninstall	Removes Auditor from the launch file. Also removes settings from the Defaults file.
Complete Uninstall	Auditor tables will be removed from the database(s) and the product will be removed from the launch file.

Auditor Registration window



You can get to this window in one of these ways:

- From the Navigation Pane.
- Go to Help > About Microsoft Dynamics GP… and from the Additional menu, choose About Auditor. Then click the Register button.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > Auditor Setup. Then click the Registration task.
- From the Rockton Software Registration Issues window, double-click a product in the list.
- Click the Administration navigation button to open the Administration Area Page. Then select Auditor Setup from the Auditor sub menu. From the drop-down, choose Registration and choose the Process button.

Description

The Auditor Registration window is where you can automatically register your product or manually import the product registration file.

You can tell from the Status field whether the product is registered or if there is an issue with the registration.

Status	Values
No registration exists	Registration request has not been made due to new product install or product has been unregistered.
Product is registered	Product was registered successfully.
Registration is expired	Existing registration has expired. For example, a trial registration expires after 30 days.
Registration is invalid	Registration information does not match information in Dynamics GP. Typically, this is due to Site Name, User Count, or Dynamics GP version not matching.

To automatically register the product, click the Register button and a request will be made to check for valid a registration. If found, the window is populated with the necessary information and the Status is set to Product is Registered. If a valid registration is not found, then you will receive more information as to the status of the registration.

If you need to manually import the product registration, click the Import Registration button. Select the XML file you received previously from Rockton Sales. If the file is valid, the Status field will show Product is Registered. If the file is not valid, the Status will show Registration is invalid or Registration is expired.

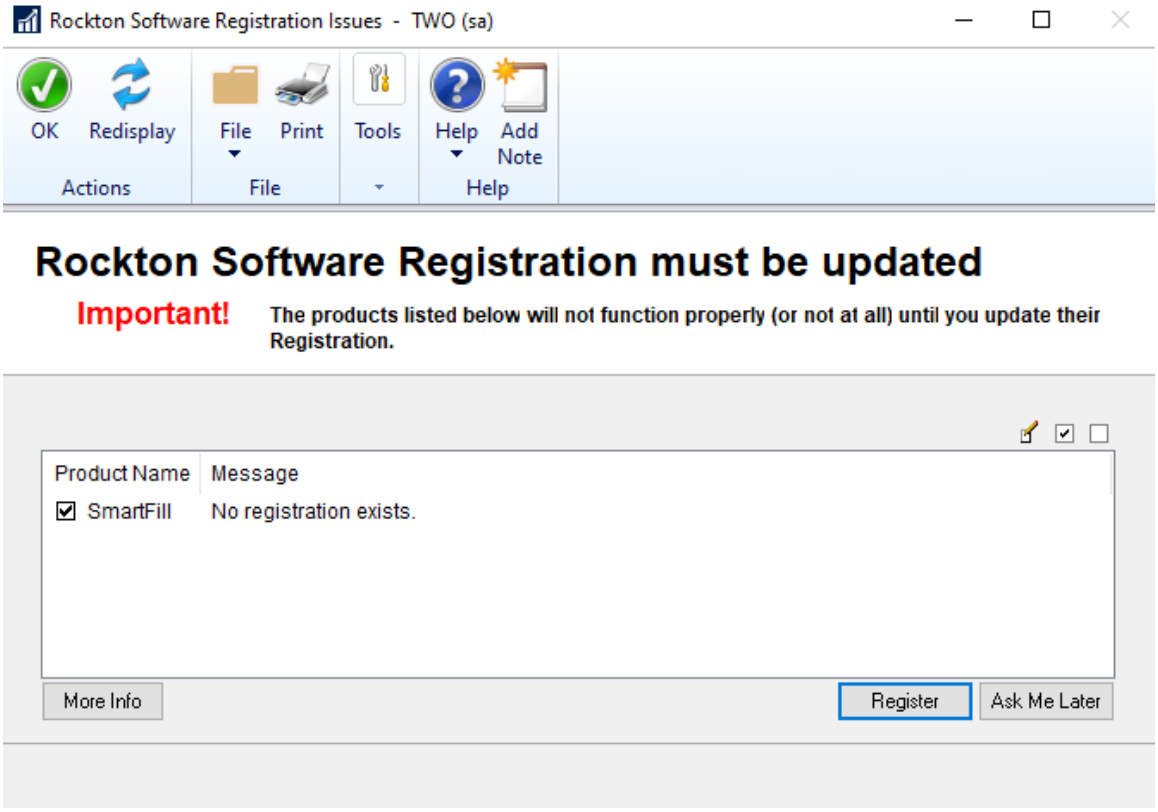
If the Site Name, Microsoft Dynamics GP Version, or user Count does not match the current Dynamics GP values, a warning indicator (⚠) will appear next to the corresponding field. If the registration has expired, you will see a warning indicator next to the Expiration Date field.

The Registration Messages box will provide additional information regarding the registration information that was obtained from the request or from the import.

Should you need to Unregister the product for any reason, click the Options button and then click Unregister product. This will automatically remove the registration information from the window.

If you hare having issues with registering the product, contact Rockton Software to verify that your Site Name, User Count and Dynamics GP version have not changed since your last registration.

Rockton Software Registration Issues window



This window opens automatically if any Rockton products are not properly registered:

- when you exit the Dynamics GP Registration window.
- when a System Administrator logs in.
- after completing the Installation Wizard.

Description

Whenever you close the Dynamics GP Registration window, the registration for all Rockton products that you have installed will be verified. If any are found to be invalid (for instance, because the User Count or Site Name has changed since the last time the Rockton registrations were updated), then this window will open automatically. The box at the bottom of the window will list each Rockton product that requires new registration.

You can attempt a new registration for the products listed. If you do not have a valid registration for any of the products listed, in most cases you will be given a temporary registration that will expire in 30 days.

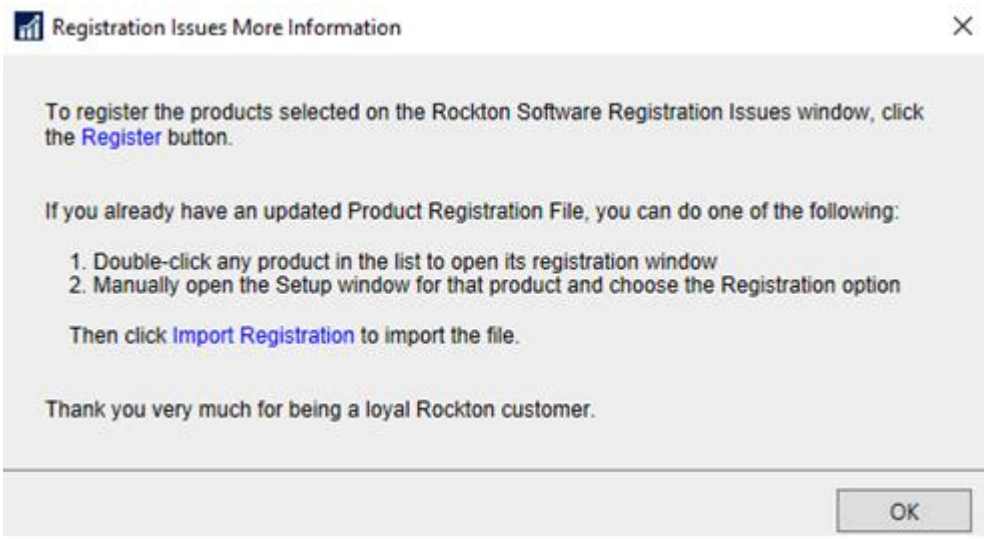
To retrieve your registration information, simply mark the check box for each product that requires new registration, and then click the Register button. This will automatically attempt to register each product selected. If registration cannot be obtained, you will see a message that indicates there was a problem. You can click the text in the Message column to see additional information on resolving the issue. After a request has been sent to register, an icon appears to the left of the Product Name that will show the results for the registration attempt. You can click the icon to get more information related to the results of the request.

You may also import the product registration file that may have been provided to you from the Rockton Sales team by double-clicking the product in the list above or clicking the Edit icon. This will open the Registration window for that product. From there, click the Import Registration button and import the file.

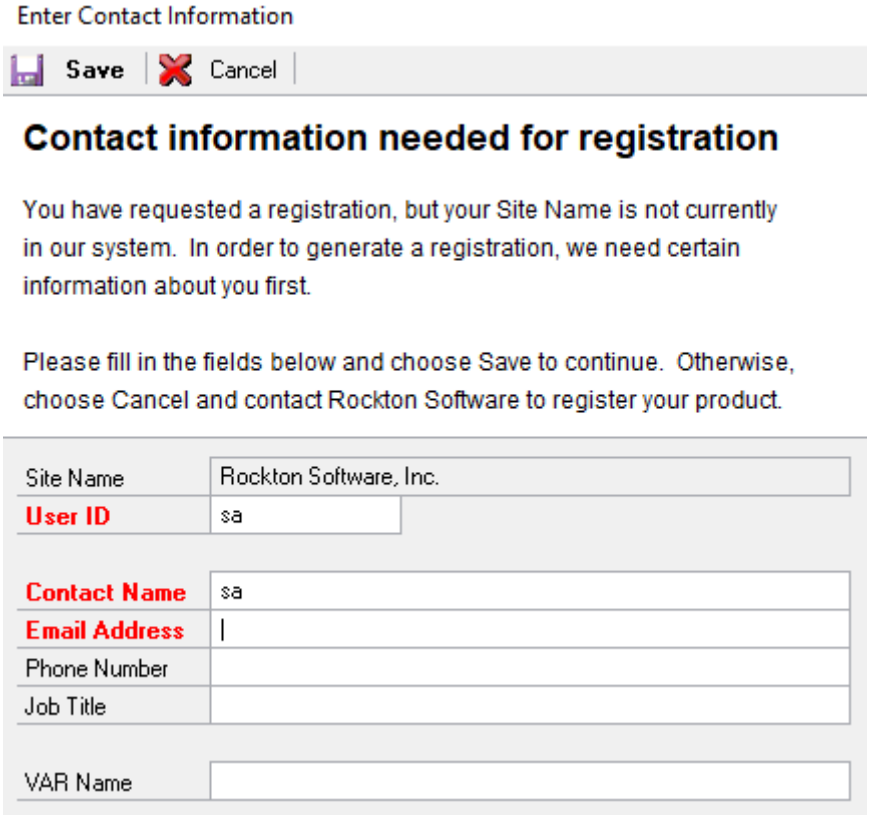
If you are using a subscription product, a subscription check is run periodically to validate the current registration. Administrator users will see a progress dialog when this request is made and will see messages if there is an issue with the registration. Non-administrator users will not see this progress so we recommend an administrator log in to Dynamics GP periodically to validate registrations for Rockton products. If information has changed regarding Site Name, User count, or Dynamics GP version, the registration will become invalid and you will need to contact Rockton Software for further assistance. If you're using a non-subscription product, your registration will continue to be verified and open the Rockton Software Registration Issue window when an issue is found.

If you plan to resolve the registration issue at another time, you can click Ask Me Later to be prompted with this window later. The options are Next Login or Tomorrow.

You can click the More Info button for steps on how to register the product.



Enter Contact Information window

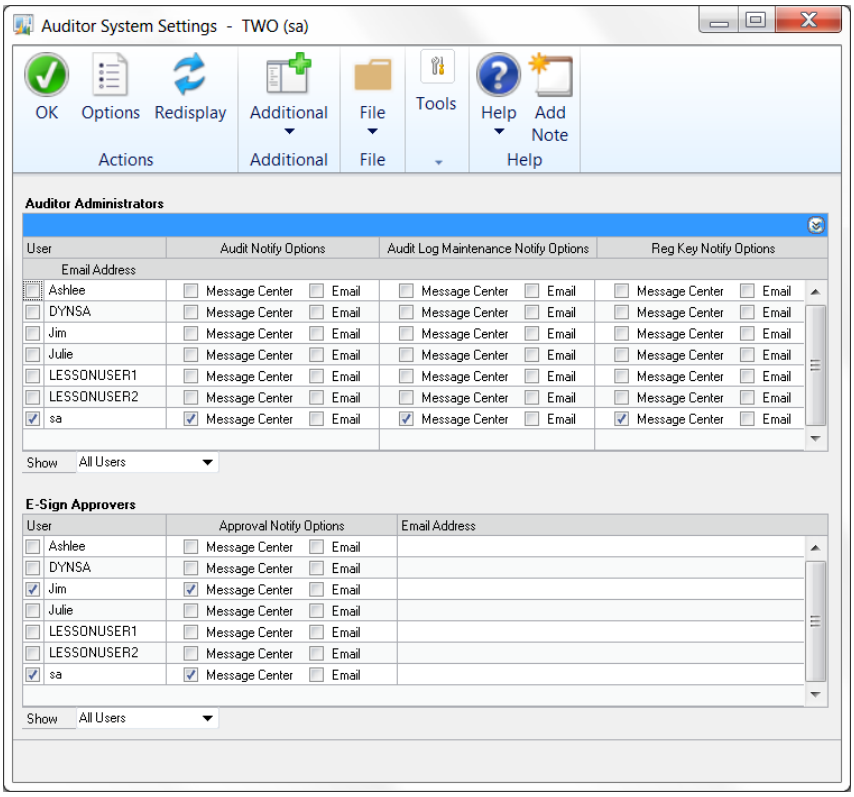


Description

This window opens automatically when a request is made for registration and your Site Name does not exist in our system. You can enter the information and click Save or you can contact Rockton Software directly to register your product.

Auditor System Settings window

This window allows you to manage Auditor Administrators and E-Sign Approvers.



If a user is in the AUDITOR AUDITORS security role, they will be able to view the Auditor System Settings window, but not make any changes to the options presented here. This is true even if the user is also in the POWERUSER or any other security role.

This window is accessible in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN or POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > System Settings.

Description

This window lets you specify users as Auditor Administrators and/or E-Sign Approvers. Auditor Administrations can optionally be notified in the Message Center or by Email when certain events occur. E-Sign Approvers are the only Users that can approve or deny changes made to fields with E-Sign Signatures assigned to them. You can select multiple Auditor Administrators and E-Sign Approvers. It is OK for a User to be both.

Auditor Administrators can be notified when certain Auditor-related things happen in the system. There are two notification options for Auditor Administrators: **Message Center** and **Email**. Selecting **Message Center** will add an item to the Auditor Message Center window for that Auditor Administrator. **Email** will send an Email to the address specified for that Auditor Administrator.

A MAPI-enabled email client such as Microsoft Outlook must be configured on the computer where the audit occurs for the email option to work.

The following notify options are available:

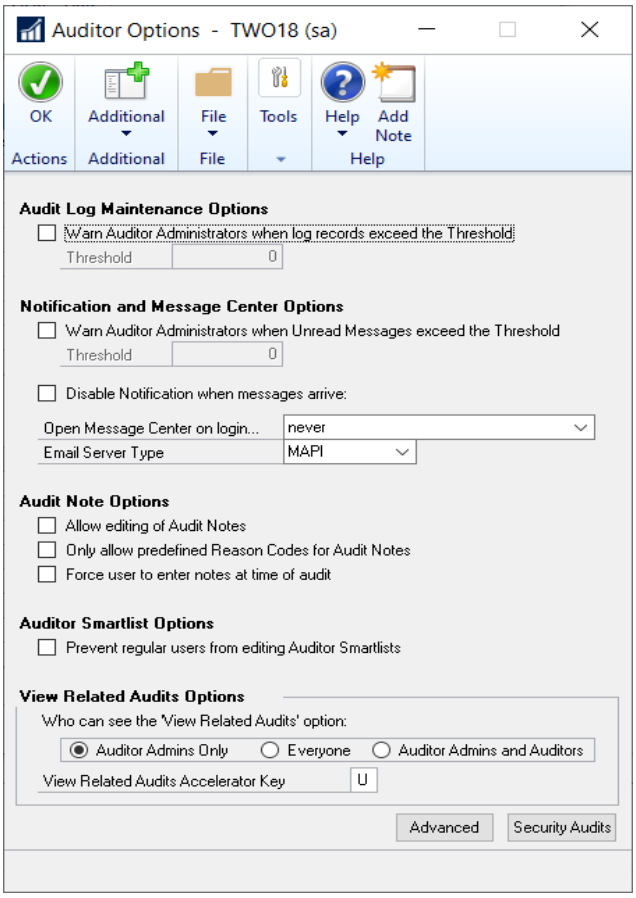
Option	Description
Audit Notify	For each audit, you can optionally notify Auditor Administrators when that audit occurs. This option indicates that this Auditor Administrator should be notified.
Audit Log Maintenance Notify	When the size of the Audit Log reaches the specified threshold, this Auditor Administrator will be notified. This notification will be sent to the Message Center only once per day for this Auditor Administrator.
Reg Key Notify	If, for some reason, your Auditor Registration Keys become invalid (e.g. you GP User Count changes or you had temporary keys that expired), this Auditor Administrator will be notified. This notification will be sent to the Message Center only once per day for this Auditor Administrator.

E-Sign Approvers will be allowed to approve or deny changes made by other Users to fields that have a Signature assigned to them. Specific Approvers can be assigned to individual Signatures as well. The same notification options exist as for Auditor Administrators,

Clicking the Options button opens the Auditor Options window.

Auditor Options window

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Auditor Options window, but not make any changes to the options presented here. This is true even if the user is also in the POWERUSER or any other security role.



Audit Log Maintenance Options

"Warn Auditor Administrators when log records exceed the Threshold" – If you check this checkbox, enter the number of records acceptable in the log file before being notified. We recommend about 10,000 records to start with. If this option is checked, then any user marked above as an Auditor Administrator will receive a warning message notifying them that the log has exceeded this limit when they log in to Dynamics GP.

Notification and Message Center Options

"Warn Auditor Administrators when Unread Messages exceed the Threshold" – Checking this box lets you specify the maximum number of unread messages in the Message Center before Auditor Admins are notified. If this option is checked, any user that is an Auditor Administrator will, upon logging into Dynamics GP, receive a warning message notifying them that the Message Center has reached its unread message limit.

"Disable Notification when messages arrive" – Prevents the notification box that normally appears in the lower-right corner of Dynamics GP from being displayed.

"Open Message Center on login…" – Select when, or if, the Message Center should open after an Auditor Administrator logs into a Company. The following options are available:

Option	Description
only when there are unread messages	The Message Center window will open only if unread messages exist for the Auditor Administrator that is logging in.
always	The Message Center window will always open after an Auditor Administrator logs into a Company.
never	The Message Center window will not open after an Auditor Administrator logs into a company.

"Email Server Type" – Select the email type you are using (MAPI or Exchange).

Audit Note Options

"Allow editing of Audit Notes" – Allows users to edit their notes in the Audit Inquiry window. Open this window from Smartlist by double-clicking an audit. Checking this box lets users edit their notes in the future rather than being limited to just the initial entry when the audit is captured.

"Only allow predefined Reason Codes for Audit Notes" – This option requires the user to pick a predefined Reason Code from the Note/Reason drop-down on the Auditor Note Maintenance window, rather than allowing them to enter freeform text for the note/reason. If you use this option, be sure that you supply a reason code on the Field Options window for any audit that requires a note.

"Force user to enter notes at time of audit" – This option won't allow a user to exit the Auditor Note Maintenance window if any audits are listed in the Outstanding Notes list.

Auditor Smartlist Options

"Prevent regular users from editing Auditor Smartlists" – Keeps users that are not in the AUDITOR ADMIN security role from being able to make changes to Auditor Smartlists that would allow them to see additional data.

View Related Audits Options

"Who can see the 'View Related Audits' option:" – Controls who sees View Related Audits on the Additional menu for windows in Dynamics GP. Choose from these options:

- **Auditor Admins only**
  Only users who are selected as Auditor Administrators on the Auditor System Settings window will be allowed to View Related Audits.
- **Everyone**
  All users are allowed to View Related Audits.
- **Auditor Admins and Auditors**
  Only Auditor Administrators marked on the Auditor System Settings window and those in the AUDITOR AUDITORS security role can View Related Audits.

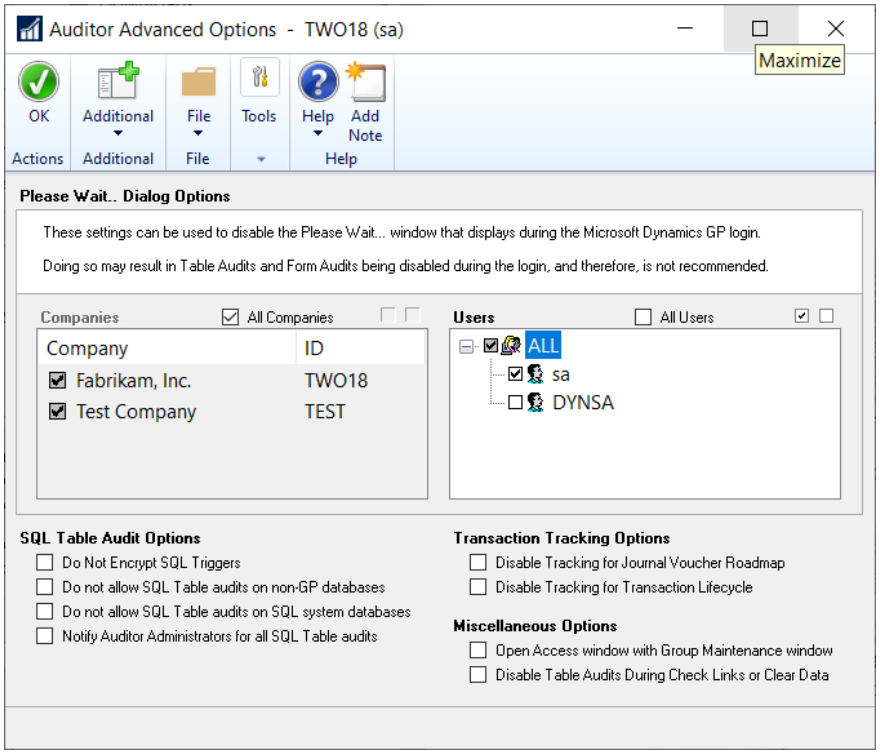
"View Related Audits Accelerator Key" – This assigns the accelerator key for the View Related Audits. E.g., enter U here and CTRL+U will open the View Related Audits window from any window with the View Related Audits option on the Additional menu.

Advanced and Security Audits options

Choosing the **Advanced** button will open the Auditor Advanced Options window. This is where you can specify settings for the Please Wait dialog, SQL Table Audit options, Transaction Tracking Options, and other Miscellaneous options.

Choosing the **Security Audits** button opens the Security Audit Options window. Here you enable automatic logging of changes to standard security settings in Dynamics GP.

Auditor Advanced Options window



Please Wait Dialog Options

The Please Wait dialog can be disabled for specified Users and Companies. We recommend that you enable this for all users in all companies as a safety feature to ensure that all Audits will be activated. See the section on this dialog for details on its purpose and how it functions.

If you do decide that you want to disable it in some cases, here is where you can do it.

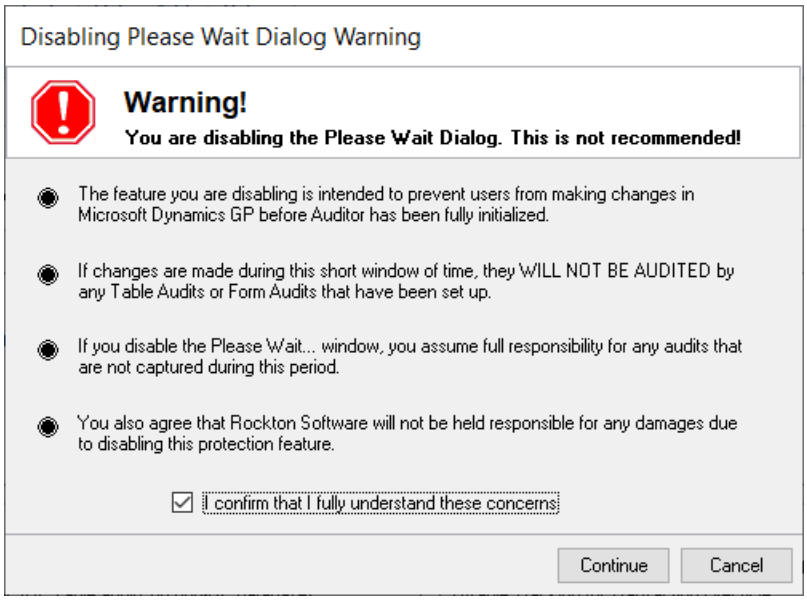
"All Companies" – Mark this box to enable the Please Wait dialog in all companies. If this box is marked, then it will be enabled even new companies added to the system.

If it is unmarked, then you will be able to select specific companies to enable or disable.

"All Users" – Mark this box to enable the Please Wait dialog for all Users. If this box is marked, then it will be enabled even new Users added to the system.

If it is unmarked, then you will be able to select specific Users to enable or disable.

Unmarking either All Companies or All Users will open the following confirmation dialog. Please read these considerations carefully before proceeding.



SQL Table Audit Options

"Do Not Encrypt SQL Triggers" – This option may be used when working with Rockton Support. Under normal circumstances you will leave this box unchecked.

"Do not allow SQL Table audits on non-GP databases" – Causes the "Rebuild SQL Tables Master" process to exclude all databases except the DYNAMICS database and all company databases used by Great Plains. These will then be the only databases that show up in the list when you attempt to add a SQL Table audit. Marking this option runs a Reconcile process that will remove any such audits that you already have defined, as well as any stranded records. You will be prompted before this process begins.

"Do not allow SQL Table audits on SQL system databases" – This option causes the "Rebuild SQL Tables Master" process to skip the master, model, msdb, pubs, ReportServer, and ReportServerTempDB databases. These databases will not show up in the list when you attempt to add a SQL Table audit. Marking this option will run a Reconcile process that will remove any such audits that you already have defined, as well as any stranded records. You will be prompted before this process begins.

Note that tables in the tempdb database will always be excluded from this list and therefore will not be available for SQL Table audits.

"Notify Auditor Administrators for all SQL Table audits" – This option controls whether or not a record is written to the Message Center for Auditor Administrators who have selected the Message Center Audit Notify option. This option only applies to SQL Table audits, but it should be noted that it applies to ALL SQL Table audits.

Transaction Tracking Options

"Disable Tracking for Journal Voucher Roadmap" – This option turns off the tracking of Batch Number, Created by, and Date Created on the Journal Voucher Roadmap window. When you change this option, you will be prompted to restart Dynamics GP.

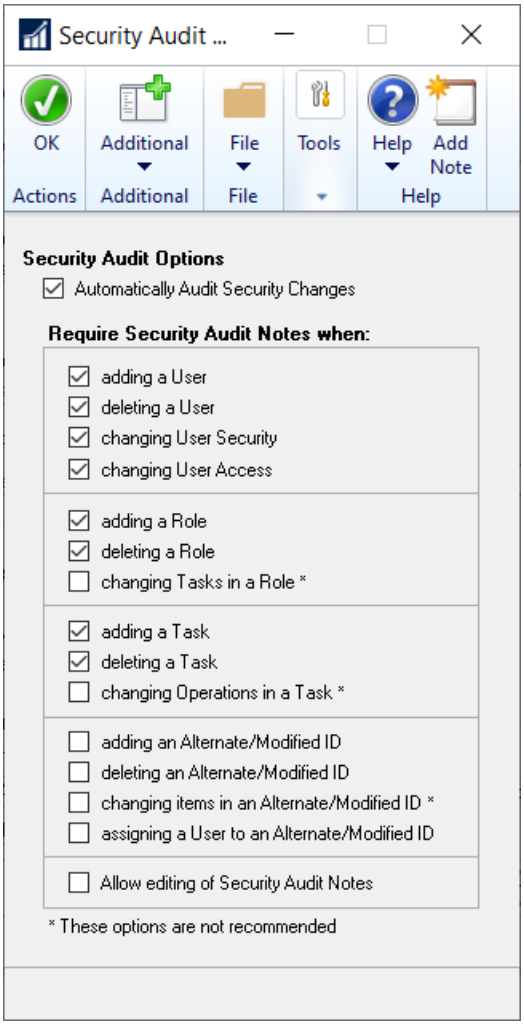
"Disable Tracking for Transaction Lifecycle" – This option turns off the tracking of Created by and Date Created on the Transaction Lifecycle window. This will affect Work records only. When you change this option, you will be prompted to restart Dynamics GP.

You may never use the Disable Tracking for Journal Voucher Roadmap or Disable Tracking for Transaction Lifecycle options, but they can be useful in troubleshooting possible negative interactions between products.

Miscellaneous Options

"Open Access window with Group Maintenance window" – Causes the Audit Group Access window to open automatically whenever you open the Group Maintenance window. This can be convenient if you have many Audit Groups that apply to only certain Users or Companies. By default, this option is unchecked.

"Disable Table Audits During Check Links or Clear Data" – Prevents table audits from being logged when running a Check Links or Clear Data file maintenance process in Dynamics GP. This can be helpful if you find that these processes are taking a lot longer to complete after you install Auditor. Typically, changes made during these process are not something that you would want to audit since each individual change was not made as a result of a user's action.



Security Auditor Options window

"Automatically Audit Security Changes" – This option causes an audit to be logged each time someone makes changes to security-related settings in Dynamics GP. No other setup is required on your part to define these audits. They will happen automatically as long as this box is checked. The Security Audits log can then be viewed from Smartlist.

Changes to the following security settings will be logged in the Security Audits log:

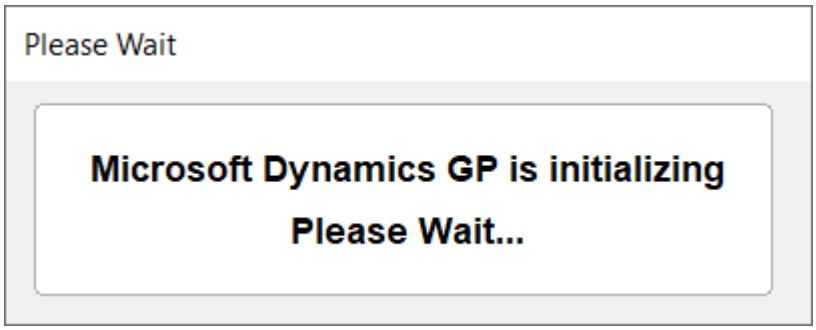
- Creating, deleting or editing a User or their Password
- Assigning or removing a User's access to a Role
- Assigning or removing a User's access to a Company
- Creating, deleting or editing a Role
- Creating, deleting or editing a Task
- Assigning or removing operations from a Task
- Creating, deleting or editing an Alternate/Modified Forms and Reports ID
- Assigning or removing operations from an Alternate/Modified Forms and Reports ID

"Require Security Audit Notes When" – Whenever a security-related audit occurs, you may want to log a reason that the change was made. If so, marking any of the checkboxes in this section will cause the Security Auditor Note Maintenance window to open for any security-related audit that occurs. This will allow the user making that security change to enter a "note", or reason, why they made that change.

We don't recommend using notes when changing Tasks in a Role, changing Operations in a Task or changing Forms and Reports in a Alternate/Modified Forms and Reports ID. This can result in a large number of changes, making note entry counterproductive.

"Allow editing of Security Audit Notes" – This option lets users edit their notes in the Security Audit Inquiry window by double-clicking a security audit from the Smartlist window. By checking this box, users can edit their notes in the future rather than being limited to just the initial entry at the time the security audit is captured.

Please Wait dialog



This dialog opens automatically after you log into a Company in Dynamics GP.

Description

The Please Wait dialog opens automatically if you attempt to open any windows before Auditor has been fully initialized. Its purpose is to prevent users from doing anything in the system that might not otherwise be audited because Auditor is not yet fully active. As long as this window is open, a user cannot do anything in Dynamics GP. Once Auditor's initialization has completed, this window will close automatically.

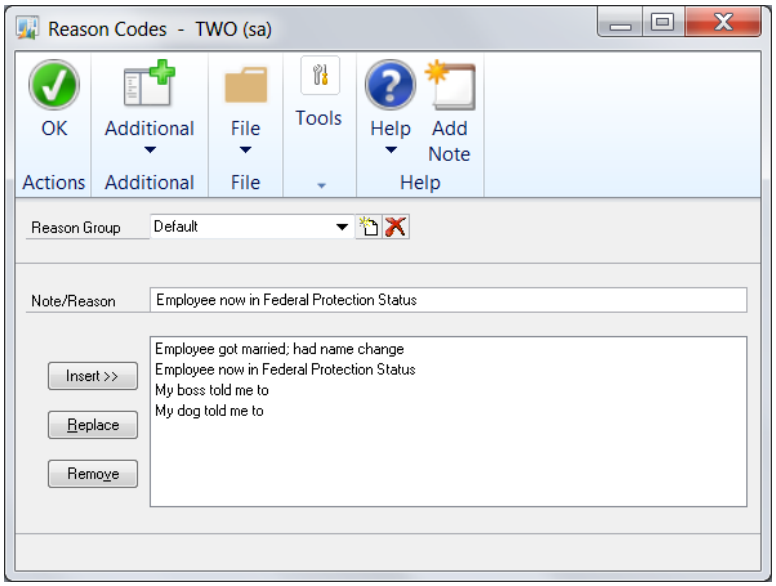
You may find that the Please Wait dialog opens shortly after you log in to a Dynamics GP Company, even though you have not attempted to open any windows. This will happen if your system is configured to automatically open any windows on the login (for example, the Reminders window). There may even be "hidden" system windows that open in the background, and which you do not see, that can trigger the Please Wait dialog to open.

Once Auditor is through initializing, the Please Wait dialog will close automatically.

The Please Wait dialog will not open if you have the Safe Login tool in Rockton Software's Dynamics GP Toolbox product enabled. This is because these two windows have equivalent functions.

Reason Codes window

The Reason Codes window is where you set up common reasons for making system changes.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > Reason Codes.

Description

Reason Codes are predefined notes that are common reasons for making changes in the system. For instance, changing an employee last name is often due to marriage or court decree. You may want to preset the reasons in a list so users can quickly choose a reason during note entry without having to type it in.

Reason Groups allow you to package several Reason Codes together. For instance, you may have three reasons for a name change on employees, and you may have six reasons why a credit memo was issued. Reasons that appear in one situation may not make sense in another. By separating these reasons into two Reason Groups, you can make Note Entry and the E-Sign Approval process more useful by specifying which Reason Group is to be used. This is specified in the Field Options window for a given Audit or E-Sign Approval.

You can create a new group by pressing the New Reason Group button ( ). This will open the Add New Reason Group window, where you will enter the Reason Group name and then press OK to add the Reason Group. Similarly, you can delete a group by pressing the Delete Reason Group button ( ).

Enter a reason in the Note/Reason box, and then press Insert to add it to the list. You can also select an entry in the list, then edit its text and press Replace. Finally, you can remove a specific reason by selecting it in the list and pressing the Remove button.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Reason Codes window, but not make any changes to any Reason Codes. This is true even if the user is also in the POWERUSER or any other security role.

Creating Audits

Overview of Auditor and Auditing

An audit is the logging of a change. When a field changes, you can either “Audit” that field or you can “Audit with Note”. Notes are helpful when you want users to explain why they made a data change. For instance, if you are auditing employee information, such as name, address, and status, you may want to use an audit for name and address fields but place an Audit with Note option on the Department field. By doing this, when a user changes the Department field for an employee, they will be required to enter a note explaining the reason for the change. Notes will be tracked as part of the audit.

You may be tempted to audit everything in your system. This is not recommended. Carefully review the reasons why you want to audit data, and what, specifically, you want to audit. Because an audit is created for every field change (except for the Table method) the audit log can grow very large very fast. An extremely lengthy audit log which tracks everything is often useless to anyone.

Performance Issues with Auditing

Because Auditor can track so much information, you might encounter performance limitations when using Auditor.

In general, auditing by the Window method shows a non-noticeable effect on performance and speed. Because auditing is done real-time, a small amount of processing occurs each time a user enters and exits a field. Only a very fast typist who changes several fields in rapid succession would notice any performance degradation, and this is highly unlikely to be noticed at all.

When auditing using the Table or SQL Table methods, it is unlikely that you will experience performance degradation unless using a batch process. If you are auditing a table where users are editing one record at a time using data entry screens, the effect is not noticeable. However, if you are posting a batch of transactions, and auditing each record, you may notice a slight delay in processing. For instance, if you are auditing deletes on unposted receivables transactions, and you post a batch of 100 transactions, a normal processing time of 30 seconds may be increased to 32 seconds. Again, the effect is usually not noticeable, but as the scale of auditing increases you may experience a slight degradation in performance.

Most administrative users of Auditor feel the slight performance hit offsets the value of the information being collected. Again, as mentioned above, it is recommended that you carefully choose what you want to audit and not simply “audit everything”. There is a performance cost for auditing in any audit system, and you may want to monitor certain audits to determine if their speed is acceptable. In general, performance degradation will not be an issue for most users of Auditor.

Audit Types

Auditor has three methods for tracking data changes in Dynamics GP: by Window, by Table and by SQL Table. The Window method is the easiest to use, while the Table and SQL Table methods are more technical in nature. Try auditing your system using the Window method first. If you cannot accomplish your auditing goals from the Window method, then try the Table or SQL Table method. At any time you can contact Rockton Software or your reseller for assistance.

The Window method allows you to “point and click” on different screens or windows in Dynamics GP. By using the Field Selection Wizard, you can simply open a window and click on the fields you wish to audit. Auditor will collect the technical information for you, and begin auditing your selections.

The Table method allows database administrators to monitor table operations in Dynamics GP. When a record is added, deleted, or modified, you can track who changed what on the record. An understanding of database structures in recommended for using this method.

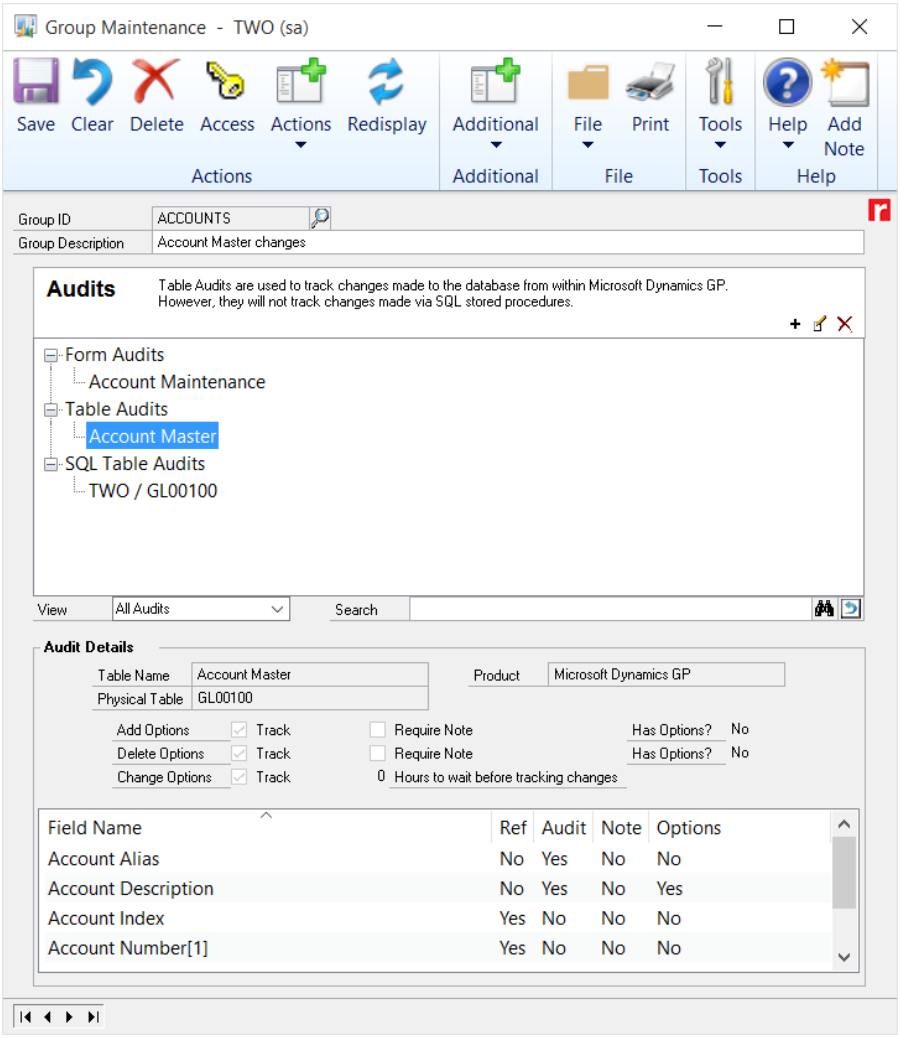
The SQL Table method also allows database administrators to monitor table operations in Dynamics GP. However, in addition to auditing Dynamics GP tables, you can also audit Inserts, Updates and Deletes that occur in any table in any database on the SQL Server instance where Dynamics GP and Auditor are currently installed.

All audits are tracked by a Record Key, which is usually the primary piece of information that tracks what has changed. For instance, if you are auditing employee information from the Payroll setup window, the Employee ID would be the Record Key. If the Employee Name changed, you would want to know for which employee the name changed, and that would be indicated by the Record Key. You can choose which fields to use for the Record Key when auditing fields on a window. However, for tables, the Record Key will always contain the fields in the table's Primary Key.

For Table and SQL Table Audits, you can optionally select additional “reference” fields to show on a particular Audit. For instance, when adding or deleting an Employee record you might want to display the Employee’s full name and Social Security Number. Any field in the table being audited can be selected as a Reference Field.

Group Maintenance window

The Group Maintenance window is the main window from which you set up audits.



This window can be accessed in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > Audit Groups.

Description

The Group Maintenance window is where you set up audits. Audits of similar function or access are collected in Audit Groups. For instance, you may want a Group for Payables, and another for Receivables. You can have an unlimited number of forms or tables in an Group. An Audit Group can be exported and sent to another site to be Imported here.

There are three Audit Types:

- **Form** audits are used to track changes as they are made on a Dynamics GP window.
- **Table** audits are used to track changes when they are saved to the database.

- **SQL Table** audits also track database changes, but unlike Table audits, they can apply to any table/database on the SQL server instance where Dynamics GP and Auditor are installed. This includes tables not related to Dynamics GP.

Some changes made from within Dynamics GP happen within a SQL stored procedure. Table audits cannot be used to track these types of database changes. If you need to track changes made by a stored procedure, use a SQL Table audit.

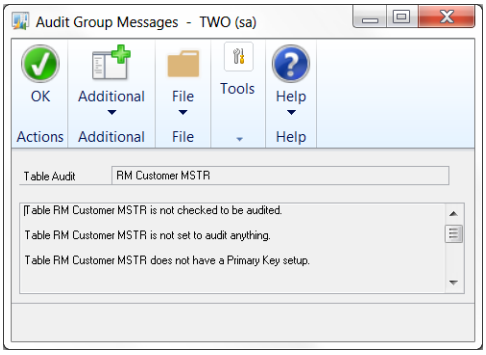
A given table or form can belong to only one Group. Therefore, how a form or table is audited can only be set up one way across all companies and users.

The Access button opens the Audit Group Access window. The Actions button has four items in its drop-list: the *Import Group* and *Export Group* options are described in the next section, **Exporting and Importing Audit Groups**; *Audit sa User* opens the Audit sa User window; *Reconcile* opens the same Auditor Reconcile window that you can access from the Auditor Setup window.

Using the Audits tree

The Audits tree at the top of the Group Maintenance window lists all audits for a given Group. The white box immediately above the tree gives you a little bit of information about the audit type that you are currently working with. The three buttons to the upper-right of the Audits tree, Add Audit +, Edit Audit , and Delete Audit , are used to set up the individual audits in a Group.

The **Add Audit** button opens a drop-list with the three different audit types (Form, Table and SQL Table). Choose the type of audit that you want to create and the lookup window for that audit type will open. After selecting a table or form, the maintenance window for that type will open and the audit will be added to the current Group. If you cancel off the maintenance window without completely setting up the audit, you will see that the audit is now listed in the Audits tree along with a warning icon ⚠. This indicates that this audit is not valid. If you click this warning icon, the Audit Group Messages window will open and show you the specifics of what is wrong with this audit.



The **Edit Audit** and **Delete Audit** buttons require you to first select an audit in the Audits tree. The Edit button is equivalent to double-clicking an audit in the tree.

You will notice, as you select individual audits in the Audits tree, that a couple of things happen. First, the description area at the top of the window changes to show you information about the audit type that you currently have selected. If you have selected an audit that you have set up in this group, then you will see the details of that audit's setup in the **Audit Details** area at the bottom of the Group Maintenance window.

The View drop-down allows you to see either All Audits in the currently selected group, or Only Audits with Errors. This second option is useful when you have a large number of audits in a group, and you don't want to scroll to find any that have problems.

Typing a value into the Search box and clicking the Search button (🔭) will display only the audits in the current group that contain the value that you typed. This is also useful when working with a very large audit group.

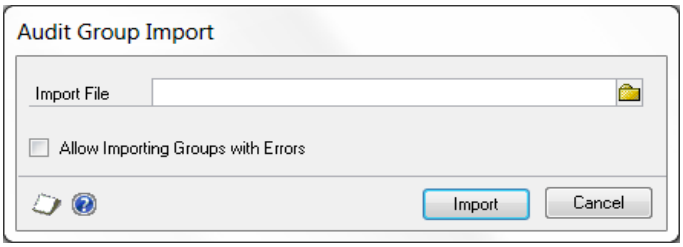
Exporting and Importing Audit Groups

The Actions Button's *Import Group* and *Export Group* options allow you to save Audit Groups that you have set up and then Import them later, even on another system.

To use the *Export Group* option, first enter or select an existing Audit Group on the Group Maintenance window. Choosing Export Group from the Actions button opens a dialog where you the location of the exported Audit Group. Then click the Save button. Your group is now exported.

It is recommended that you keep the file extension as ".auditor" because this will help you find the Audit Group later when you attempt to import it. The Import dialog looks for files of type ".auditor" by default.

The *Import Group* option opens the Audit Group Import window, below.



First, enter the Import File name and location. Or select it by clicking on the Path button to the right of the Import File field.

Next, decide if you want to import this group even if it has errors in it. This is sometimes useful in troubleshooting. If you do, then mark the Allow Importing Groups with Errors check box. Otherwise leave this option unmarked.

Now click the Import button. If the group you selected does contain errors, parts of that group may not be imported, depending upon if selected the Allow Importing Groups with Errors option. In either case, you will be given the option to view an error report. Of course, if there are no errors, then the Audit Group will be imported normally.

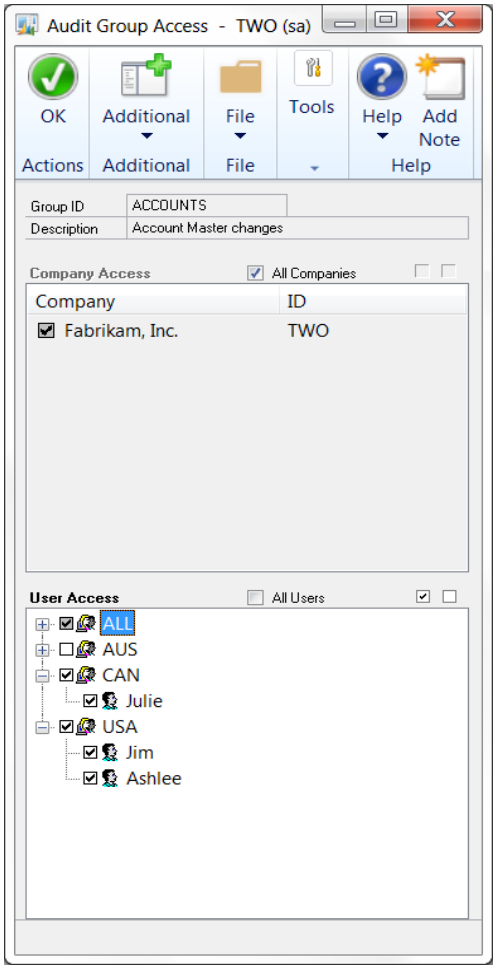
Specific User and Company selections are NOT imported or exported.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Group Maintenance window, but not make any changes to any of the audit definitions contained in any Audit Group. This is true even if the user is also in the POWERUSER or any other security role.

Two pre-configured Audit Groups are included with Auditor: AUDITOR SETUP and E-SIGN SETUP. These groups can optionally be imported if you want to audit any changes made to Auditor and E-Sign setups. Both of these groups use SQL Table audits.

Audit Group Access window

The Group Access window lets you select the Users and Companies to which an Audit Group applies.



You can access this window in one of two ways:

- First open the Group Maintenance window and select or enter a Group ID. Then choose the Access button.
- If you have marked the 'Open Access window with Group Maintenance window' option on the Auditor Options window, then this window will open automatically when you open the Group Maintenance window.

Description

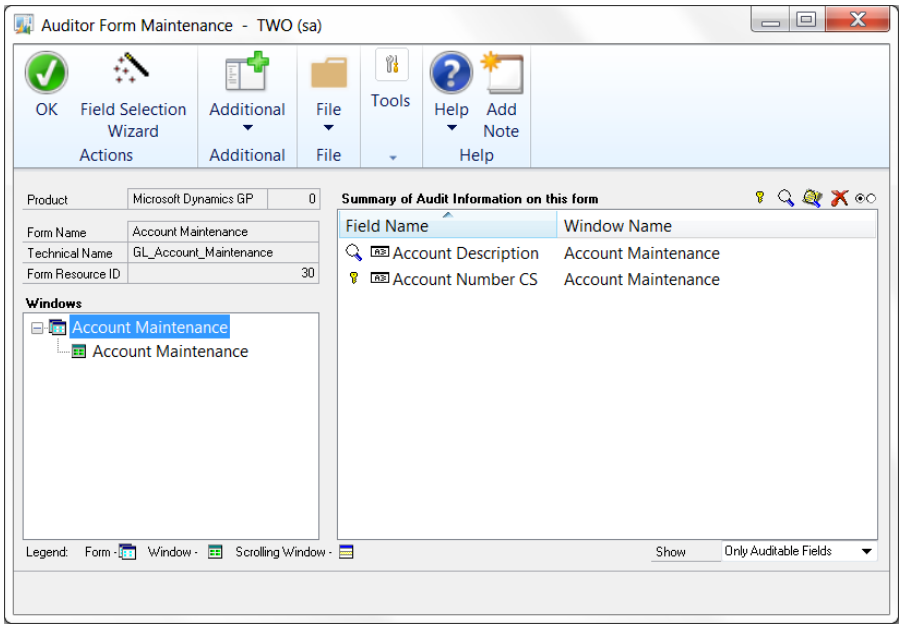
The Group Access feature limits audits in this Group to specific companies or users. By default, a new Group will work for all companies and all users.

The Company selection applies to Form and Table audits by default. To have this selection to apply to a SQL Table audit, check the Use Company Access box on the SQL Table Maintenance window for that SQL Table audit.

Specific User and Company selections are NOT imported or exported.

Auditor Form Maintenance window

The Auditor Form Maintenance window is where you can select the window fields that you want to audit, and how you want to audit them.



To get to this window, first open the Group Maintenance window. Then double-click one of the forms listed under the **Forms** node in the **Audits** tree.

Description

A Form is a "container" for windows, and often a form contains one window with the same name as the form. The Windows tree, on the left side of the window, will show the form name on the first line, followed by all of this form's windows. The Field List, on the right, shows the fields associated with what you have selected in the Windows tree.

Selecting the form name in the Windows tree will display all audited fields from all windows on this form on the right. Selecting a window on the left will display all fields on that window to the right, whether or not they are part of an audit.

To mark a field as a Key Field, Audit, or Audit with Note, select that field in the list and click the appropriate button at the upper-right of the list area. When you mark a field, an icon will appear next to that field designating its purpose.

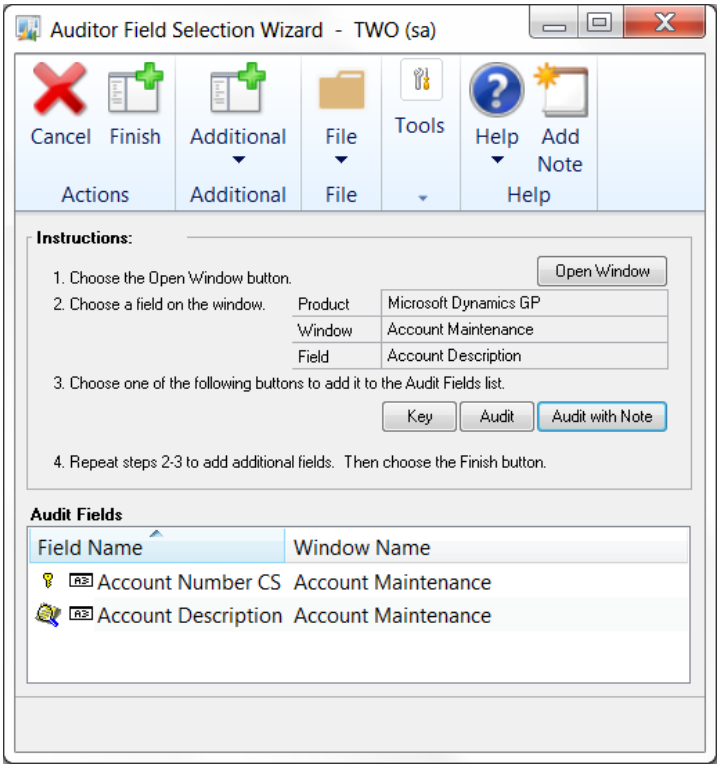
A field cannot be audited if it has been marked as a Key field.

The Show drop-down can be used to limit the list of fields that are shown in the field list. If Only Auditable Fields is selected, then you will be able to mark any field in the list using the process described above. However, there may be times that you wish to see all of the fields on a window, including those that are not available to be audited. To do that, choose All Fields from this drop-down.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Form Maintenance window, but not make any changes to any of the options presented here. This is true even if the user is also in the POWERUSER or any other security role.

Using the Field Selection Wizard

The easiest way to set up a Form audit is by using the Field Selection Wizard. Press this button to start the Wizard.



From the Field Selection Wizard window, press the Open Window button to open the window you are auditing. With this window open, click on a field that you want to audit. Notice that Product, Window and Field on the wizard window will change values to show the field that you have clicked.

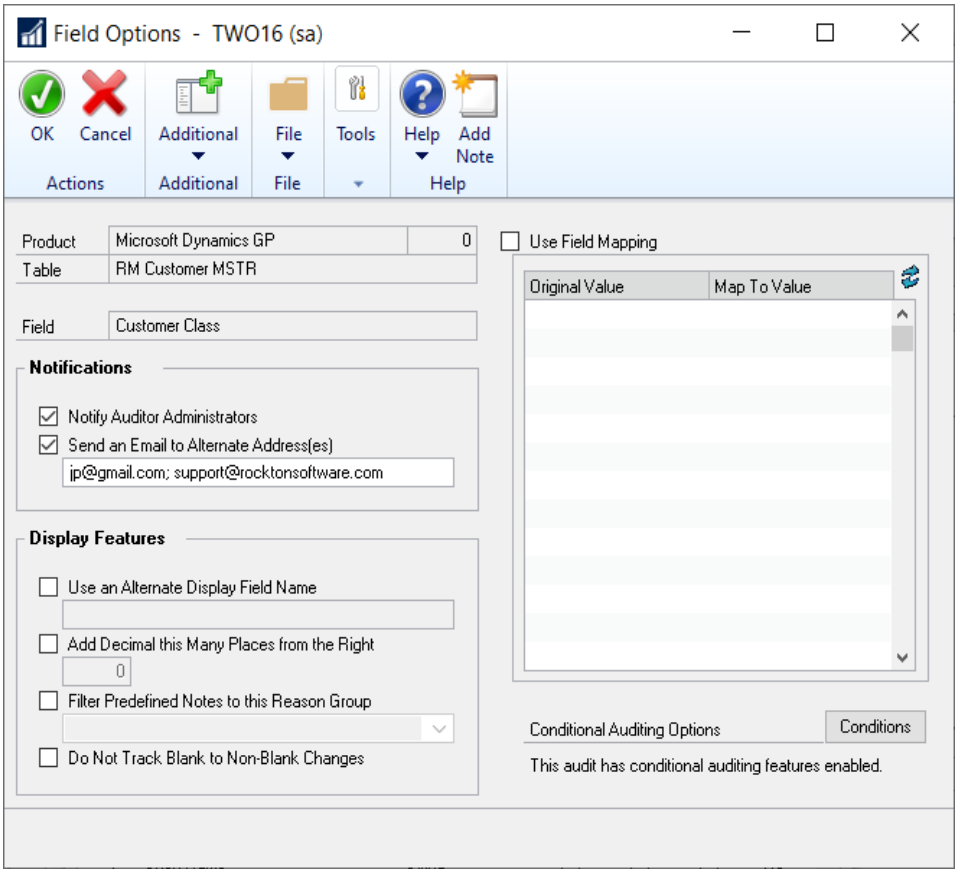
Now, press the Audit or Audit with Note button on the Auditor Field Selection Wizard window. You will see that this field is automatically added to the Audit Fields list. Continue this process until you have selected all of the fields that you want to audit.

Finally, select the fields that you want to be identified as Key fields in the same manner as you did the Audit Fields, but this time use the Key button.

When you are done, press the Finish button on the Wizard. This will close both the wizard window and the window that you originally opened with the Open Window button.

Field Options window

You can choose useful options for each field that you audit. Select a field in the list on the right, then press the Field Options button (◉○). The following window will appear:



You can access this window in one of these ways:

- From the Auditor Form Maintenance window, choose a field in the list box on the right, then click the Field Options button.
- From the Auditor Table Maintenance window, choose the Add Options button or the Delete Options button.
- From the Auditor Table Maintenance window, choose a field in the list box at the bottom, then click the Field Options button.

Description

You can choose useful options for each field that you audit. Options are found on the Auditor Form Maintenance window and the Auditor Table Maintenance window. In general, you will see a Field Options button (◉○) wherever options are available. They may pertain to a field in a list box, or to an audit type, such as Track Adds or Track Deletes.

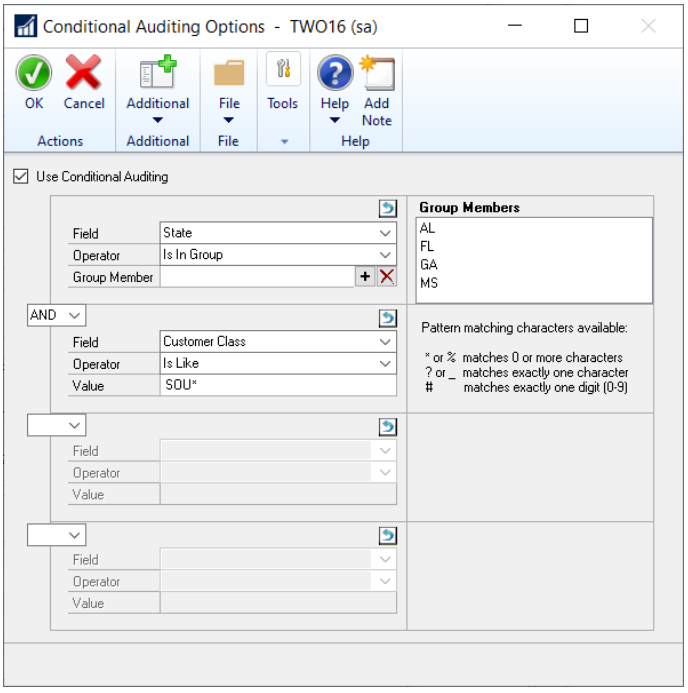
Options available for auditing are described below:

Option	Description
Notify the Auditor Administrators	Choose this option to send an email to each Auditor Administrator's email address (as specified in the System Setting setup window) or to update the Message Center.
Send an Email to Alternate Address(es)	Choose this option and specify email addresses, separated by semi-colons, to send a notification of an audit on this field.
Use an Alternate Display Field Name	You can specify a more useful name for a field than the system default to appear in the Audit Log. For instance, a field may be called "User Defined 1" and in your setup that field may track "Customer Status". You can specify the alternate field name here and the Audit Log will show the alternate name instead.
Add Decimal this Many Places from the Right	Dynamics GP tracks currency fields with misleading decimal places. For instance, $98.00 might be tracked as 9800 when audited. By putting a 2 in this field, the 9800 will be recorded as 98.00.
Filter Predefined Notes to this Reason Group	Once you have Reason Groups defined, you can assign a specific group to display in Note Entry for this audit field.
Do Not Track Blank to Non-Blank Changes	It is sometimes useless to audit a field that changes from blank to a valid value, which often occurs when entering data for the first time. Use this option to exclude audits of blank to non-blank values.
Use Field Mapping	It is often the case that lists, radio buttons, or checkboxes appear as numbers instead of useful descriptions. For instance, the Sales module has a SOP Type field that, when audited, appears as the numbers 1 through 5. You can map the value "1" to "Quote" and "2" to "Order", etc. so that the audit log reflects more useful data.
Use Conditional Auditing	Choose this button to make an audit conditional. The condition(s) you specify must be true for an audit to occur. See the Conditional Auditing section below for more information.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Field Options window, but not make any changes to any of the options presented here. This is true even if the user is also in the POWERUSER or any other security role.

Conditional Auditing

Choose the Conditions button to open the Conditional Auditing Options window.



To enable Conditional Auditing, mark the Use Conditional Auditing check box.

You will now be able to specify up to four conditions, joined by AND or OR, that will determine if this audit should be captured. For each condition, select the field that you want to compare to, the Operator, and the Value or Group Members for that Operator.

The Operators and their requirements are described below:

Operator	Additional Field to Enter	The audit will be captured if Field's value…
Is Equal To	Value	exactly matches Value.
Is Not Equal To	Value	does not exactly match Value.
Is Greater Than	Value	is greater than Value.
Is Not Greater Than	Value	is less than or equal to Value.
Is Less Than	Value	is less than Value.
Is Not Less Than	Value	is greater than or equal to Value.
Contains	Value	contains the exact characters, consecutively, specified in Value.
Does Not Contain	Value	does not contain the exact characters, consecutively, specified in Value.
Begins With	Value	starts with the exact characters, consecutively, specified in Value.
Is Like	Value	matches the pattern specified in Value (see below for pattern matching characters available).
Is Not Like	Value	does not match the pattern specified in Value (see below for pattern matching characters available).
Is In Group	Group Member(s)	exactly matches any of the items inserted into the Group Members box (see below for instructions on adding and removing Group Members).
Is Not In Group	Group Member(s)	does not exactly match any of the items inserted into the Group Members box (see below for instructions on adding and removing Group Members).

Pattern Matching Characters

The characters available to use in pattern matching are as follows:

* *(asterisk) or % (percent)* – matches 0 or more characters.

Examples:

- ABC*3 matches ABC3 (* matches 0 characters)
- ABC%3 matches ABCshh334093 (% matches shh33409)
- ABC%321 does not match ABCshh33409 (the string does not end in 321)

? (question mark) or _ (underscore) – matches exactly 1 character.

Examples:

- ABC?3 matches ABCD3 (? matches D, which is exactly 1 character)
- ABC_3 does not match ABCshh334093 (_ does not match because shh33409 is more than 1 character)

(pound sigh or hash symbol) – matches exactly 1 numeric digit.

Examples:

- ABC###3 matches ABC0123 (### matches 012)
- ABC##3 does not match ABC0123 (## does not match because 012 is 3 characters, and we only have 2 #s in the pattern)

Adding and Removing Group Members

If you choose either the Is In Group or Is Not In Group operator, you will somehow need to specify the members of the group to which you are comparing the selected Field. To do this, the Group Member field will be available for you to enter members into the group.

Add a new member to the group by typing a value in the Group Member field and then choosing the *Insert member into group* button (+) to the right of the Group Member field. You will now see that the member has been added to the list box at the right.

To remove a group member, first select (highlight) the member to remove in the Group Members list box at the right; then choose the *Remove member from group* button (✕) to the right of the Group Member field. The member will be removed from the group.

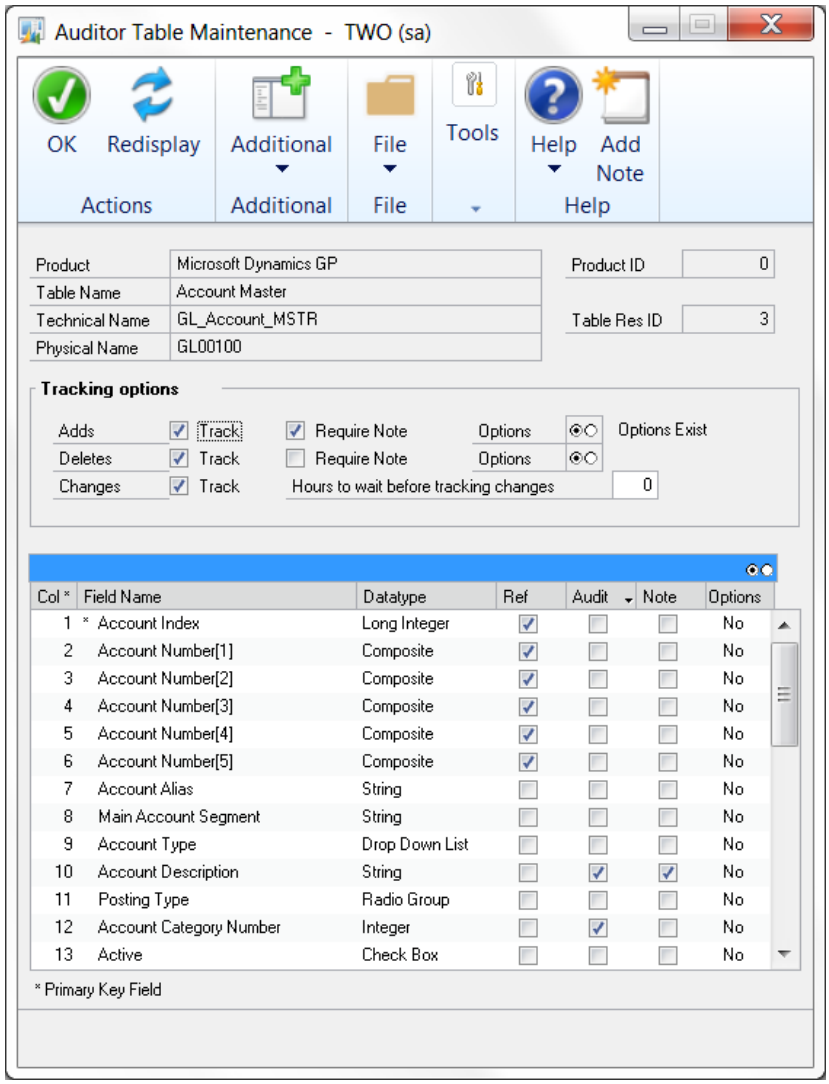
Other Buttons

If you want to clear an entire condition, choose the *Clear this condition* button ( ) located to the upper-right of the condition. You will be prompted to confirm. If you choose Yes, that entire condition and the associated AND/OR operator will be removed.

Once you are done editing the conditions on this window, be sure to press the OK button. This will ensure that your changes are saved.

Auditor Table Maintenance window

The Auditor Table Maintenance window is where you can select the table fields that you want to audit, and how you want to audit them.



To get to this window, first open the Group Maintenance window. Then double-click one of the tables listed under the **Tables** node in the **Audits** tree.

Description

You can select specific fields and/or table operations to audit. The field list can be sorted by clicking the column headings.

For each field selected, you may specify the same field options that are available for window fields. You can do this by focusing your cursor to the Field Name column of the field for which you want to specify Field Options, then clicking the Field Options button (⦿○) at the upper-right of the field list. This functionality is described in detail under Field Options in the Form Maintenance window section above.

If Field Options have been specified for a field on the table, the Options column will show "Yes" for that field. Otherwise, it will show "No".

For adds to or deletions from the table, you may require that the user enter a Note. In addition, you may specify the options described above by clicking the appropriate Options button in the **Tracking options** section of the window.

If Options have been specified for Adds or Deletes to the table, "Options Exist" will show to the right of the Options button.

For changes to the table, you may specify that the audit will only take place after a certain amount of time has elapsed.

These options are described in the tables below:

Option	Description
Track Adds	Check this option if you wish to audit when users add records to this table.
Track Deletes	Check this option to track deletions of records from this table.
Track Changes	Check this option to track specific field-level changes (which also must be selected in the field list below). You can also optionally choose to track changes only after a certain number of hours of adding a new record. This is useful in case you are not tracking new records, and it is likely that insignificant changes will be made in the first few hours of a new record being added.
Require Note	If Track Adds or Track Deletes is selected, you can require a Note to be entered for the user to explain why they added or deleted the record.
Options button	If Track Adds or Track Deletes is selected, you can specify options on that audit, such as emailing a notification or specifying conditions for when to audit. Pressing this button will open the same Field Options window that is used above in Form Maintenance. Keep in mind some options are not valid for additions and deletions of records.

The following options are available for each field in the field list:

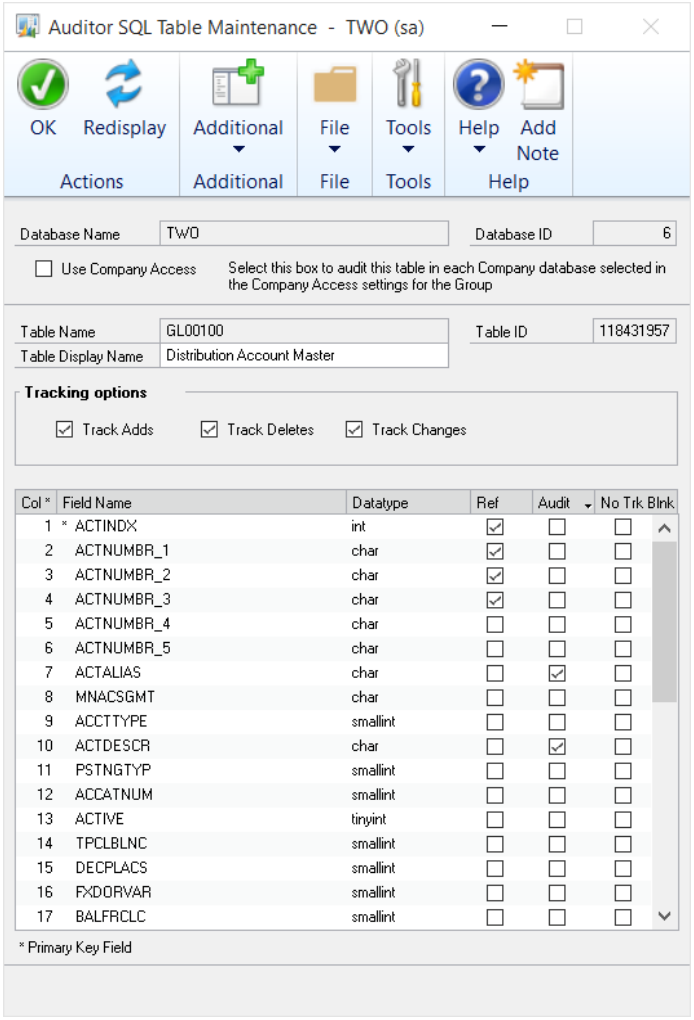
Option	Description
Ref	Use this column checkbox to mark "Reference Fields." Reference Fields are additional pieces of information that you want to see for each audit to help identify, or just provide more information about, the record being audited. These fields will show up in the Audit Log for Adds, Changes and Deletes. Note that all fields in a table's primary key will automatically be marked as Reference Fields.
Audit	Mark the fields for which you wish to track changes. Only the fields marked will be audited.
Note	When a field is audited, you can optionally check the Note checkbox to force a user to explain why a field was changed. Users are prompted with note entry after they modify a record if this box is checked. The user can close the note window, but they will be prompted repeatedly until they complete the notes.

When you have completed specifying what to audit, click the OK button. Auditor will now audit the tables and fields you have set up.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Auditor Table Maintenance window, but not make any changes to any of the options presented here. This is true even if the user is also in the POWERUSER or any other security role.

Auditor SQL Table Maintenance window

The Auditor SQL Table Maintenance window is where you can select the table fields that you want to audit, and how you want to audit them.



To get to this window, first open the Group Maintenance window. Then double-click one of the tables listed under the **SQL Tables** node in the **Audits** tree.

Description

SQL Table audits are similar to Table audits, but they differ in two very important ways:

1) SQL Table audits are not limited to database changes made from within Dynamics GP. If someone has run SQL scripts in SQL Server Management Studio, or if they have made database changes via some outside application, SQL Table audits will track these changes. Also, some changes in Dynamics GP happen as a result of SQL stored procedures. These changes cannot be tracked by Table audits, but they CAN be tracked by SQL Table audits.
2) SQL Table audits can be used to track any table on the same SQL Server instance as Dynamics GP, even if they have no relationship to Dynamics GP.

You can select specific fields and/or table operations to audit. You can also select whether or not you should audit if the user is changing a field from blank to some non-blank value. The field list can be sorted by clicking on the column headings.

The tracking options are described in the tables below:

Option	Description
Track Adds	Check this option if you wish to audit when users add records to this table.
Track Deletes	Check this option to track deletions of records from this table.
Track Changes	Check this option to track specific field-level changes (which also must be selected in the field list below).

The following options are available for each field in the field list:

Option	Description
Ref	Use this column checkbox to mark "Reference Fields." Reference Fields are additional pieces of information that you want to see for each audit to help identify, or just provide more information about, the record being audited. These fields will show up in the Audit Log for Adds, Changes and Deletes. Note that the fields in the table's Primary Key will always be Reference Fields.
Audit	Mark the fields for which you wish to track changes. Only the fields marked will be audited.
No Trk Blnk	It is sometimes useless to audit a field that changes from blank to a valid value, which often occurs when entering data for the first time. Use this option to exclude audits of blank to non-blank values.

When you have completed specifying what to audit, click the OK button. If everything is valid, Auditor will audit the tables and fields you have set up. Otherwise you will be given the option of seeing a report that shows any found errors for this SQL Table audit.

Use Company Access

Use Company Access should be checked if you want the company selections that you have made on the Audit Group Access window to apply to this SQL Table audit. By default, this box is unchecked, which means that the SQL Table audit will only apply to the specific database that you have selected.

Use Company Access will only be available for databases that are Dynamics GP company databases.

Using Company Access settings with a SQL Table audit can be tricky. As with Form and Table audits, you may only audit a given table in a given database one way. When you choose Use Company Access, that SQL Table audit now applies to each company database that has been selected on the Audit Group Access window. However, you *are allowed* to set up another SQL Table audit on this same table, as long as it is for a database that has not been selected in the original Group's Company Access.

For example, let's say you have created a Group called ACCOUNTS where you have a SQL Table audit defined on the GL00100 table. On this audit, you have selected Use Company Access. On the Audit Group Access window, you select All Companies. This means that you cannot create another SQL Table audit on the GL00100 table in this or any other Group, because this single audit definition applies to all company databases.

However, let's say that you uncheck All Companies on the Audit Group Access window, and you select company NORTH, company EAST, and company WEST, but you do not select company SOUTH. This means that the SQL Table audit that you have set up only

applies to the databases for the NORTH, EAST and WEST companies (because those are the ones selected in Company Access). You are now free to add a separate SQL Table audit for GL00100 in the SOUTH database, in this Group or any other Group, and this audit can have totally different characteristics than the original one has.

The rule of thumb with SQL Table audits is: you cannot audit a table more than once in the same database. To prevent you from doing this, Auditor adheres to these rules:

When checking Use Company Access on a SQL Table audit

- Look for another SQL Table audit for this table in this or any other group with Use Company Access unchecked. If one exists for a selected company in the current group's Company Access settings, you will not be allowed to check Use Company Access.

When adding a new SQL Table audit

- See if there is already another SQL Table audit for this table in this or any other Group with Use Company Access checked. If one exists, and that Group's Company Access settings include the company database for which you are trying to add the new SQL Table audit, then you will not be allowed to add this audit.

When changing a Group's Company Access settings

See the section on the Audit Group Access window for more information about changing access settings for a Group.

- When checking All Companies, look at each SQL Table audit in this Group to see if any audits that have Use Company Access checked also exist individually (i.e. with Use Company Access unchecked) in any Group. If any are found, then you will not be allowed to check All Companies.
- When selecting a single company, look at each SQL Table audit in this Group to see if any audits that have Use Company Access checked exist individually (i.e. with Use Company Access unchecked) *for the company you are selecting* in any Group. If any are found, then you will not be allowed to select this company.

Required Permissions to Create SQL Table Audits

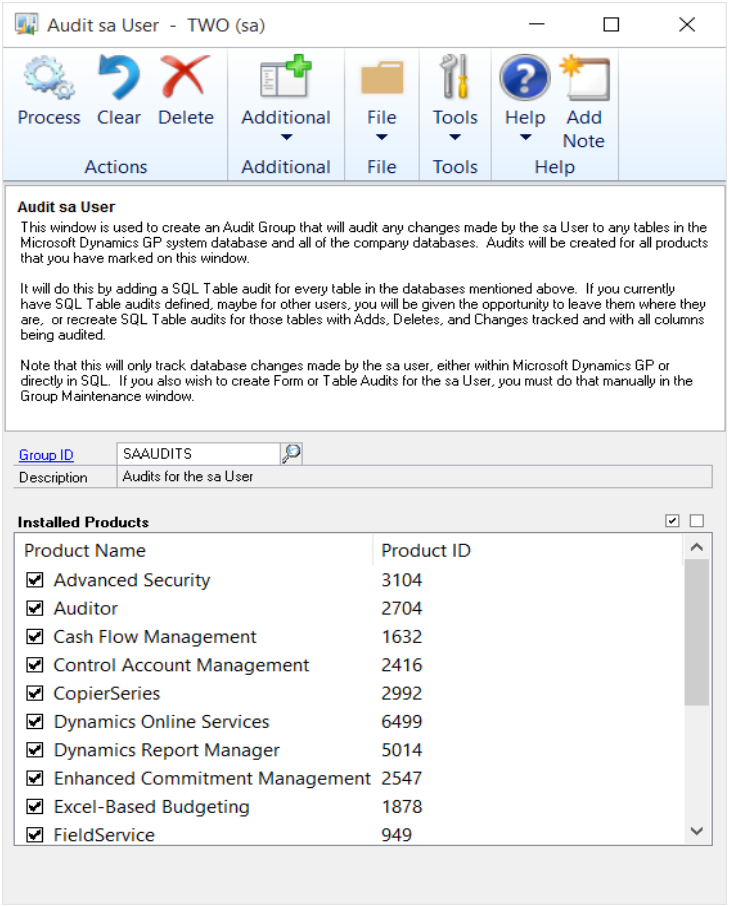
Your User ID must have sufficient rights to create database triggers on the SQL Server in order to complete the setup of a SQL Table audit. This means that the User must be in the 'sysadmin' fixed server role or it must be in the 'db_owner' role for the database on which you are attempting to create the SQL Table audit.

If you do not have sufficient rights to create the SQL trigger, then only the setup information will be saved (i.e. audits will not be logged). To complete the SQL Table audit setup, log in as a User with the previously described rights and run the 'Rebuild SQL Triggers' process from the Auditor Setup window.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Auditor SQL Table Maintenance window, but not make any changes to any of the options presented here. This is true even if the user is also in the POWERUSER or any other security role.

Audit sa User window

The Audit sa User window is used to create an Audit Group that will audit all Dynamics GP database changes made by the sa user.



To get to this window, first open the Group Maintenance window. Then, from the Actions button, choose Audit sa User.

Description

This window can be used to easily create an Audit Group that contains SQL Table audits for every table in any Dynamics GP database. Each audit will track Adds, Deletes, and Changes to each table audited; for Changes, each auditable field will be tracked. This can be useful if you want to audit what the system administrator (specifically, the SQL sa User) is doing in your accounting system.

*While this process creates a normal Audit Group that can be maintained on the Group Maintenance window, we **strongly recommend** that you do not assign access to any user other than the SQL system administrator user, sa. Auditing every table will certainly have a significant negative impact on performance in Dynamics GP. Since this user does not typically need to perform accounting functions within the system, this should not be a problem for most companies. However, a typical user of Dynamics GP may find the system essentially unusable if they are included in this Audit Group.*

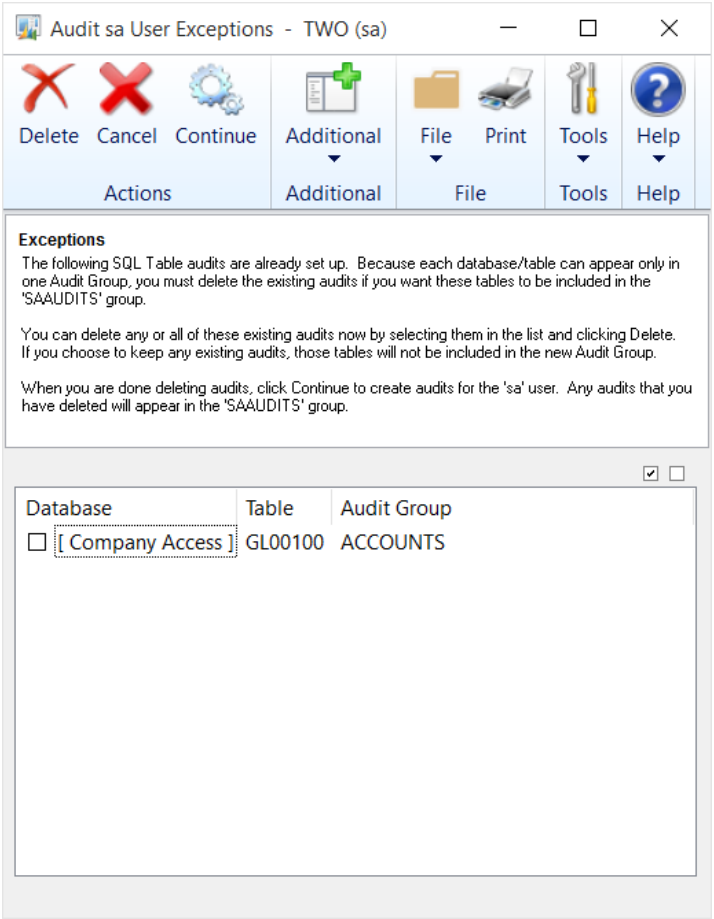
Creating the Audit Group

To create the group, first enter or select an Audit Group ID that will contain the SQL Table audits. If you select an existing group, all of its contents will be deleted. Therefore, this is only recommended if you are rebuilding a group that was previously created by this process, or if you simply want to delete the contents of the group you have selected and want to reuse it. For convenience, a Delete button is provided so that you can clear a group from this window.

Next, review the Installed Products list box. This contains all of the products that you currently have installed on this computer. The purpose of the list is to select the products whose tables you want to be audited. Typically, we recommend that you keep all products selected. However there may be some products that are not of as much concern to you from a security standpoint. If that is the case, you may wish to unmark those products to cut down on the processing time for this procedure, and to make the resulting Audit Group smaller and easier to work with.

Finally, to start building the group, choose the Process button. The system will verify that the group you have selected is empty. If it is not, you will be prompted to either: a) delete the group and continue, or b) cancel the process to select another group.

The next step in this process is to verify that there are no SQL Table audits set up in any other groups for any of the selected products. The reason for this is that you cannot have the same table audited two different ways in two different groups. To prevent this sort of conflict, you will be presented with the Audit sa User Exceptions window if any existing SQL Table audits are found:



To remove any of the existing SQL Table audits and have them recreated in the new group, simply select them and choose the Delete button. This will remove only those SQL Table audits from the Audit Groups that are listed on this window. No other audits will be affected. Also, no Table or Form audits will ever be removed.

However, you may wish to keep a SQL Table audit in the group where it currently resides if it was created for Users other than sa, or if you have options specified that are different than the default options described below in the **SQL Table Audit options** section. For instance, you may want to only audit certain fields on one table, rather than all fields. Or, you may want to use the No Track Blank option on some fields. Since this process will only create SQL Table audits as described below, you may want to keep those audits in their current groups and not recreate them in the new group.

If you wish to keep any of your existing SQL Table audits with the settings that they currently have, simply do not delete them on this window. When you are done deleting the audits that you do want to be a part of this group, click the Continue button and anything still listed on this window will be excluded from the new group.

You should carefully review any SQL Table audits that you choose to exclude from this process. The reason is that you may not be auditing all fields on these tables, and the 'sa' user may not even be audited by the group that contains your existing audits.

Building the new Audit Group will commence either when you click the Continue button on the Audit sa User Exceptions window or when you click Process on the Audit sa User window if no exceptions were found. Please note that this process will likely take a considerable amount of time, and that time will be extended depending upon how many Dynamics GP company databases you have.

SQL Table Audit options

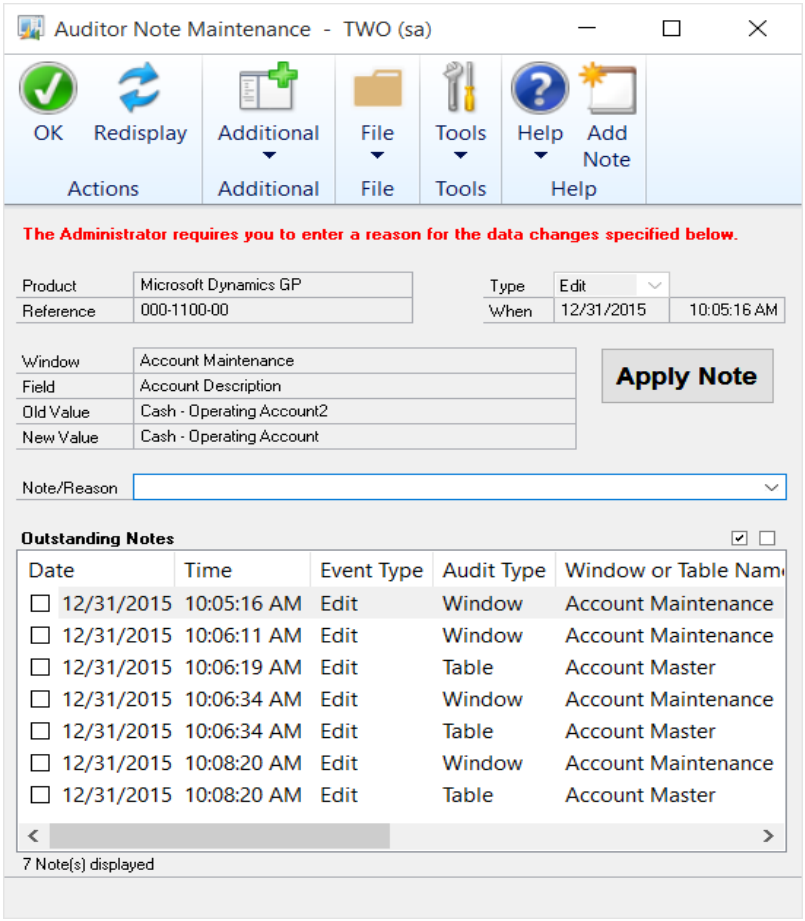
The SQL Table audits created for each table will have Track Adds and Track Deletes checked. In addition, if there are any auditable fields on the table, then they will be selected under the Audits column and Track Changes will be marked as well. Auditable fields are any fields that have a datatype that is not text, ntext, or image.

Each table will end up with two or three SQL triggers: 1) an INSERT trigger, 2) a DELETE trigger, and 3) an UPDATE trigger if there are any auditable fields on that table.

If a user is in the AUDITOR AUDITORS security role, they will not have access to the Audit sa User window. This is true even if the user is also in the POWERUSER or any other security role.

Auditor Note Maintenance window

The Auditor Note Maintenance window is where the User enters the reason for making any change in the system that has been set up to require a note.



This window is accessible in one of these ways:

- Go to Microsoft Dynamics GP > Tools > Setup > Auditor > Note Maintenance.
- This window will also open automatically whenever the User makes a change to a field that has been set to Audit w/ Note. See the descriptions of the Auditor Form Maintenance and Auditor Table Maintenance windows, discussed previously in this document, for more information about how to set up this type of audit.

Description

If you set up an audit and require a note, upon logging that audit the Auditor Note Maintenance window will appear. It will specify the details of the change, and instruct the user, in **red, bold text**, to enter the reason that they made the change.

The user can enter a Note (reason for the change) by typing in freeform text into the Note/Reason field and then clicking the Apply Note button and choosing “to displayed change” from the button drop list. If a Reason Group was specified in Field Options on the audit definition, they can also choose a predefined note from the drop-down list.

There is a System Settings option that will optionally require the user to pick an item from the list rather than allowing them to type in their own reason. See the section on the Auditor Options window for more.

Using the Outstanding Notes list

You will notice that there is a list box labeled, Outstanding Notes. There are two reasons that audits will be listed here: 1) the action you just took resulted in multiple audits that required notes, or 2) you had clicked OK when this window had been previously displayed, but you did not complete Note entry for all of the audits that required notes at that time.

As an example of the first case, you may have audits set up on both the Customer Name field and the Short Name field on the Customer Master table, and both of these audits are set up to require a note from the user. If a user changes both of these fields and clicks the Save button, two audits will be written at that time, both requiring reasons for making those changes. The user will then see those two audits listed in the Outstanding Notes list.

For the second case, there may be situations where a User does not have all of the information they need to be able to enter a valid reason on the Auditor Note Maintenance window. In these cases, it is possible for users to press OK and not enter a note or reason as required. The next time that user makes a change that requires a note, these previous, incomplete audits will be listed in the Outstanding Notes list along with the current audit that requires a note.

There is a System Settings option that will optionally force the user to enter all outstanding notes before they can exit the Auditor Note Maintenance window. See the section on the Auditor Options window for more.

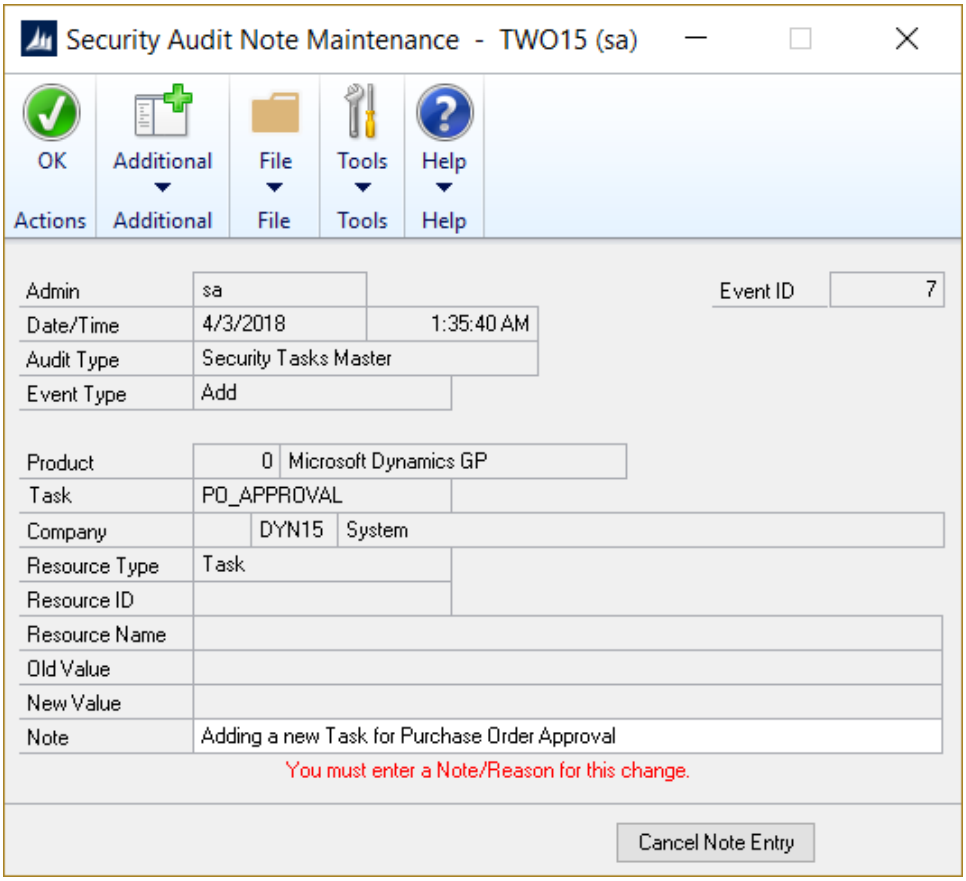
In addition, Auditor has a “nag” feature which will continually present the Auditor Note Maintenance window to the User each time they log into Dynamics GP. Ultimately, it will behoove the User to enter notes as soon as possible so they do not have too many incomplete noted audits.

As you click on the audits in the list, you will see that they details for that audit are displayed in the top portion of the Auditor Note Maintenance window. If you enter or select a Note/Reason and then click the Apply Note button and choose “to displayed change” from the button drop list, that note will be applied to the selected (displayed) audit.

However, you can also select multiple audits in the list by checking the box to the left of each line. You can also use the Mark All or Unmark All buttons at the upper-right of the list. This will then allow you to choose “to all changes marked below” from the Apply Note button’s drop-list and the Note/Reason entered will be applied to all marked audits.

Security Audit Note Maintenance window

This window is where the User enters the reason for making any Security change in the system that has been set up to require a note.



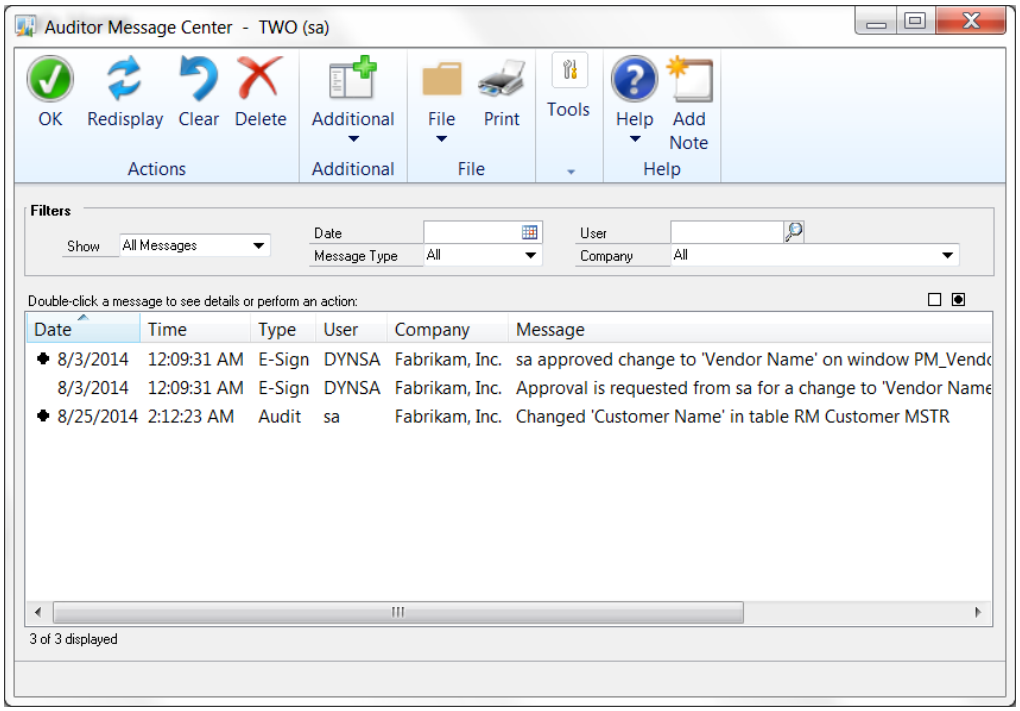
This window will open automatically whenever the User makes a Security change that has been set to require a Note. See the section on the Auditor Options window for more information about requiring Notes.

Description

If you choose to audit a security setting that requires a note, upon logging that audit the Audit Inquiry window will appear and allow you to enter the Note. It will specify the details of the audit that occurred. This screen will prompt once for each audit that needs a note until Note Entry is complete. This screen can also be accessed from Smartlist by double-clicking on an audit.

Auditor Message Center window

The Auditor Message Center window is where Auditor Administrators and E-Sign Approvers are notified about system events.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > Message Center.

Description

The Auditor Message Center shows all of the events about which an Auditor Administrator or E-Sign Approver has chosen to be notified. Messages listed can be sorted by any column by clicking on the column heading. You can also limit which messages are displayed by selecting one of the Filters at the top of the window. If you change one or more of the Filters, then you will need to press the Redisplay button to refresh the list.

The Date and Time fields indicate when then event referred to in the message occurred.

The Type field is the Message Type. It can have one of the following values: Audit, E-Sign, Registration or Log.

User indicates the User that took the action that caused this notification to be sent.

Company shows the name of the Company in which the action took place. Company only applies to Audit and E-Sign messages since the other types are system-level events, not Company-specific ones.

The status area appears below the list. On the left you will see the number of messages that exist and that are currently displayed. On the right you may see a message indicating that you need to refresh the list to see all messages available. This will happen if you change any of the Filters at the top of the window. In the screen shot

above, the Message Type Filter has been changed to Audit, so you see a message indicating that you need to press the Redisplay button to refresh the list. You will see a similar message when you first open the Message Center window.

You can see more information or take action on a particular message by double-clicking it. The action taken when you double-click depends upon the Message Type:

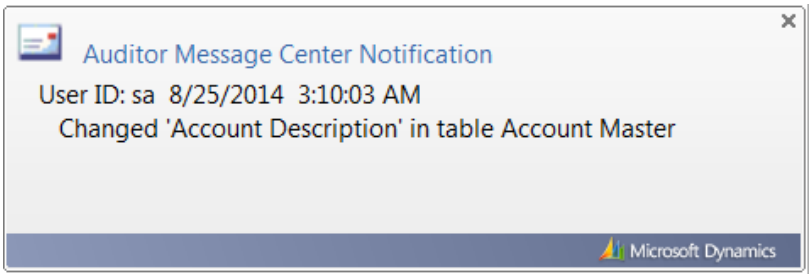
Message Type	Action
Audit	Opens the Audit Inquiry window, where you can see details about the Audit selected.
E-Sign	Opens the Approval Inquiry window, where you can see details about a completed Approval. Additionally, you can also approve or deny a Pending Approval, if you are the Approver.
Log	Opens the Auditor Table Archive/Purge window where you can archive and purge the Audit Log and E-Sign Approval Log.
Registration	Opens the Auditor Registration window where you can enter or review the Registration Keys for Auditor.

Messages that have not yet been read (by double-clicking them) will have a dot (●) to the left of the Date column. This is only for your reference and to give you the ability to filter by Read or Unread Messages. You can also mark a group of messages as read or unread by clicking the Mark buttons (☐ ◉) at the upper-right of the message list. A group of messages can be deleted by clicking the Delete button (✕) at the upper-right of the message list.

Print a report of the messages displayed by clicking the Print button (). The report generated will use whatever filters you have selected in the Message Center window.

Notification Box

By default, when a new message arrives in the Message Center for a particular Auditor Administrator, if that admin is logged in at the time the message arrives they will see a Notification Box similar to this one appear in the lower-right corner of the window:



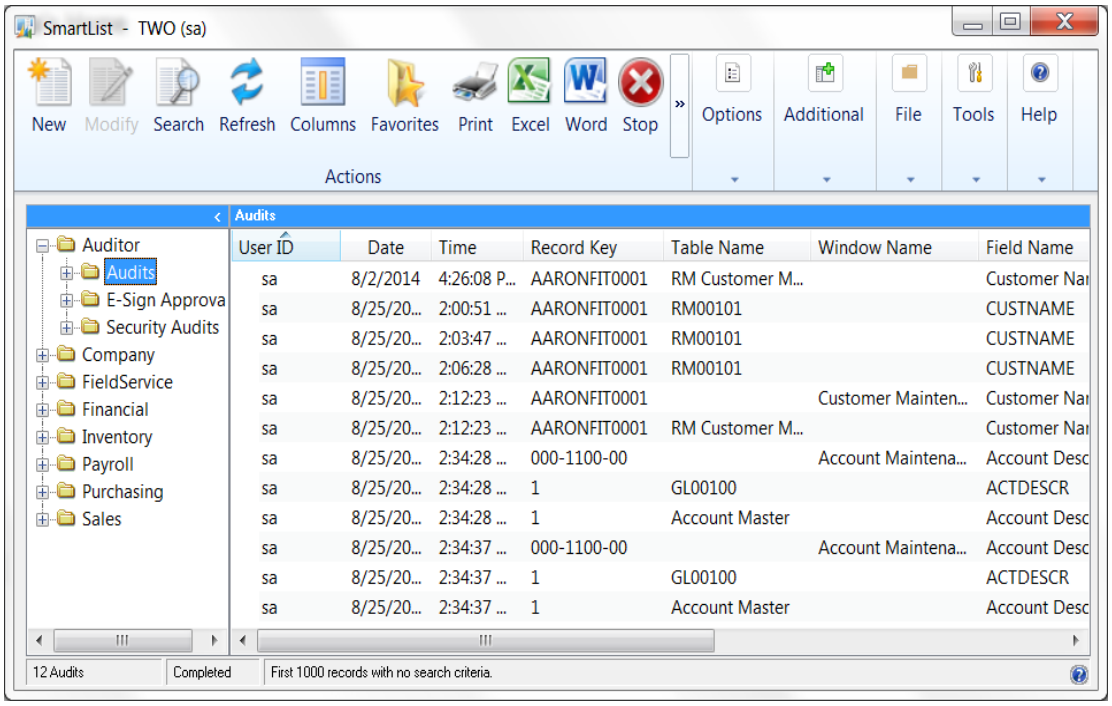
If there is User activity, then this Notification Box will remain for 15 seconds. If there is no activity at the time, then it will remain displayed until the user performs some action.

If the Auditor Administrator clicks on this Notification Box, the appropriate window will open depending upon the Action or Event that is described in the notification. See the table above for details of what action will be taken for each Message Type.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Auditor Message Center window, but not make any changes to any of the messages presented here. This is true even if the user is also in the POWERUSER or any other security role.

Inquiry

Audit Reporting using Smartlist



To get to this window, go to Microsoft Dynamics GP > Smartlist, or press the Smartlist icon ( ) on the Microsoft Dynamics GP toolbar.

Description

All audits are tracked in the system database and can be reported on using Smartlist. Smartlist is the only built-in way of directly viewing audits. Using Smartlist's features, you can filter and sort your audits and export them to Word or Excel for further evaluation. You can also double-click on an audit and the Audit Inquiry window will open giving you details about that audit event. The Audits, E-Sign Approvals, and Security Audits objects appear automatically in Smartlist after Auditor is installed.

If a user is not assigned to the AUDITOR ADMIN or AUDITOR AUDITORS security roles, then they will not be able to make some changes to Auditor favorites in Smartlist. This is so that they will not be allowed to see any data other than what they were allowed to see when the favorite was originally set up. Specifically, these users:

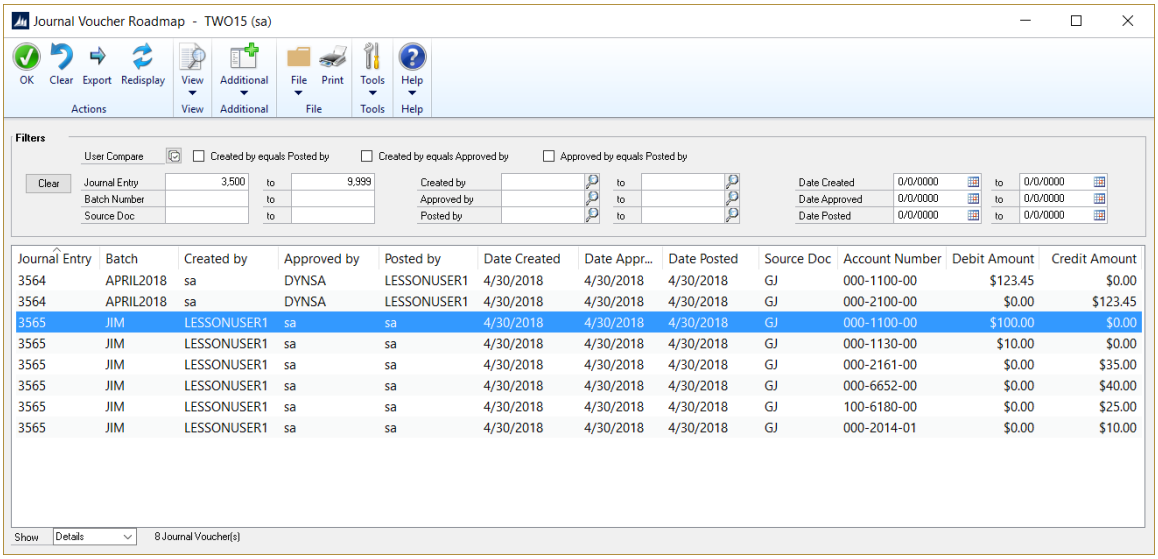
- can't make changes to existing Search criteria; they can add new searches
- can't add Columns to a Search other than the ones they are allowed to add – in other words, they can choose the Columns button, but they cannot choose Add to add any other columns to the list
- can't choose the Clear All button because that would clear existing criteria

For more technical reporting of audits, you can access these tables directly in SQL by querying the DYNAMICS database for the following:

Audit Type	Database tables
Audits	RSAS015 and RSAS031
E-Sign Approvals	RSAS039 and RSAS044
Security Audits	RSAS045

Journal Voucher Roadmap window

The Journal Voucher Roadmap window shows posted Journal Entries along with the history of who created, approved, and posted them along with the date that these events occurred.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Go to Microsoft Dynamics GP > Tools > Inquiry > Auditor > Journal Voucher Roadmap.

Description

This window gives you a way to track GL Journal Vouchers from the point where they are originally entered thru approval and up to posting. It shows the person who performed each of these steps as well as the time these steps were performed.

You can limit the number of records shown by using the Filters section at the top of the window. Enter values for any or all of the “from” and “to” ranges. Use the User Compare check boxes to see all transactions where the same user created and posted, or created and approved, or posted and approved them. The User Compare filters have Mark All ( ) and Unmark All ( ) buttons to aid in quickly making these selections. You can clear all of your filter selections by clicking the Clear button located to the left of the filter ranges.

After entering your filters, choose the Redisplay button to see the results based on your selections. You will need to click Redisplay to see results any time you make changes to the Doc Statuses, Transaction Types, or Filters.

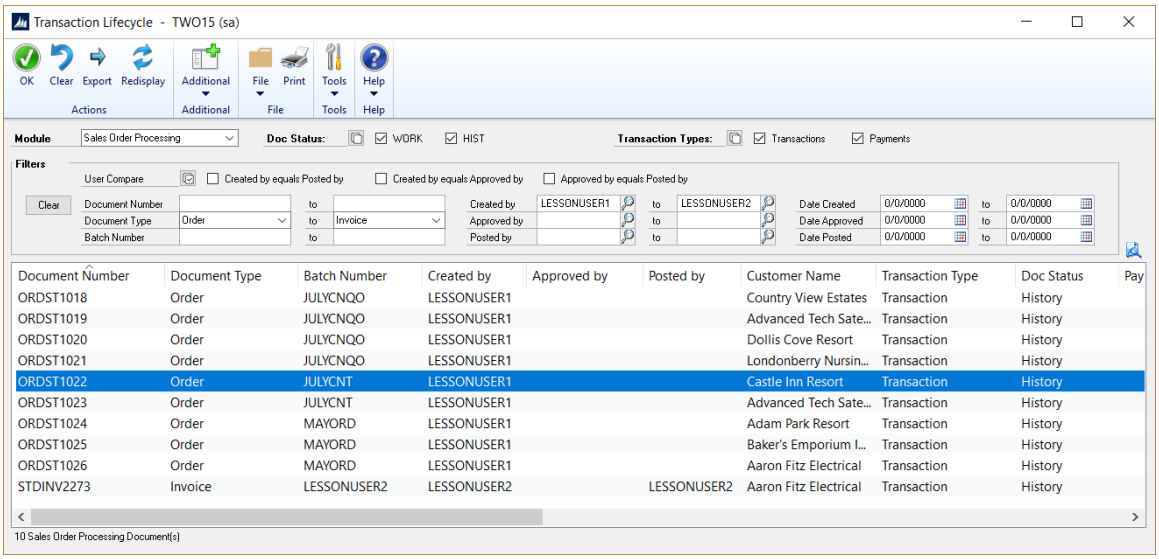
You can zoom on a line to get more information by double-clicking that line.

To see details for each journal entry, choose Details in the Show drop-down at the lower-left. If you want to just see one line per journal voucher, choose Summary. In Summary view, you will not see the Account Number, Debit Amount, or Credit Amounts.

If you want to export the results shows to a CSV file, click the Export button in the ribbon. If you need a report of these results, click the Print button in the ribbon. Either of these options will output whatever is currently listed, including the selected filters.

Transaction Lifecycle window

This window shows who created, approved, and posted transactions in PM, RM, POP, and SOP.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Go to Microsoft Dynamics GP > Tools > Inquiry > Auditor > Transaction Lifecycle.

Description

The Transaction Lifecycle window shows who has created, approved, and posted transactions in any of the following modules:

- Sales Order Processing
- Purchase Order Processing
- Receivables Management
- Payables Management

To use this window, first select the desired Module. The Doc Status and Transaction Type check boxes that appear will pertain to the module that you selected. Initially, they will all be marked, but you can unmark the ones that you do not wish to see. Next, enter any Filters to specify which transactions you are interested in. Finally, click the Redisplay button to show the requested data.

The Doc Status check boxes let you see work, open, and/or historical transactions. You may also choose the transaction types you wish to see by marking any of the Transaction Type boxes. Each of these options has Mark All (☑) and Unmark All (☐) buttons to aid in quickly making these selections.

You can limit the records shown by using the Filters section at the top of the window. Enter any or all of the “from” and “to” ranges. User Compare filters show all transactions where the same user created and posted, or created and approved, or posted and approved them. User Compare filters also have Mark All and Unmark All buttons. Click the Clear button, located to the left of the filter ranges, to clear all your filter selections.

After entering your filters, click Redisplay to see results based on your selections. You will need to click Redisplay to see results any time you make changes to the Doc Statuses, Transaction Types, or Filters.

You can zoom on a line to get more information by double-clicking it. You will also be able to select certain transactions and choose the View in Journal Voucher Roadmap button ( ) to see the journal entries associated with that transaction. See the section on the Journal Voucher Roadmap window for more information on using that window.

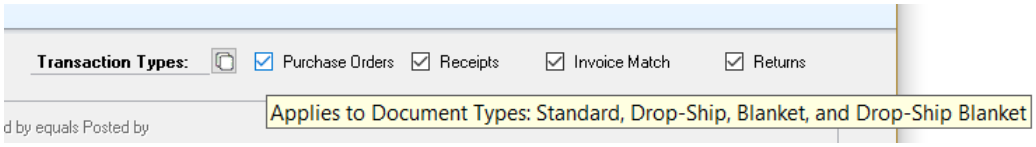
If you want to export the results shows to a CSV file, click the Export button in the ribbon. If you need a report of these results, click the Print button in the ribbon. Either of these options will output whatever is currently listed, including the selected filters.

Filtering on Document Type

When using the Document Type filter, you may notice, in some cases, that the drop-down contains many more items than you would normally see in Dynamics GP. For some modules, you will be able to see certain Document Types for one Transaction Type, but then a different group of doc types for another Transaction Type. All of these options will show in the drop-down list for the Document Type filters so that you can select ranges for any of the possible records that might be displayed. Just be aware that if you choose a range that pertains only to one Transaction Type, then no records from any other Transaction Type will be displayed.

For instance, in the Purchase Order Processing module, the only doc types that apply to Purchase Orders are Standard, Drop-Ship, Blanket, and Drop-Ship Blanket. However, you can choose to see Purchase Orders, Receipts, Invoice Matches, and Returns all listed together if you have all the Transaction Types marked. If you then choose Standard as your From Document Type and Drop-Ship Blanket as your To Document Type and click Redisplay, the only records that will be displayed will be Purchase Orders, even though you have the other Transaction Types marked. This is because you have chosen to filter doc types that only apply to Purchase Orders.

To make this a little bit clearer, each of the Transaction Type check boxes contain tooltips that show which Document Types apply to each Transaction Type. Simply hover over a Transaction Type check box to see a list of the doc types that apply.



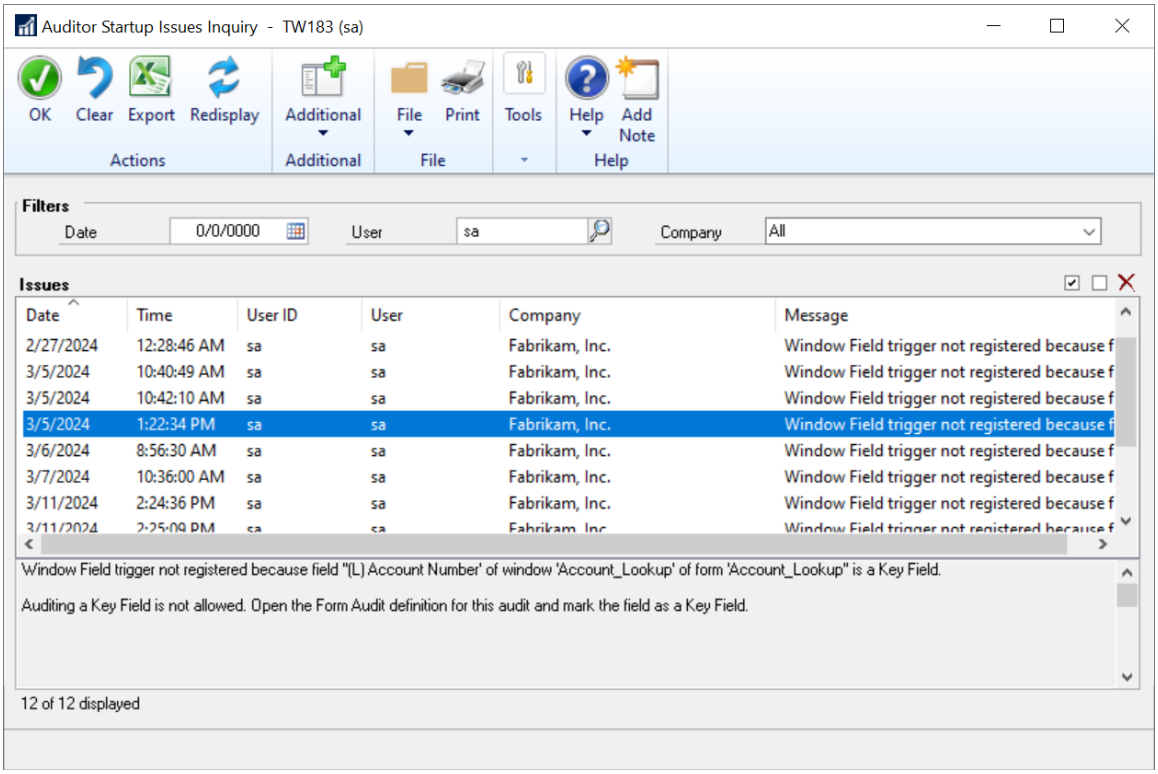
As another example, let's say that you choose Blanket as your From Document Type and Invoice as your To Document Type. This will result in the following doc types being displayed when you click Redisplay:

- Blanket
- Drop-Ship Blanket
- Shipment
- Invoice

The doc types in the range you select are determined by the order that they appear in the range's drop-down list. To add one other point, suppose you did not mark the Purchase Orders Transaction Type check box. In that case, you would only see transactions with doc types of Shipment and Invoice, even though you selected a Purchase Order doc type as the To Document Type in your filter.

Audit Startup Issues Inquiry

This window lists problems that have occurred while initializing Auditor.



This window is accessible in one of these ways:

- Go to Inquiry > Auditor > Auditor Startup Issues Inquiry.
- By double-clicking a startup message on the Auditor Message Center window.

Description

This window shows any Auditor issues that may be encountered when a user logs in to Dynamics GP. The most common issues would be with initializing Form or Table audits. Since problems of this type would prevent these audits from being recorded, we log them when they occur and notify Auditor Administrators who have an Audit Notify Option marked on the Auditor System Settings window. Note that SQL Table audits will not be checked during Auditor's initialization because there is no initialization process for these audits. In addition, if the system cannot properly check if Auditor is registered, a message will be logged as well. You can see all of these message types on this window.

When you select an item in the list, the full text of the message will be shown in the box at the bottom of the window. You will also see a suggestion of the recommended action to take when this message occurs.

You may export the message listed on the window by clicking the Export button in the ribbon. If you wish to delete messages from this window, select one or more message, then click the Delete Message(s) button ( ).

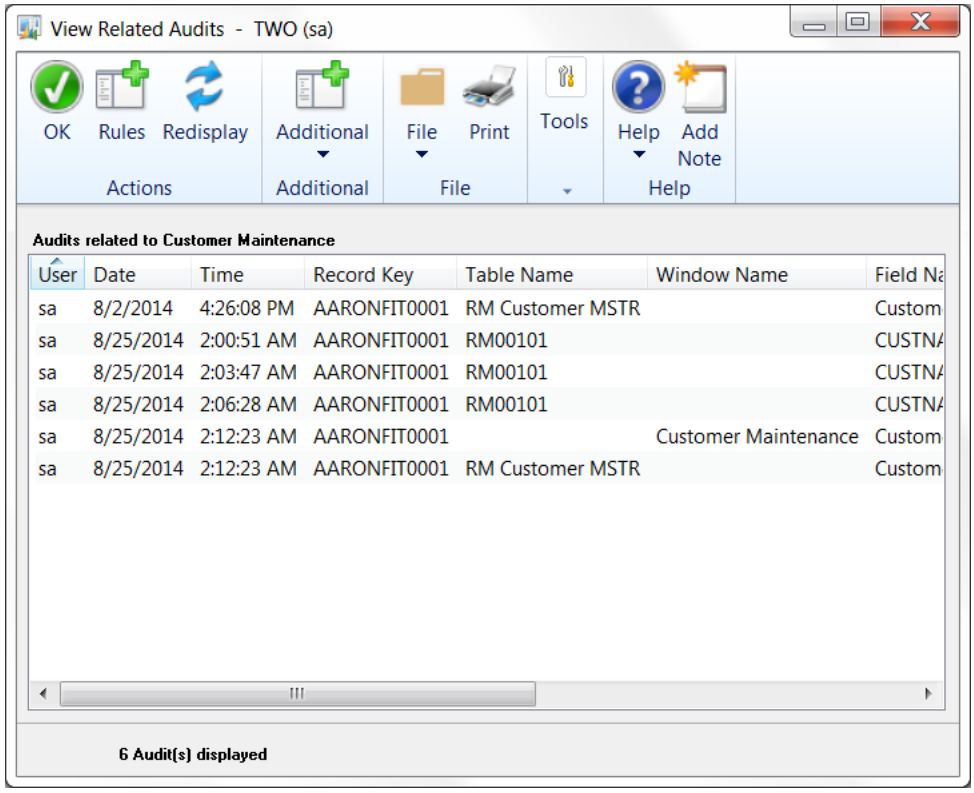
View Related Audits

The Related Audits feature allows you to see audits that have been captured for what is displayed on the window that you are currently viewing. This is enabled by defining one or more rules that specify which audits you want to see for a given window.

Several of the most used entities in the system will be enabled for you automatically. However, because we have used a flexible, rule-based setup, you can to turn on this functionality for virtually any window in Dynamics GP.

View Related Audits window

This window lists all Audits related to whatever is displayed on the window you are viewing.



This window is accessed from the View Related Audits option on the Additional menu of almost any window in Dynamics GP.

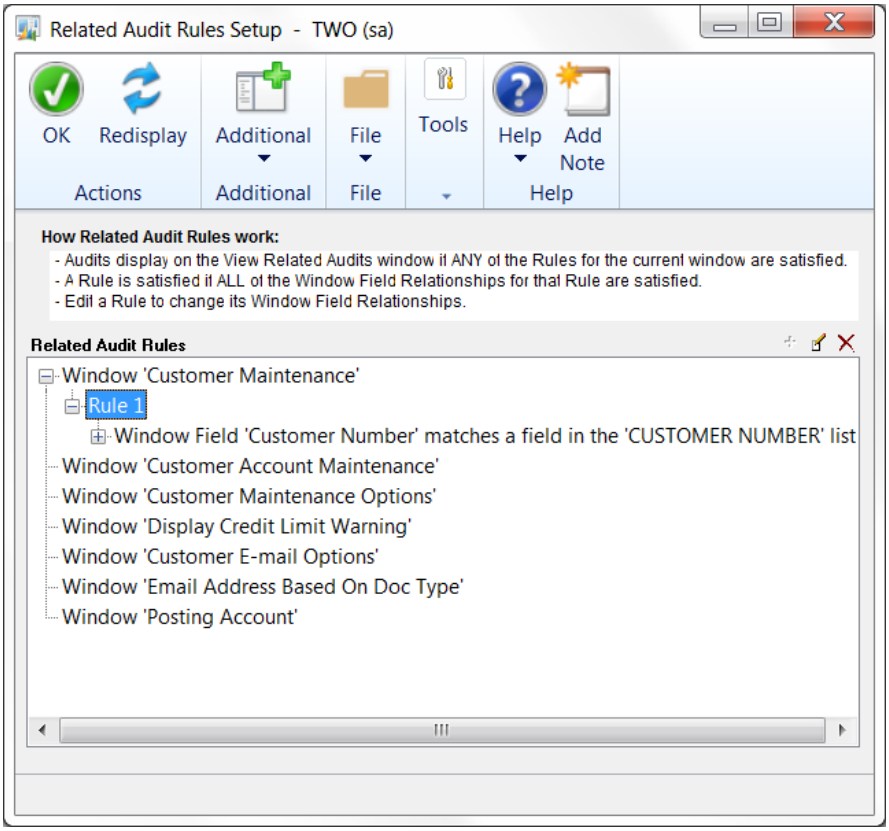
Description

To view Related Audits for a given window, simply choose the View Related Audits item from the Additional menu on that window. You can click the Rules button to open the Related Audit Rules Setup window. This will allow you to see the rules that determine which audits will be shown on that window.

If you are an Auditor Administrator, as defined on the System Settings window, then you will also be able to add, change, or delete the rules on the Related Audits Rules Setup window.

Related Audit Rules Setup window

This window lists all of the Related Audit Rules that have been set up for a given Dynamics GP window and all of its child windows.



This window opens when you click the Rules button on the View Related Audits window.

Description

This window shows all of the Rules that are set up for a given Dynamics GP "form." A form can be thought of as a container that holds a window and all of its child windows. As you can see in the example above, the Customer Maintenance window's form actually contains four windows. This window shows all of the Rules for all of the windows in the Customer Maintenance form.

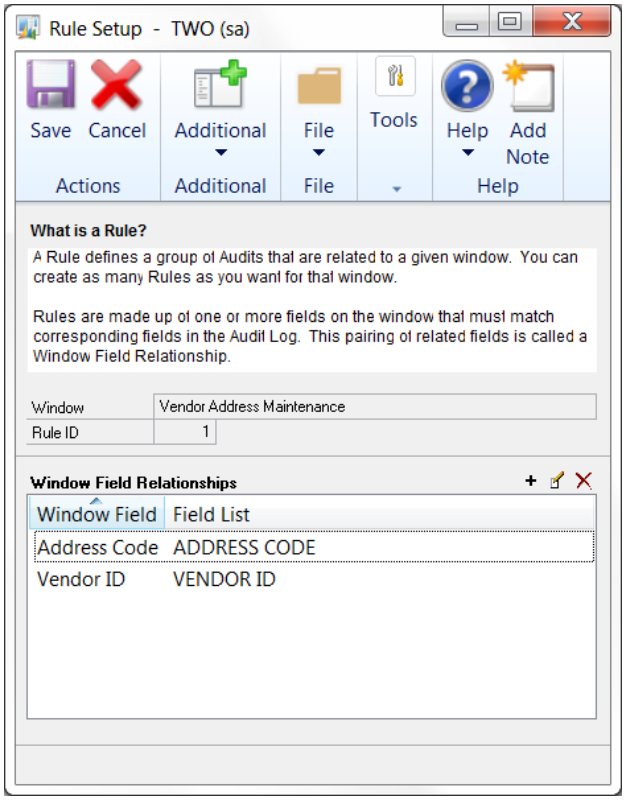
If you are an Auditor Administrator, you will be able to add, change, or delete Rules from this window. But, if you are not an Auditor Administrator, you will only be able to view the information on this window. This can be useful if you want to know which Related Audits are supposed to show for a given window. In this case, you will not see the Add, Edit and Delete buttons to the upper-right of the Related Audit Rules tree.

Auditor Administrators can add a new Rule by selecting a window in the Related Audit Rules tree and then clicking the Add Rule button (+). However, to edit or delete a Rule, you must select that Rule (as opposed to the window name) and then click the Edit Rule button ( ) or Delete Rule button ( ).

Whether or not you are an Auditor Administrator, you can expand a Rule to show all of the Window Field Relationships for that Rule. In addition, you can expand a Window Field Relationship to show all of the fields in its Field List.

Rule Setup window

This window is where you define a single Rule for a window in Dynamics GP.



This window is accessible in one of these ways:

- By editing a line on the Related Audit Rules List window.
- By editing a Rule on the Related Audit Rules Setup window.

Description

You may wish to show several groups of audits on a given window. For instance, on the Customer Maintenance window, you would likely want to show anything that was audited for the displayed Customer Number. In addition, you may also want to show any audits that relate to the Salesperson for that Customer. These two separate groups of audits are defined by two separate “Rules.”

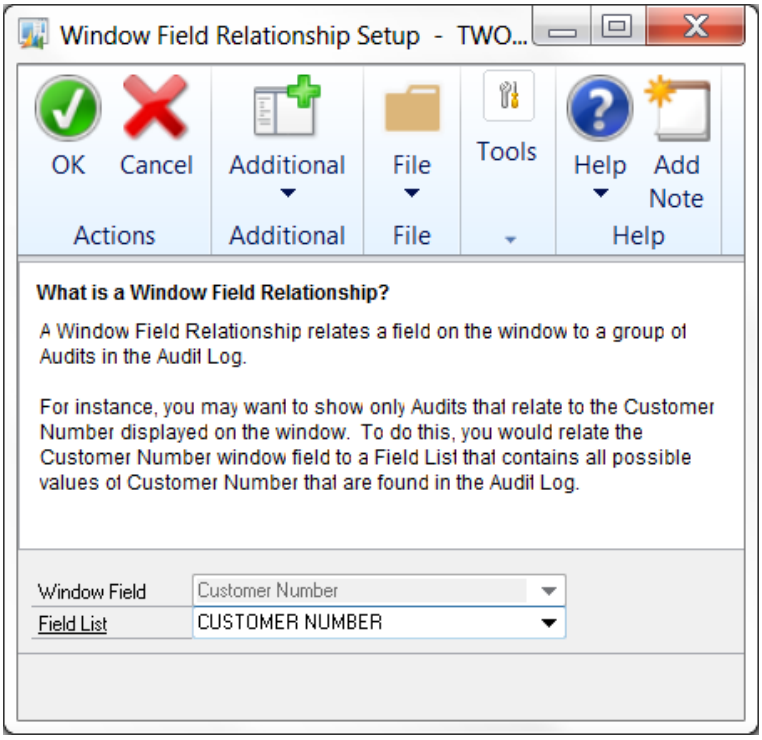
This window is used to define a single Rule for a window. A Rule is comprised of one or more “Window Field Relationships,” which are merely a way to say that the value of a field on the window must match the value of that field in the Audit Log in order for an audit to be displayed. If you have more than one Window Field Relationship for a Rule, then all of them must be satisfied in order for the Rule itself to be satisfied.

In the example above, we want to show all audits with an Address Code that matches the one displayed on the Vendor Address Maintenance window, and a Vendor ID that matches the one shown on that window. If either of these two conditions are not met for a given audit, then that audit will not be displayed on the View Related Audits window.

Since you can add, change, and delete Rules here, only Auditor Administrators, as defined on the System Settings window, can get to this window.

Window Field Relationship Setup window

This is where you relate a window field to a Field List.



This window is accessible by editing a line in the Window Field Relationship list on the Rule Setup window.

Description

The Window Field Relationship window is how you relate a group of audits in the Audit Log to a field on a window. In other words, this is how you tell Auditor that, for a given window, you only want to show audits where the value of a field on that window matches the value of the same field in the Audit Log.

There are two parts this specification. First, you must indicate which Window Field that you want to compare to the values in the Audit Log. The Window Field drop-down will list all fields on the window for which you want to display Related Audits. Enter or select the window that you want to compare.

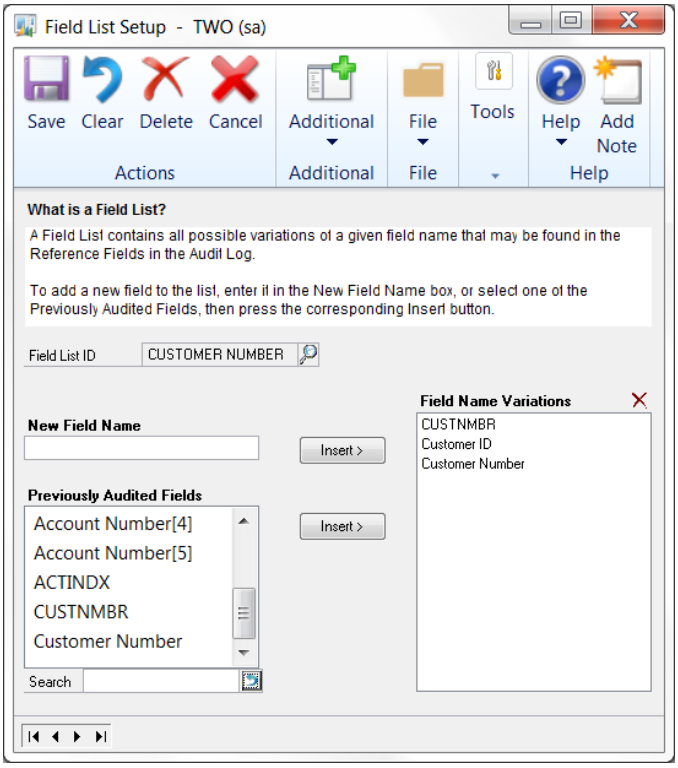
Next, choose a Field List from the drop-down. A Field List is defined in detail on the Field List Setup window section, later in this document. For now, just consider a Field List as the way you define how a field is named in the Audit Log.

By linking these two things together in a Window Field Relationship, you are saying that you want to only display audits that contain an Audit Reference field where the value of that Reference field matches the value of the Window Field chosen.

Since you can add, change, and delete Window Field Relationships here, only Auditor Administrators, as defined on the System Settings window, can get to this window.

Field List Setup window

This is where you manage all the Field Lists in Auditor.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Go to Microsoft Dynamics GP > Tools > Setup > Auditor > Field Lists.
- From the Window Field Relationship window, click on the Field List zoom.

Description

A Field List is a list of possible variations of how a given field can be named in the Audit Log. For instance, A Customer Number is usually called ‘Customer Number’, when it appears in a table or on a window. However, if you have created a SQL Table audit, then the SQL technical name for this field, ‘CUSTNMBR’, would be what you would see in the Audit Log. It is also possible that some window or table may have a ‘Start Customer Number’ and an ‘End Customer Number’. All of these variations, regardless of how they are named, are ultimately just Customer Numbers. So the purpose of the Field List is to tie all of these variations together into one definition that you can then use in any Window Field Relationship.

There are two ways to add a field name variation to a Field List. First, you can simply enter it in the New Field Name box and then click the top Insert button. This will allow you to enter any possible variation that you can think of that may end up being audited.

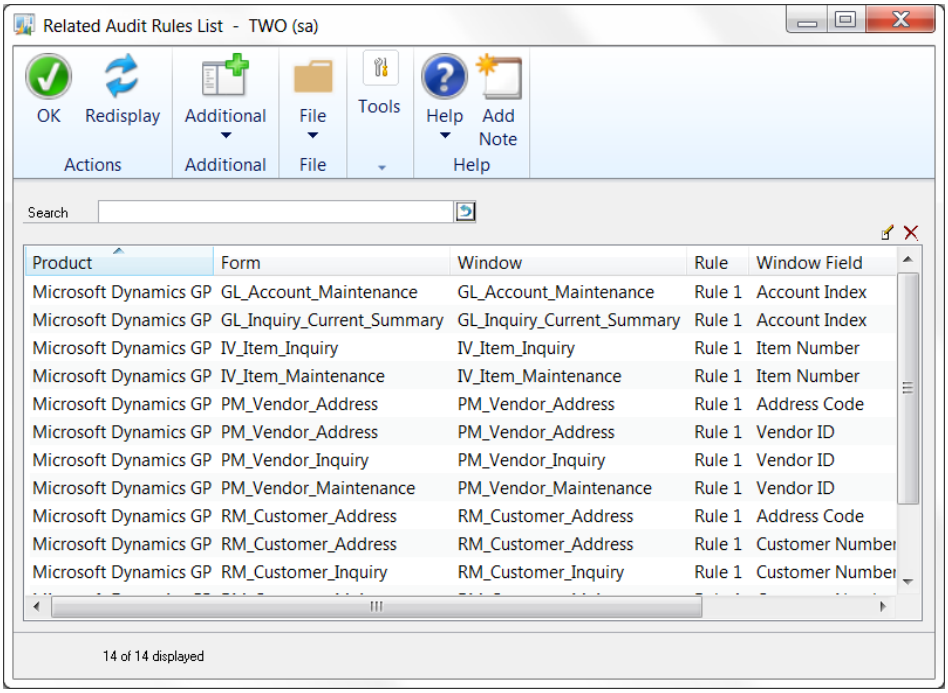
The second way may be more helpful. The Previously Audited Fields box lists all the Reference Fields that appear on any audit in the Audit Log. Use the Search field below the list box to narrow down the list to only those containing a certain value. This may be easier than coming up with these variations on your own. Select one or more fields from the list box and add them to the Field List by clicking the bottom Insert button.

You can also remove a field from the Field List by selecting it in the Field Name Variations list box and clicking the Remove Field Name from Field List button (✕).

Since you can add, change, and delete Field Lists here, only Auditor Administrators, as defined on the System Settings window, can get to this window.

Related Audit Rules List window

This window lists all of the Related Audit Rules that have been set up in Auditor.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Go to Microsoft Dynamics GP > Tools > Setup > Auditor > Related Audit Rules.

Description

This window is simply a list of all the Related Audits Rules that have been previously set up. To be more precise, it lists all of the Window Field Relationships for each rule in the system. From here, you can edit a particular rule by double-clicking on a line in the list, or selecting it and clicking the Edit Rule button (✎). Additionally, you can delete one or more Window Field Relationships by selecting them and clicking the Delete Window Field Relationship (✕) button.

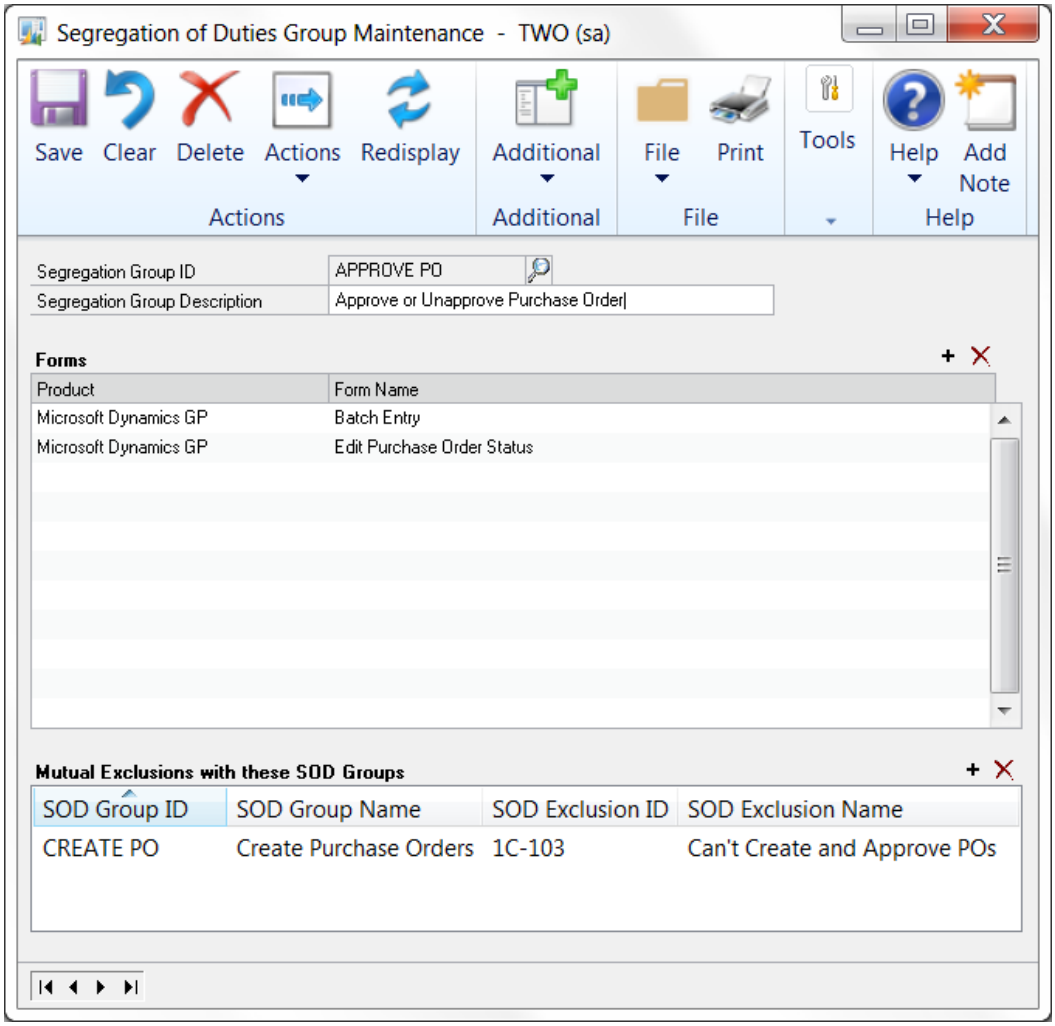
Use the Search field to narrow down the list. Whatever you enter here will be compared to each of the columns in the list. If none of these fields contains the Search value you entered, then that line will not be displayed.

Since you can change and delete Related Audit setups here, only Auditor Administrators, as defined on the System Settings window, can get to this window.

Segregation of Duties

Segregation of Duties Group Maintenance window

Segregation of Duties Group Maintenance is where you manage Segregation of Duties.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Go to Microsoft Dynamics GP > Tools > Setup > Auditor > Segregation of Duties Groups.

Description

Segregation of Duties is accomplished by putting similar tasks in a Segregation of Duties Group (or SOD Group, for short), which is tracked by a SOD Group ID and Description. For instance, the screen shot above shows the forms that are required for the task of approving a Purchase Order. The Dynamics GP forms Batch Entry, Edit Purchase Order Status, and Purchase Order Entry are added to this Group.

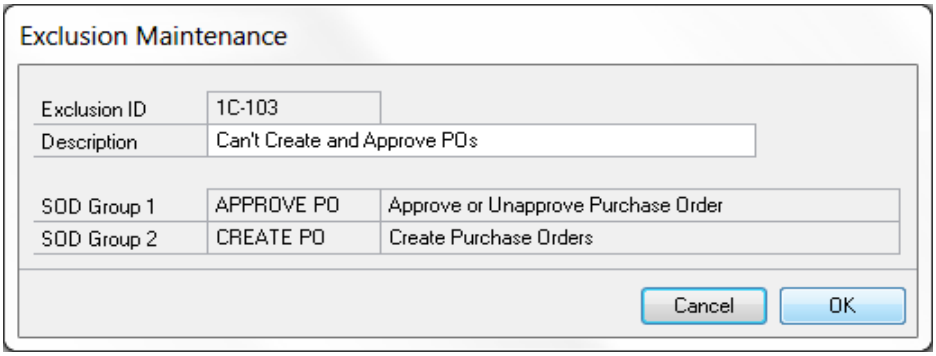
Once this SOD Group is created, you can make it mutually exclusive with other SOD Groups. This means that if a given user has security to any form in SOD Group 1, and then also has security to forms in SOD Group 2, a conflict is flagged.

Creating Segregation of Duties Groups

To create a SOD Group, enter the SOD Group ID and Description. Add or remove forms from the SOD Group by clicking on the Add SOD Group or Remove SOD Group buttons at the upper-right of the Forms list. Once you have set up at least two SOD Groups, you can add an Exclusion by clicking the Add SOD Exclusion button to the upper-right of the Mutual Exclusions with these SOD Groups list.

You may also create a SOD Group automatically by importing an existing Security Task. Do this by clicking the Actions button and choosing Import Security Task from the drop-list. You will then be presented with the Security Task Lookup, where you will select the Task that you want to import. The Task ID will become the new SOD Group Name and the Task Name will become the SOD Group's Description. If the Task ID is longer than 15 characters, then you will be asked to enter a shorter SOD Group ID.

You can have unlimited Exclusions set up between SOD Groups.



Rockton Software does not provide templates for SOD Group setups because every entity has unique requirements for Segregation of Duties. You will have to determine what is best for your organization when setting up SOD Groups and Exclusions.

You can Export your entire setup of Segregation of Duty Groups clicking the Actions button and choosing Export SOD Groups from the drop-list. This will create one file (called RSA_SODGROUPS.auditor, by default) that contains all Groups. The Import SOD Groups option will read a file of the same format and create all SOD Groups from that file.

The Build Security Manager Filter option will create a Filter that contains only the windows in the currently displayed SOD Group. The Filter ID will be the name of the SOD Group, prefixed with "SOD-".

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Segregation of Duties Group Maintenance window, but not make any changes to any of the groups presented here. This is true even if the user is also in the POWERUSER or any other security role.

E-Sign

Overview

E-Sign is an “electronic signature” function that gives you the ability to specify that changes to certain fields in the accounting system require the signature of the User making the change, and optionally, an approver’s signature. Users and Approvers “sign” actions by entering their Dynamics GP password. The record of this approval is stored in the E-Sign Approval Log tables on the system database.

Setting up E-Sign requires three simple steps:

1. Select which Users will be E-Sign Approvers. This is done on the Auditor System Settings window.

2. You require a Signature or Approval for changing a field by creating an E-Sign Signature Definition (or “Signature”, for short). Here you can attach a Reason Group and optionally assign specific Approvers to that field’s Signature requirement. You can also specify the Users and Companies to which this Signature applies.

3. Attach the Signature to each field on each window where that requirement should be active. This is called a Signature Assignment (or “Assignment” for short). Assignments are made via a Wizard that gives you step-by-step instructions for assigning a signature to a field on a window.

Repeat steps 2 and 3 for each Signature requirement that you have. E-Sign will then be completely set up.

The Approval Process

A user that makes a change to a field that has a signature assigned to it, that user is referred to as the Requestor. When one of these changes is made, either the E-Sign Approval Needed window will open (if the change must be approved first) or the E-Sign Signature Needed window will open (if you simply want the Requestor to certify that they have made the change by signing it).

If only a signature is required, then the Requestor simply needs to enter their Dynamics GP User ID and Password. They will then be allowed to proceed with the change.

If their change requires an approval, they will need to enter their own Dynamics GP User ID and Password, as in the signature-only scenario. However, they will also need to have a second user approve their change as well.

Depending upon how the signature was defined, they will have up to three options for obtaining that approval:

- Local Approval
- Remote Approval
- Queued Approval

Local Approval

The simplest option, which will always be available, is the Local Approval. In this case, the Requestor will click the Approve button, which will open the Approver Password window so that the Approver you have selected can enter their password at your computer. Once the Approver has entered their password, the Approval process is complete.

This method is only useful, of course, if the Approver can physically come to the Requestor's location. However, if this is not possible or convenient, then there is another option.

Remote Approval

If an Approver is currently logged into Dynamics GP, you can submit an approval request to that Approver by clicking the Submit button. This will give the Approver the ability to approve or deny the request at his or her own desk.

Clicking the Submit button will put the approval in a status of Pending and the Requestor will see this in the status area in the upper-right corner of the window.

After approximately one to two minutes have passed, this will automatically open the E-Sign Pending Approval Requests window on the Approver's computer. Here, they can approve or deny this request, or any other outstanding (Pending) requests.

Once that Approver has approved or denied the request, the status area on the E-Sign Approval Needed window on the Requestor's computer will reflect this result automatically. Also, if the request was denied, then a pop-up message will display the reason that the Approver entered for denying the request.

The Requestor can now click OK to complete the Approval process. If the request was denied, then the original change that the user made will be undone. If it was approved, then one of the following actions will occur:

- If the field being approved was a button field, then that button will be processed automatically.
- If the field being approved was not a button, then the user will be returned to the original window with their change intact. They can now continue with their work on this window. If they choose to change the value of that field at this time, the approval process will start over again.

It should also be noted that while a submitted request is awaiting completion, the Requestor can cancel that request by clicking the Cancel button. This will remove it from the E-Sign Pending Approval Requests window on the Approver's computer.

Queued Approval

A drawback of using a Remote Approval is that the Requestor must wait for their change to be approved or denied before they can proceed with any other work in Dynamics GP. This can be inconvenient if they Approver is logged in to Dynamics GP, but not at their computer at the time that a request is submitted. For this reason, we have included a third approval type called a Queued Approval.

Queued Approvals allow you to submit a change request to a queue, thereby allowing you to continue with your work independent of the Approver's availability. Once the request has been approved or denied, the E-Sign Request Status window will automatically open in the Requestor's Dynamics GP session to notify them of this outcome. If the request was approved, they will then be able to choose what to do with that change request:

- Click the Apply button to make the change at that time;
- Click the Later button to defer making the change until a later time;
- Click the Decline button to discard the change even though it was approved.

When the Requestor chooses to either Apply or Decline the change, the original request will be updated with that final status in the E-Sign Approval Log table.

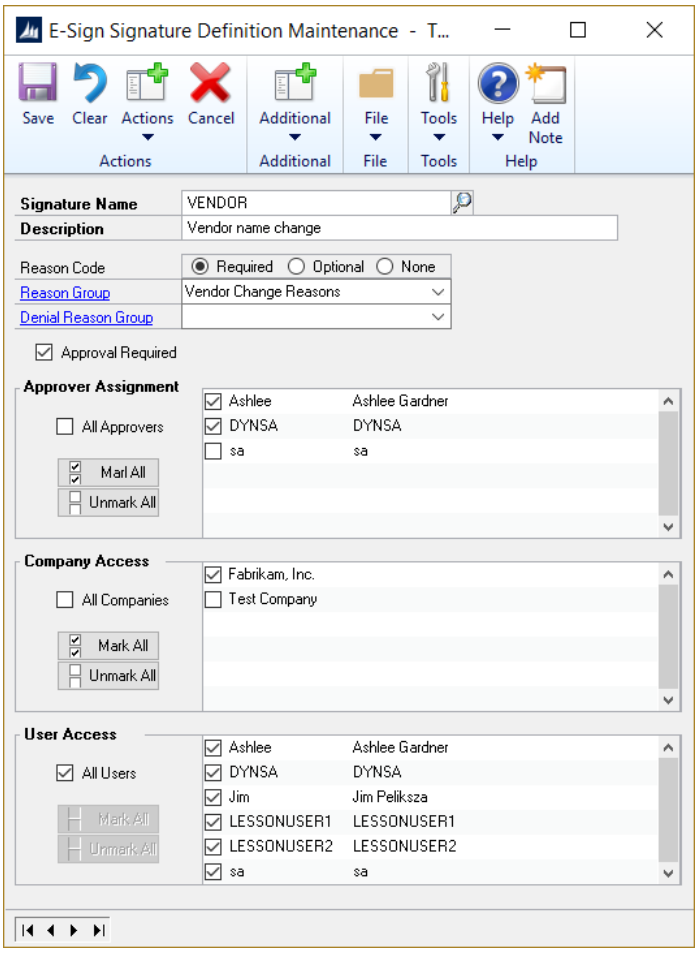
If you wish to review the approval requests that you have queued, you can do this by opening the E-Sign Queued Approval Requests window. Here, you will be able to view the status of your requests, and cancel any requests that you no longer need.

You will probably find that queued approvals are the most useful of these three types. However, there are some cases where the window to which you want to assign a signature has some complexity that renders the queued approval process impossible. In those cases, you will need to set up a non-queued approval.

One particular case where you will always need to set up a non-queued approval is when you want to assign a signature to a button field, such as a Save button or Post button.

E-Sign Signature Definition Maintenance window

The E-Sign Signature Definition Maintenance window is where you specify which fields will require a signature or authorization to change them.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > E-Sign Signatures.

Description

The E-Sign Signature Definition Maintenance window allows you to set up all of the requirements for a Signature. Here you will specify a Name and a Description that will be displayed to the User when they are asked to approve a change.

You can specify whether you want the User to give a reason why they are making a particular change with the Reason Code radio group. If you choose the Required radio button, then you must also select a Reason Group that will be presented to the User on the Approval Needed or Signature Needed windows.

If you only want the User to sign the change they are making, but do not require a separate Approver's signature as well, uncheck the Approval Required check box. If approval is required, however, then you will also need to choose a Denial Reason Group and one or more Approvers.

Assigning Approvers

When a User makes a change to a field that requires approval, they will be provided with a lookup of the applicable Approvers for that Signature. An Approver can be used only if the following criteria are met:

- They are an Assigned Approver on the Signature Definition, or 'All Approvers' is marked on the Signature Definition
  AND
- The Approver has access to the Company in which the change was made.

By default, when you setup a new Signature Definition, the 'All Approvers' check box is checked. This means that any Approver can potentially be used when this Signature is invoked, as long as the Approver has access to the Company in which the change was made. If you add new Approvers on the Auditor System Settings window, then they will automatically be available to all Signatures with 'All Approvers' checked. However, if you uncheck 'All Approvers', then you must assign specific Approvers to that Signature.

Company and User Access

You can make a Signature apply to only specific Companies or Users by unchecking 'All Companies' or 'All Users' and then selecting the Companies or Users that do apply.

Note that each Company that this Signature has access to must have at least one Approver assigned that has access to that Company. If you see the words "**No Approvers**" to the right of the Company Name then you must either select an additional Approver or remove access to this Company.

Assigning the Signature

Now that you have completed your Signature Definition, you need to tell E-Sign where the Signature should be activated. You do this by checking the Actions button at the top of the window and choosing Assignments from the drop list. This will open the Signature Assignment window, which is described later in this document.

Importing and Exporting Signature Setups

You can Export a Signature Definition and all of its associated Signature Assignments to a text file. This can then be Imported at another site or just saved as a backup. You do this by first displaying the Signature that you wish to Export and then clicking the Actions button and choosing Export from the drop list. This will create a text file with the Signature Name as the file name and ".signature" as the extension.

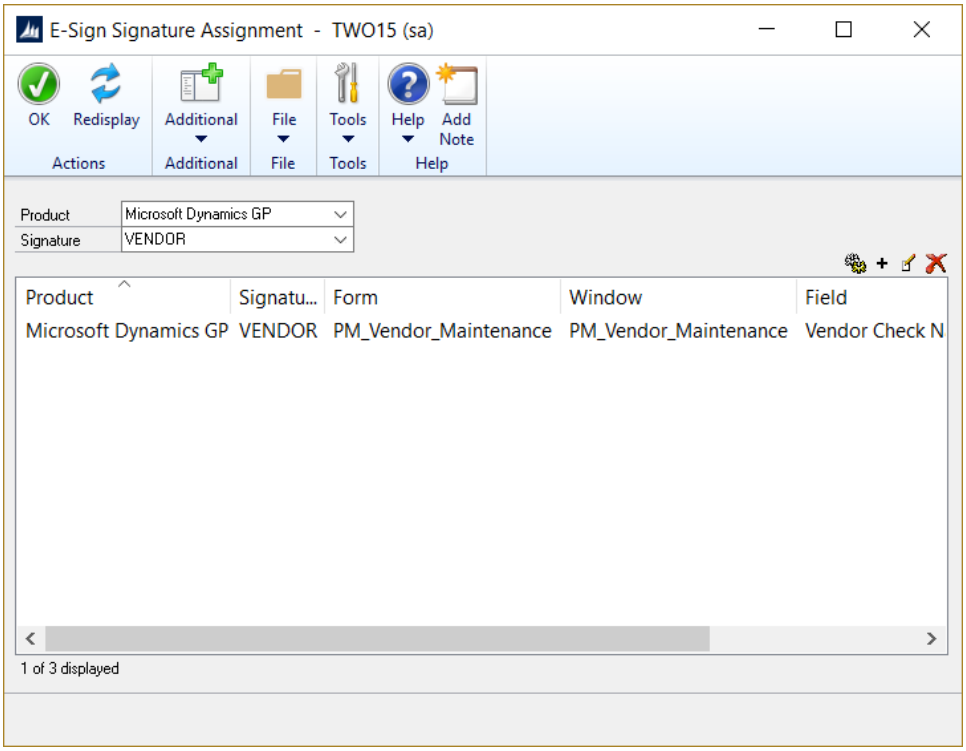
To Import a Signature Definition, click the Actions button and choose Import from the drop list, then browse to the location of the Signature file that you want to Import. If a Signature with the same name as the one you are trying to Import already exists in the system, you will be asked if you want to replace it.

One thing to keep in mind is that the Approver assignments, Company Access and User Access will not be Exported or Imported. If you Import a Signature, then 'All Approvers', 'All Companies' and 'All Users' will be checked.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the E-Sign Signature Definition Maintenance window, but not make any changes to any of the options presented here. This is true even if the user is also in the POWERUSER or any other security role.

E-Sign Signature Assignment window

The E-Sign Signature Assignment window is where you tell E-Sign to which windows and fields a Signature applies.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Open the E-Sign Signature Definition Maintenance window and click the Actions button, then choose Assignments from the drop list.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > E-Sign Signature Assignments.

Description

The process of creating a functional Signature is not complete until you assign that Signature to each field on each window where you want that set of signature or approval requirements to be activated. The E-Sign Signature Assignment window is where you link a Signature Definition to the window field(s) to which it applies.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the E-Sign Signature Assignment window, but not make any changes to any of the options presented here. This is true even if the user is also in the POWERUSER or any other security role.

The Actions button ( ) allows you to register and unregister Signature Assignments. This is not something that you would normally do unless requested by Rockton Support

To assign a Signature to a window field, first click the Add Assignment button (+) to open the wizard. See the section on E-Sign Signature Assignment Wizard window for more information on this procedure.

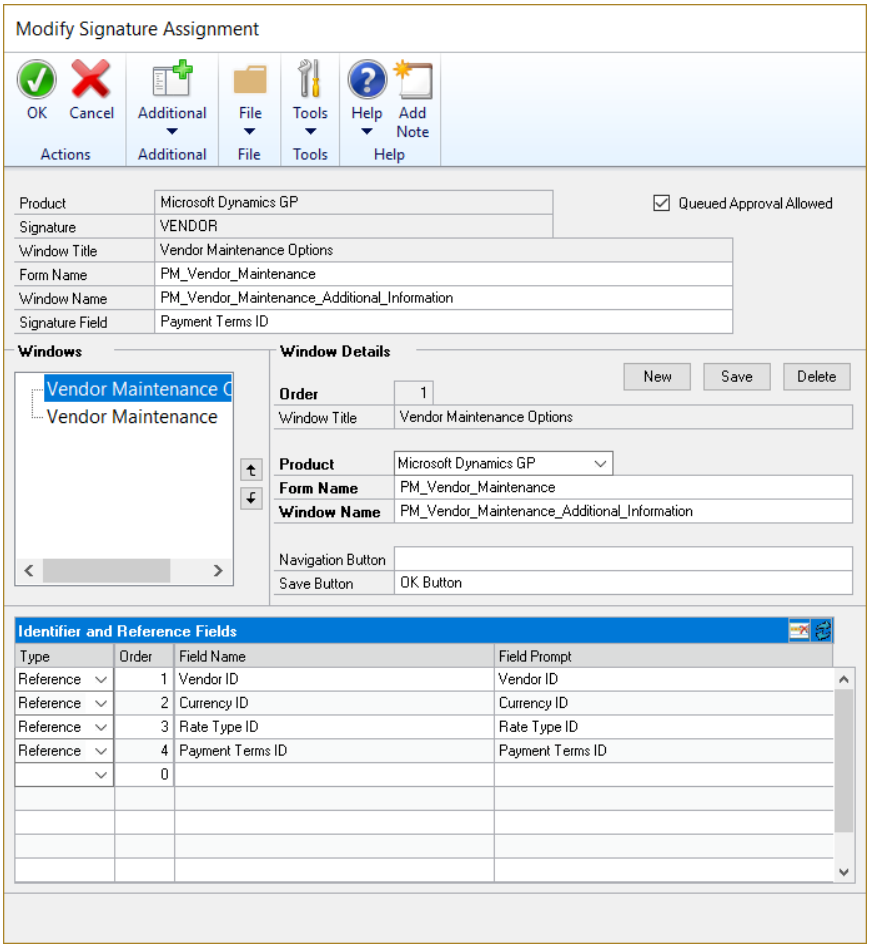
To remove a Signature Assignment, select it in the list; then click the Delete button (✕).

You can make changes to a Signature Assignment by selecting it in the list and clicking the Edit button ( ). This will open the Modify Signature Assignment window (see below) where you can change aspects of the Signature Assignment manually.

Modify Signature Assignment window

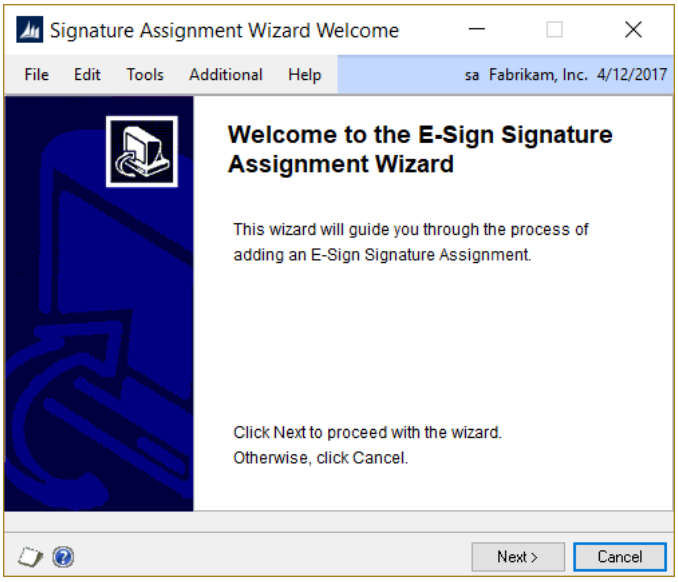
We typically do not recommend using the Modify Signature Assignment window to make changes to your signature assignments. However, in certain exceptional situations, you may be asked to do so by Rockton Support.

If a user is in the AUDITOR AUDITORS security role, they will be able to view the Modify Signature Assignment window, but not make any changes. This is true even if the user is also in the POWERUSER or any other security role.



E-Sign Signature Assignment Wizard window

The E-Sign Signature Assignment Wizard helps you to connect Signatures to fields on windows.



This window is accessed by clicking the + button on the E-Sign Signature Assignment window.

Description

The easiest way to assign a signature to a window field is by using the E-Sign Signature Assignment Wizard. You will be able to assign both queued and non-queued approvals using this wizard.

A Queued Approval is one that will allow you to submit the change request to an approver and then allow you to go on with your work without waiting for the request to be completed. You will probably find that queued approvals are the most useful. However, there are some cases where the window to which you want to assign a signature has some complexity that renders the queued approval process impossible. In those cases, you will need to set up a non-queued approval.

One particular case where you will always need to set up a non-queued approval is when you want to assign a signature to a button field, such as a Save button or Post button.

Using the Signature Assignment Wizard

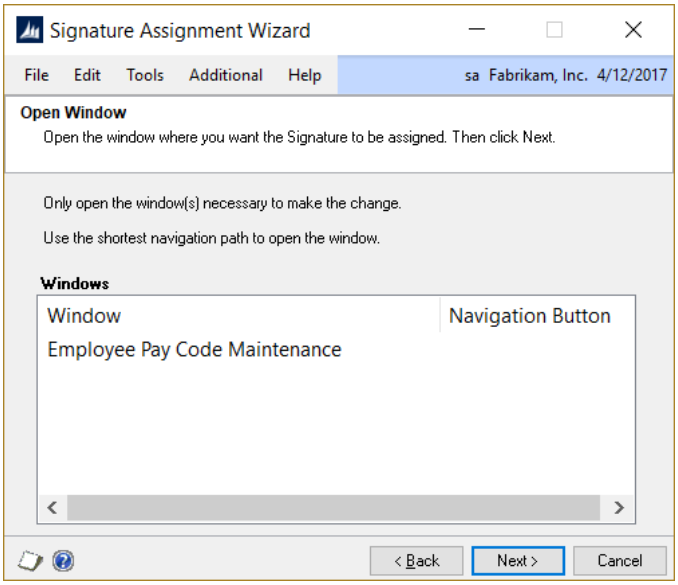
The following procedure will detail how to use this wizard to assign a queued approval:

1. First open the E-Sign Signature Assignment window by going to Microsoft Dynamics GP > Tools > Setup > Auditor > E-Sign Signature Assignments.
2. Click the Add Assignment button (+). This will open the Signature Assignment Wizard Welcome window shown above. Click the Next button to start the wizard.

3. **Select the E-Sign Signature.** Type the signature that you want to assign to a window field, or click the lookup button (🔎) and select it from the list. You can also type a new Signature Name and you will be given the option to create a new signature definition on the E-Sign Signature Definition Maintenance window.

4. Choose Yes or No in the "Can this Signature be Queued?" drop-down to specify if you want this signature to be queued. Then click the Next button.
5. **Open Window.** The next window you see depends on what you chose in step 4.

   For Queued Signatures:



   Open the window where you want to assign this signature. Each window that you open will appear in the Windows list. *Open the fewest number of windows possible.* For example, to assign the signature to the Customer Address Maintenance window's Contact field, do not go to Cards > Sales > Customer, then click the Address button to open Customer Address Maintenance. Instead, navigate directly to Cards > Sales > Addresses. When you are done, click Next.

The reason for specifying the "shortest path" is that if you use a longer one, the approval will only work if the user making a change request uses that longer path to get to the window. If they were to use a shorter path, then they would see errors when they try to apply an approved change and the approval process would fail.

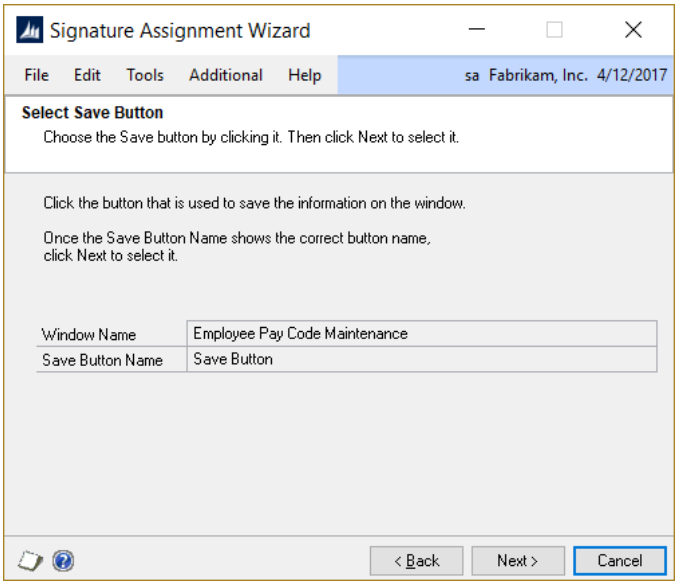
For Non-queued Signatures:

Open the window where you want to assign this signature. The Window Name will appear in the wizard window above. Then, click Next.

6. **Select Signature Field.** Move your cursor to the field to which you want to assign this signature. It will appear as the Signature Field on the window below. When you are done, click Next. If this field already has a signature assigned, you will be asked if you want to continue and delete this signature. If you want to assign to a button field, you must choose No in step 4.

   Note: If you chose No in step 4, you will be sent to step 9 \when you click the Next button.

7. **Select Save Button**. Click the button that is used to save the information on the window. That button will appear as the Save Button Name. Then, click Next.



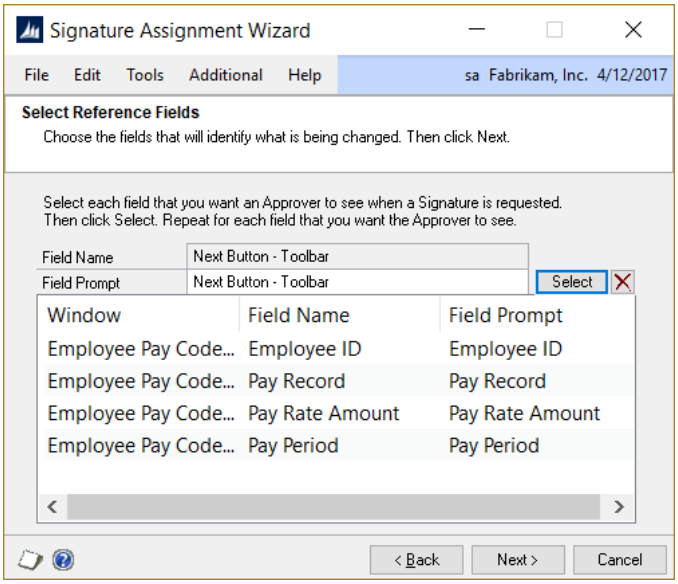
8. **Select Identifier Fields**. Identifier Fields are those that a user must enter to display a record in the window you selected in step 5. You choose an Identifier Field by moving your cursor to that field and then clicking the Select button in the middle of the wizard window. To remove a field that was added incorrectly, highlight it and click the Delete Field button (✕).

   For instance, on the Employee Pay Code Maintenance window, you must first select an Employee ID. After that, you must then select the Pay Code that you want to display for that Employee. This will result in both fields being displayed on the Signature Assignment Wizard window.

   When you are done selecting Identifier Fields, click the Next button. If you had to open more than one window in step 5, you will be asked to select Identifier fields for each of those windows.

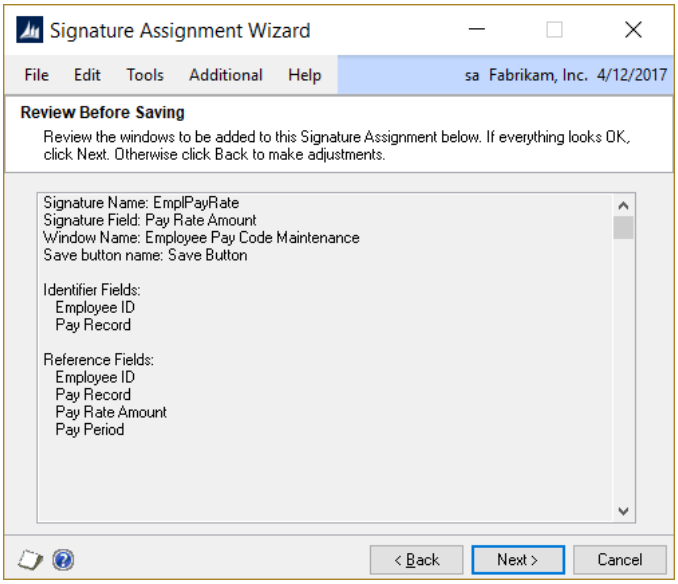
9. **Select Reference Fields**. Reference Fields are fields that you want an Approver to see when the Signature is requested. Typically, you would choose the fields that help the Approver to determine which record is being changed. You choose a Reference Field by moving your cursor to that field and then clicking the Select button in the middle of the wizard window. To remove a field that was added incorrectly, highlight it and click the Delete Field button (✕).

If a field that you want to select is locked, you may need to click that window's Clear button so that the field becomes enterable.



When you are done selecting Reference Fields, click the Next button.

10. **Review Before Saving**. Review the information that you have selected on the previous windows. If you need to make any changes to anything that you have specified previously, click the Back button until you get to that step. Otherwise, if you are satisfied with your selections, click the Next button.

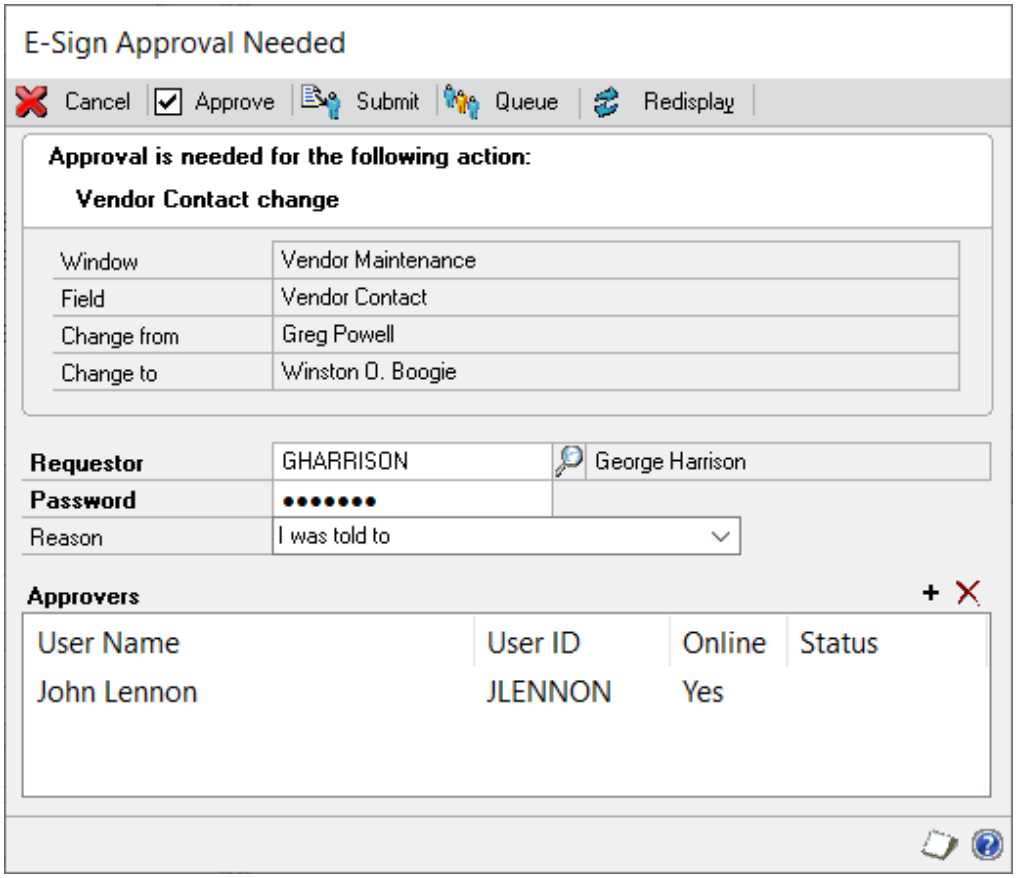


11. **Signature Assigned Successfully**. The process of assigning your signature is now complete. If you wish to view the assignment on the Modify Signature Assignment window, mark the “Display the Signature Assignment” check box. Then click the Finish button to close the wizard.

We typically do not recommend using the Modify Signature Assignment window to make changes to your signature assignments. However, in certain exceptional situations, you may be asked to do so by Rockton Support.

E-Sign Approval Needed window

This window is where a User requests approval for a change that they have made.



This window will open automatically when a User makes a change to a window field that has an E-Sign Signature assigned to it that requires an approval.

Description

This window opens after a User makes a change to a field that has an E-Sign Signature Assignment, if the Signature Definition has the Approval Required option set. The User making the change is called the Requestor. The Requestor must complete the Approval process or click Cancel before they can proceed. If the Requestor clicks Cancel, the Approval request will be removed and the change will be undone.

Enter or select the Requestor's User ID in the Requestor field. This field will be defaulted to the User that is currently logged in; however, this can be over-ridden. This may be necessary if the Requestor is making the change while logged in as another GP User.

Next, enter the GP User Password for the Requestor.

Enter the Reason for why the change is being made. This field may or may not be required, or may even be disabled, depending upon what was chosen on the Signature Definition. You can type a reason into this field or select one from the drop-down list.

Choose the Add Approver button (+) to select one or more Approvers. This will open the Approvers lookup, which will give you a list of all valid Approvers for this Signature.

Local Approval

If an Approver can be available right at the Requestor User's desk, they may use the Approve button to perform a Local Approval.

1. Add only one Approver to the Approvers list at the bottom of the window. If you don't have exactly one Approver, then the Approve button will be disabled.
2. Press the Approve button.
3. The Enter Approver Password dialog will open. Enter the Approver's Dynamics GP password and choose the Approve button to complete the Approval.
4. You will now be allowed to save the approved change.

Remote Approval

Use the Submit button to remotely notify one or more online Approvers (those logged in to Dynamics GP) that you have a change that needs to be Approved.

1. Add one or more Approvers to the Approvers list at the bottom of the window.
2. Press the Submit button.
    a. If at least one selected Approver was found to be online at the time the User pressed Submit, **Pending…** will show as the status in the upper-right of the E-Sign Approval Needed window. Each online Approver will show a Status of Submitted.
    b. If any Approvers were offline at the time the User pressed Submit, a message will be displayed stating that some Approvers were not notified.
    c. If no Approvers were found to be online at the time the User pressed Submit, a message will be displayed stating that no Approvers were notified and that the Submit failed.
3. If a request for approval has been successfully submitted to at least one Approver, the Requestor User will then need to remain on the E-Sign Approval Needed window until that request is either Approved or Denied.
4. Notified, online Approvers will see the E-Sign Pending Approval Requests window open shortly after a request is submitted. Here, they may choose to respond to any request that has been assigned to them.
5. Once an Approver responds to a request, the Requestor User will get notified on the E-Sign Approval Needed window:
    a. For an approved request, **Approved** will show as the status in the upper-right of the window. In the Approvers list, the responding Approver will show a status of Approved; each other Approver will show a blank Status.
    b. For a denied request, **Denied** will show as the status in the upper-right of the window. In the Approvers list, the responding Approver will show a status of Denied; each other Approver will show a blank Status. The Requestor will see a message showing why the request was denied.
    c. The only active buttons on the window will be OK and Redisplay.
6. The User may then click OK to close the E-Sign Approval Needed window.
7. If the request was approved, then the requested change will be available to be saved; if the request was denied, then that change will be backed out.

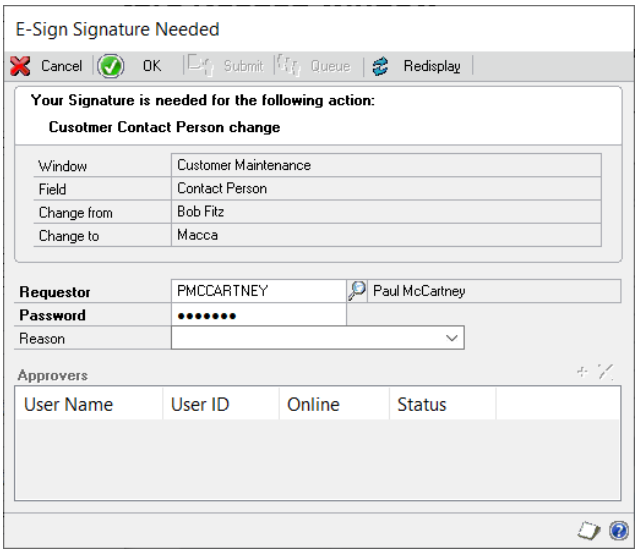
Queued Approval

Use the Queue button to notify one or more Approvers (logged in to Dynamics GP or not) that you have a change that needs to be Approved. The advantage of this method is that you can close the window and do other work while you await an Approver's response. The disadvantage is that this method may not work in some situations where a Remote Approval or Local Approval may work.

1. Add one or more Approvers to the Approvers list at the bottom of the window.
2. Press the Queue button.
3. The Requestor will see a message indicating that they can close the window and continue with their other work while they await an Approver's response. After the user closes this message, the E-Sign Approval Needed window will close.
4. Notified, online Approvers will see the E-Sign Pending Approval Requests window open shortly after a request is submitted. Here, they may choose to respond to any request that has been assigned to them.
5. Once an Approver responds to a request, the E-Sign Request Status window will automatically open on the Requestor User's computer if they are logged into Dynamics GP. This window will show the status of the request as well as give the Requestor the ability to apply an approved change or discard it.

E-Sign Signature Needed window

This is where a User enters their Signature for a change that they have made.



This window opens automatically when a User makes a change to a window field that has a Signature assigned to it that does not require an approval.

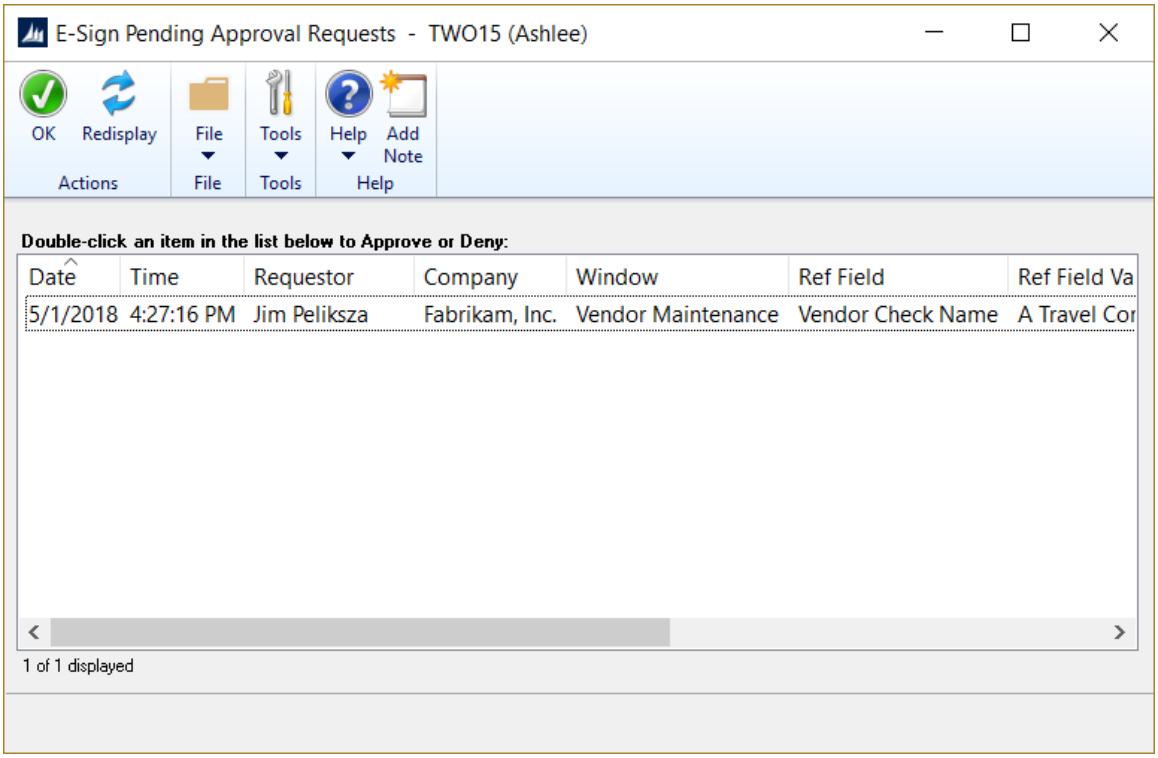
Description

This window will open after a User makes a change to a field that has a Signature Assignment if the Signature Definition does not have the Approval Required option set.

Enter or select the Requestor's User ID and Password, and optionally the Reason for the change. Then click OK. Clicking Cancel will undo the Requestor's change.

E-Sign Pending Approval Requests window

The E-Sign Pending Approval Requests window is where you can see changes that currently need your approval.



This window will open automatically for Approvers that have pending approval requests.

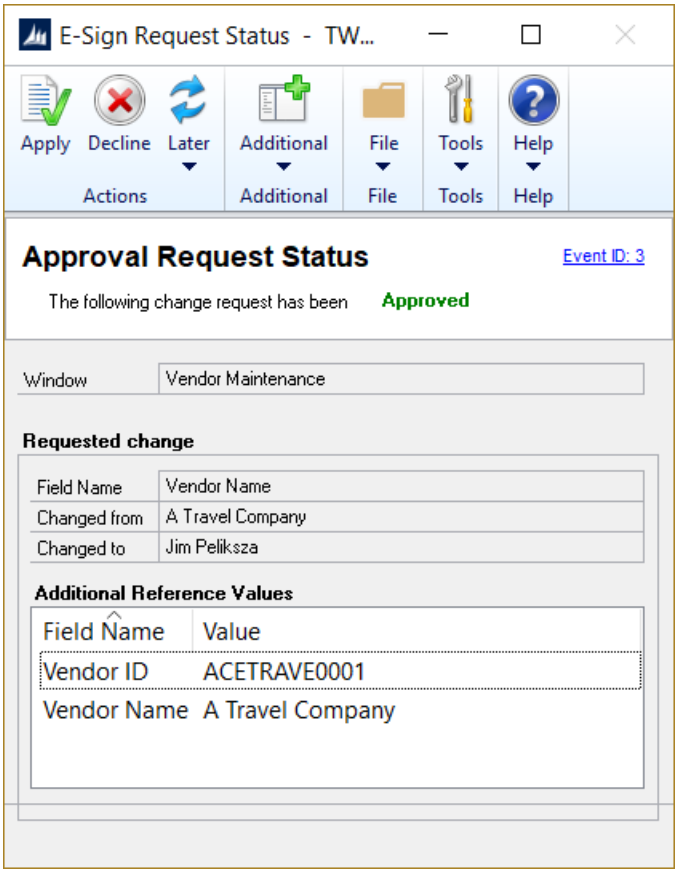
Description

This window opens automatically on an Approver's computer when a Requestor submits an approval request. If an Approver sees this window, he or she should try to approve or deny the pending request immediately if possible, because the Requestor cannot proceed until the request has been completed. For this reason, though this window can be closed temporarily by clicking the OK button, it will continue to be opened automatically until all pending requests are completed.

To complete a pending request, double-click it. This will open the Approval Inquiry window. On this window, you will see details of the request as well as an Approve button and a Deny button. The approver must choose one of these buttons and enter their password to complete the request. If they are denying the request, then they must also enter a reason for why they are doing so.

E-Sign Request Status window

This window is where you can apply or decline an approved change request.



This window is accessible in one of these ways:

- This window will open automatically after a queued approval request is approved or denied.
- Double-click an approved or denied request on the E-Sign Queued Approval Requests window.

Description

After an Approver approves or denies a queued approval request, that request will essentially be queued back to the Requestor for notification. After approximately one to two minutes, if the Requestor is logged in to Dynamics GP, the E-Sign Request Status window will open to inform them of the status of the change request. This can be seen in white **Approval Request Status** area at the top of the window. It will either show the word Approved, in green (see above), or the word Declined, in red.

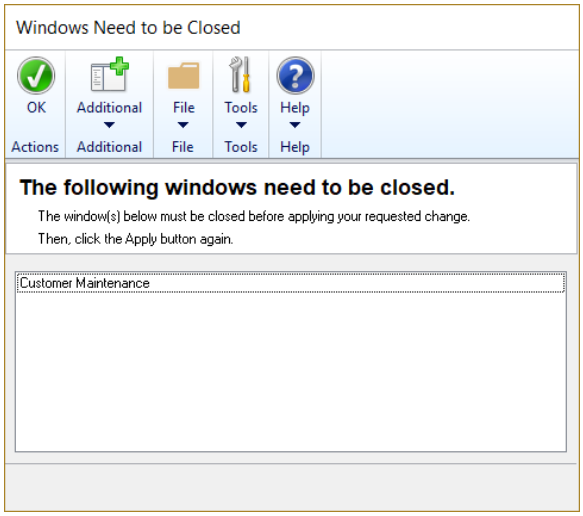
The main body of the window will show the Window where the change occurred. If the change was denied, you will see the Denied Reason below the Window. The Requested Change section will show the Field Name that was changed along with the value it was changed from and the value it was changed to. Below that, you will see the Additional Reference Values that were defined when you assigned the signature to that field.

Approved Requests

If the request was approved, you will see an Apply button, a Decline button, and a Later button at the top of the window. If you click Apply, the system will automatically apply the change by performing the following steps:

1. Open the window where you originally made the change, including any necessary preliminary windows;
2. Display the record that was changed;
3. Change the value of the field to its new value;
4. Click whatever button performs the Save action for that window;
5. Close the window(s) that needed to be opened in step 1 to make the change.

If any of these windows are already open when you click the Apply button, you will be notified that you first need to close them before you can apply the approved change.



If you see this window, note the windows listed and click OK to close the window. Leave the E-Sign Request Status window open while you complete your work on each window listed, and then close those windows. Then click the Apply button on the E-Sign Request Status window again.

The Later button will allow you to defer applying the approved change until a later time. Clicking this button gives you a drop-list with options to wait for 15 minutes, 30 minutes, 1 hour, 4 hours, 1 day, or 1 week before you will be presented with this particular approved change request. If you later decide that you want to go ahead and apply the approved change before that time has elapsed, simply open the E-Sign Queued Approval Requests window and double-click that request. This will open this window again immediately for that request.

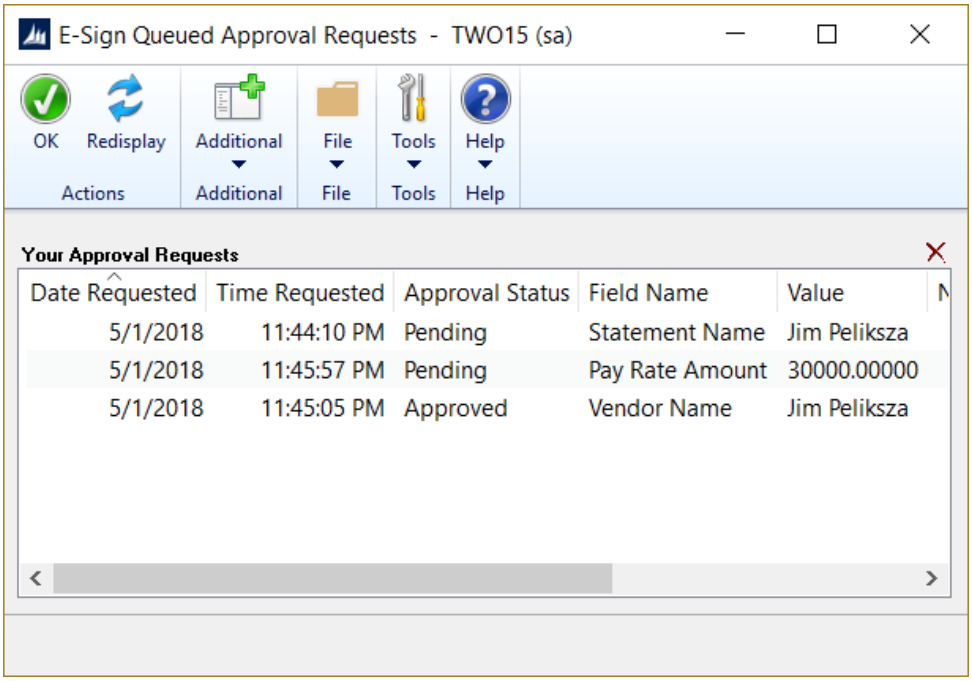
If, by the time your change was approved, you decide that you no longer need to make that change, simply click the Decline button. This will mark this approval as having been declined and the field you originally changed will not be modified.

Declined Requests

If the request was declined, the only action button you will see is an OK button, which will close the window.

E-Sign Queued Approval Requests window

The E-Sign Queued Approval Requests window is where you can review the outstanding change requests that you have submitted.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN or POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Utilities > E-Sign > Queued Approval Requests.

Description

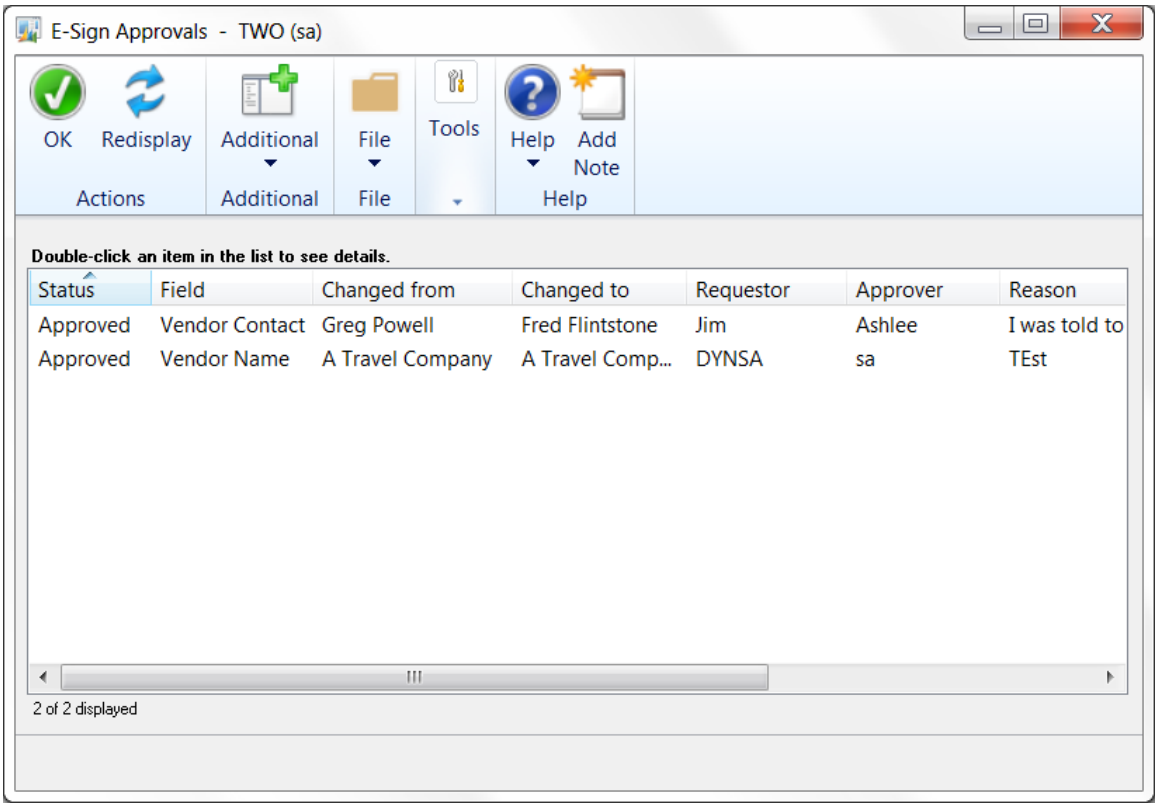
This window shows all the queued approval requests that you have submitted, but that are not yet completed. This list will mostly consist of requests with an Approval Status of Pending, meaning that an Approver has not yet approved or denied the request. However, there is usually a one to two minute lag between the time that a request is approved or denied and the time that you see this on the E-Sign Request Status window. Therefore, you may also briefly see requests with an Approval Status of Approved or Denied on this window as well.

If a request is still in Pending status, the only action you can perform on it is to delete it. You do this by selecting one or more pending requests and clicking the Delete Approval Request button (✕).

For requests that have been approved or denied, you can simply wait for E-Sign Request Status window to open. There you will be able to apply or discard an approved request or see the reason for a denied request. However, if you do not wish to wait, you can double-click a request that is in Approved or Denied status and that will open the E-Sign Request Status window immediately.

E-Sign Approvals window

The E-Sign Approvals window is where you can see changes that have been approved or denied for a window.



From a window that has had completed approvals, go to Additional > View E-Sign Approvals.

Description

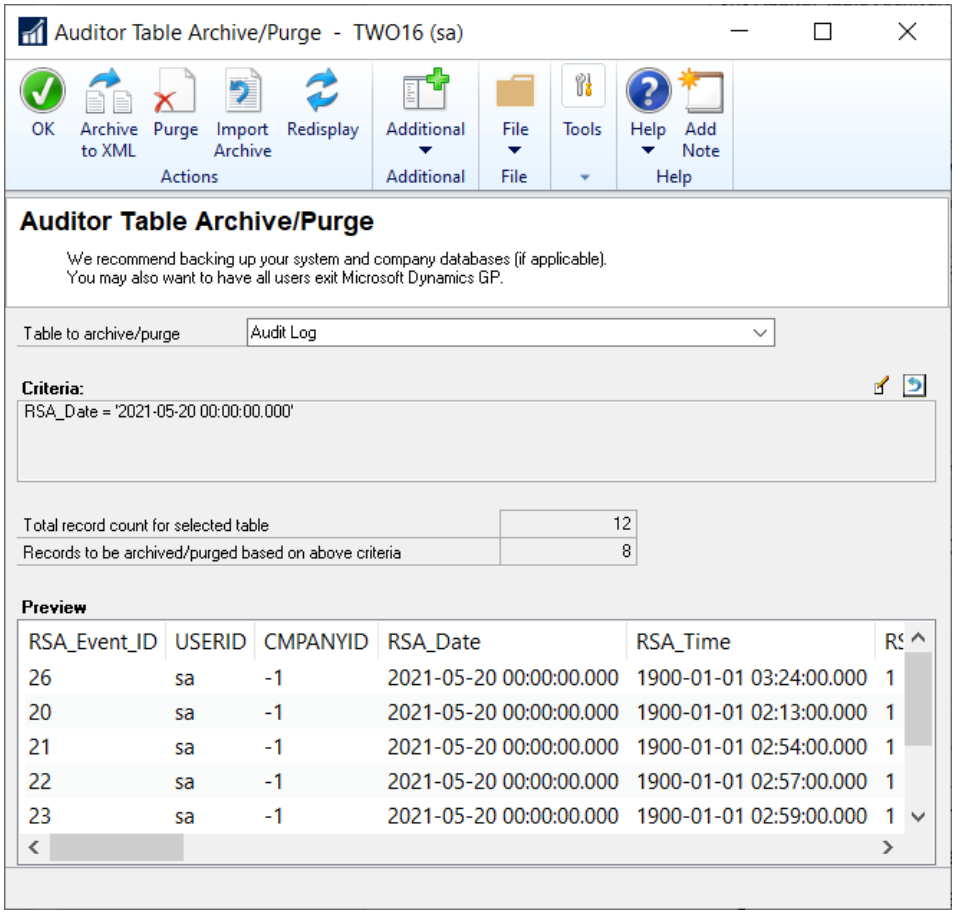
This is where you can view all changes that have been approved or denied for a window. If there has not been any E-Sign activity for a given window, then the Additional menu option will not be available.

You can see details of a particular approval or denial by double-clicking it.

Maintenance

Auditor Table Archive/Purge window

The Auditor Table Archive/Purge window is used to purge or archive Auditor records.



This window is accessible in one of these ways:

- From the Navigation Pane.
- Log on as a User in the AUDITOR ADMIN Security Role or the POWERUSER Security Role and go to Microsoft Dynamics GP > Tools > Setup > Auditor > Auditor Setup. Then choose the Auditor Table Archive/Purge task.

Description

The Auditor Table Archive/Purge window is used to purge or archive records from tables that typically tend to grow large over time. This may result in reduced system performance, especially in viewing Auditor items in Smartlist. This window will permanently archive selected records to XML files and then purge these records.

The Tables to archive/purge drop-down lists the following items:

Drop-down item	Database tables
Audit Log	RSAS015 and RSAS031
Approval Log	RSAS039 and RSAS044
Security Audit Log	RSAS045
Journal Voucher Roadmap Tracking	RSAS1000
Transaction Lifecycle Tracking	RSAS1100 and RSAS1200

All are in the DYNAMICS database.

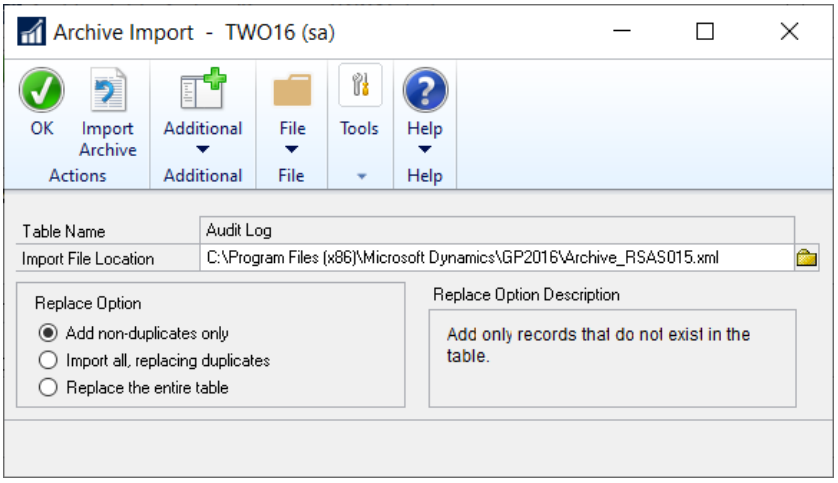
You can define a query to select records for purging and/or archiving to XML. Press the Edit Criteria button ( ) to open the Query Builder window where you can define a selection query to apply to the table. See the following section on the Query Builder window for more information.

Once you have defined your Criteria, the number of records that match the query will be in the 'Records to be archived/purged based on above criteria' field. Notice that the total number of records in the table is also shown. These records will be listed in the Preview list at the bottom of the Auditor Table Archive/Purge window. You have several actions that you can take on this group of records.

Archive to XML will create files in XML format that have textual representations of these records. You can view these files in most browsers or in an XML editor.

Purge will delete the selected records from the table; these records can be recovered by importing a previously created XML archive or by restoring from a backup.

Import Archive will open the Archive Import window where you can bring the contents of a previously created XML archive file back into the original master tables.



First, enter or select the path and filename of the XML archive file to import.

This file must be one that was created by the Archive to XML function on the Auditor Table Archive/Purge window for it to be imported properly.

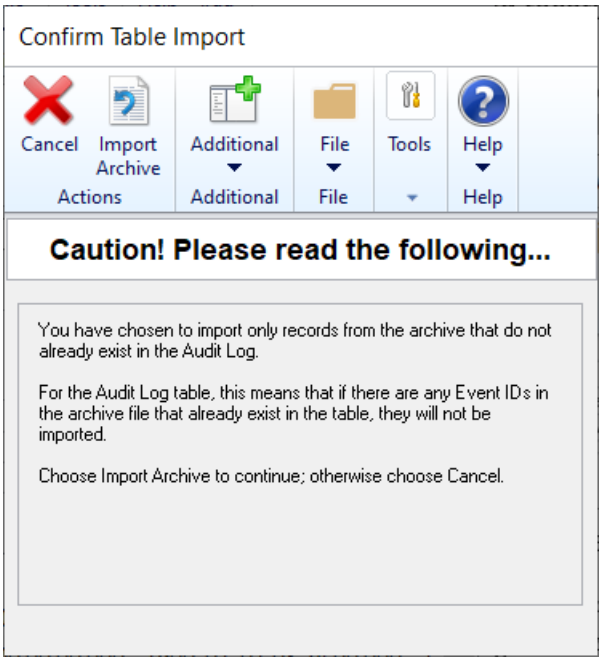
Next, choose a Replace Option to indicate what you want to happen if duplicates are encountered. An item in the archive file is considered a duplicate if the values for all of its table's primary key fields match a record in the table itself.

The options available are:

- *Add non-duplicates only* – only items in the archive file that do not match records in the table will be imported; any duplicates will be ignored.
- *Import all, replacing duplicates* – all items in the archive file will be imported; if any duplicates are found, the corresponding record in the table will be replaced with the values in the archive file.
- *Replace the entire table* – all records will be removed from the table first; then all of the records in the archive file will be imported.

Once you have made your selections, choose the Import Archive button. You will then be asked for confirmation. For most tables, you can choose Continue or Cancel.

For some tables, you may see the Confirm Archive Import dialog. This will give you a more detailed information about how duplicates will be handled for this table. This is may be because this table is handled differently. It may also be simply because this table contains especially sensitive data, and you need to be sure of the action that you are about to take. Please note this information carefully before proceeding. Then choose either Import Archive or Cancel to complete the import process.



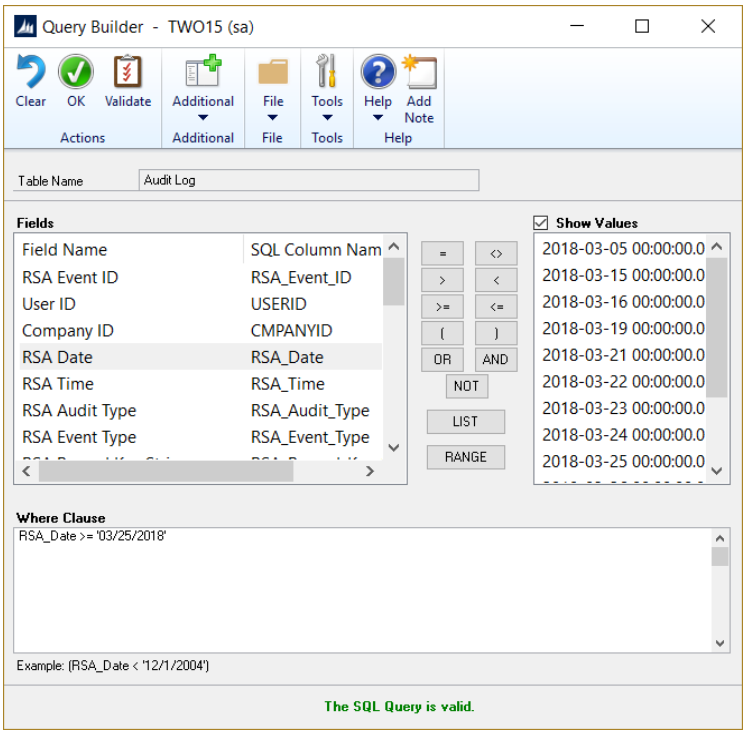
You can use the Auditor Options window to notify Auditor Administrators when a specified size threshold is reached for the Audit Log table.

If a user is in the AUDITOR AUDITORS security role, they will not have access to the Auditor Table Archive / Purge window. This is true even if the user is also in the POWERUSER or any other security role.

After purging or importing an archive, an Audit will be written to track that this action has occurred. The audit will be of type Table Audit and will show the Criteria used when the action was processed. The Note field will state that the audit is for a purge or import event.

Query Builder

This window builds a query that will filter the records that you want to purge or archive.



In general, you will start by double-clicking a field in the Fields list box at the left. This will add that field's SQL name to the Where Clause box at the bottom (this is the query you are building). Next, choose an operator button between the Fields and Values list boxes. Finally, you will either double-click a value in the Values list box to add it to the query, or just type a value into the query.

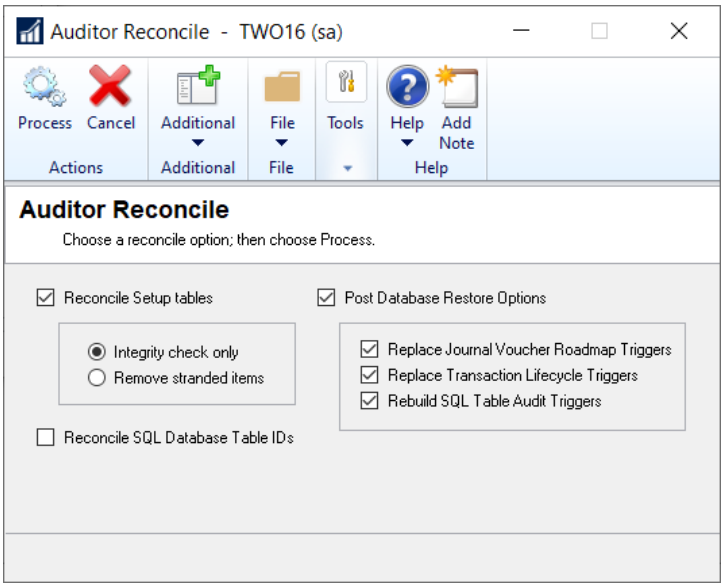
The List and Range buttons will prompt you with instructions for using those operators.

You may either use the method above, or simply type a SQL where clause manually. You can then click the Validate button to make sure your syntax is correct.

If you need additional help with this feature, please contact Rockton Software or your reseller for support.

Auditor Reconcile window

This window allows you to run a process that will ensure the integrity of your audit setups.



To access this window, open Auditor Setup, then choose the Reconcile task from the Setup tab.

Description

The Auditor Reconcile window should be used to ensure the integrity of Auditor's setups. Rockton Support may ask you to run this process. Or you may want to run this process periodically as part of regular system maintenance, as you might run any other reconcile.

Setup tables

You will be prompted to run this reconcile errors are found after exiting the Group Maintenance window. This will ensure that all records in the tables involved in setting up each type of audit have the expected references to records in other tables. If they do not, you will see each discrepancy listed on a report along with whatever action was taken.

There are two options: *Integrity check only*, which will show a list of all discrepancies, and *Resolve stranded items*, which will remove or correct any discrepancies along with showing you the report.

Post Database Restore Options

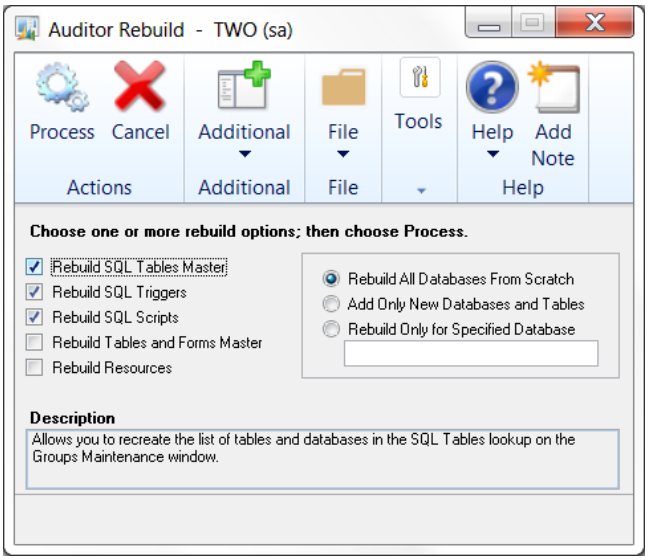
Use these options after restoring a company database from a backup that was made from another database. This will usually happen when restoring a production company's backup into a test company's database. Using these reconcile options will ensure that the company database you are restoring to has no extraneous triggers from the original company's database. It will also rebuild any necessary triggers for the test database.

SQL Database Table IDs

Run this reconcile whenever you recreate a SQL database or a table within a database. This may happen when restoring a database or table from a backup, or when reinstalling your databases due to upgrading hardware. In other words, if the internal ID has changed for a database or table on your SQL Server, then you should run this reconcile. This will make sure that all of these IDs are synchronized with your Auditor setups.

Auditor Rebuild window

This window allows you to rebuild system tables or SQL objects.



To access this window, open Auditor Setup, then choose Rebuild from the Troubleshooting tab.

Description

When you install Auditor with E-Sign, several system tables that are required for most functions of the system are built. Many of these tables contain resource information such as window, table, and field names. Occasionally, these tables may become outdated, especially if you have added or removed integrating products from your Dynamics GP system. In these cases you may find it helpful to rebuild these tables.

In addition to these resource tables, you may also find it necessary or helpful to rebuild the SQL Triggers that are automatically created by setting up SQL Table audits. There are also some other SQL objects (stored procedures and functions) that can be recreated here, in case they have been accidentally deleted or modified.

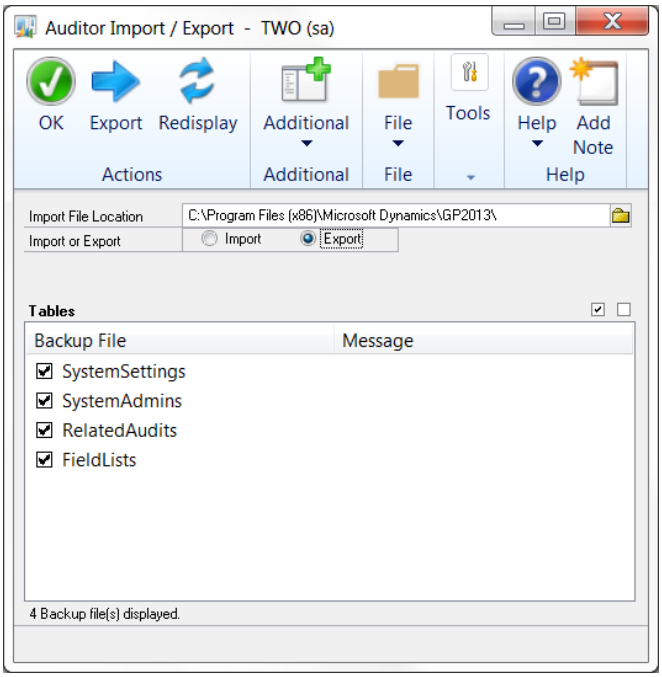
The following table describes each of the rebuild options:

Rebuild Option	Description
Rebuild SQL Tables Master	Allows you to recreate the list of tables and databases in the SQL Tables lookup on the Groups Maintenance window.
Rebuild SQL Triggers	Drops and re-creates all SQL Triggers associated with SQL Table audits that you have defined.
Rebuild SQL Scripts	Drops and re-creates all SQL stored procedures and functions for Auditor, as well as SQL Triggers for the Journal Voucher Roadmap and Transaction Lifecycle windows.
Rebuild Tables and Forms Master	Allows you to recreate the list of tables and forms used in the lookups on the Groups Maintenance window.
Rebuild Resources	Rebuilds the resource table used by the Segregation of Duties calculation process.

If a user is in the AUDITOR AUDITORS security role, they will not have access to the Auditor Rebuild window. This is true even if the user is also in the POWERUSER or any other security role.

Auditor Import / Export window

This window allows you import or export data from Auditor.



You can access this window by first opening the Auditor Setup window, then choosing the Import / Export task from the Setup tab.

Description

The Import / Export window can be used to transfer data in and out of Auditor. At this time, only a select group of tables is available to import or export.

The naming convention used for the export or import files is as follows:

RSA_BACKUP_<*table-name*>.xml

where <*table-name*> is the name that shows in the Tables list, but with underscores in place of spaces.

Exporting data

Tables will be exported in XML format. The export file will consist of all records in the selected table.

To export one or more tables:

1. Select or enter the location of the folder where you want the export files to be created.
2. Select the Export radio button in the 'Import or Export' radio group.
3. Mark the table or tables that you want to export. Note that you can use the Mark All and Unmark All buttons to the upper-right of the Tables list.
4. Click the Export button.

Once the Export completes, the record count for each exported table will show in the Tables list.

Importing data

When you import an XML file in this format, you will see a Replace Option radio button group. The options available are:

- **Add new records only** – this will ignore any duplicates that are found
- **Delete existing records, then import** – this will remove all records from the table you are importing into first. In effect, you will be replacing the contents of the table with what is in the XML file you are importing.

To import one or more tables:

1. Select or enter the location of the folder that contains the XML files to be imported.
2. Select the Import radio button in the 'Import or Export' radio group.
3. Select the desired option from the 'Replace Option' radio group.
4. Mark the table or tables that you want to import. Note that you can use the Mark All and Unmark All buttons to the upper-right of the Tables list.
5. Click the Import button.

Once the Import completes, the record count for each imported table will show in the Tables list. If you have chosen **Add new records only** from the 'Replace Option' radio group, then you will see a count of the records added along with a count of the duplicates that were found, if there were any, for each table selected.

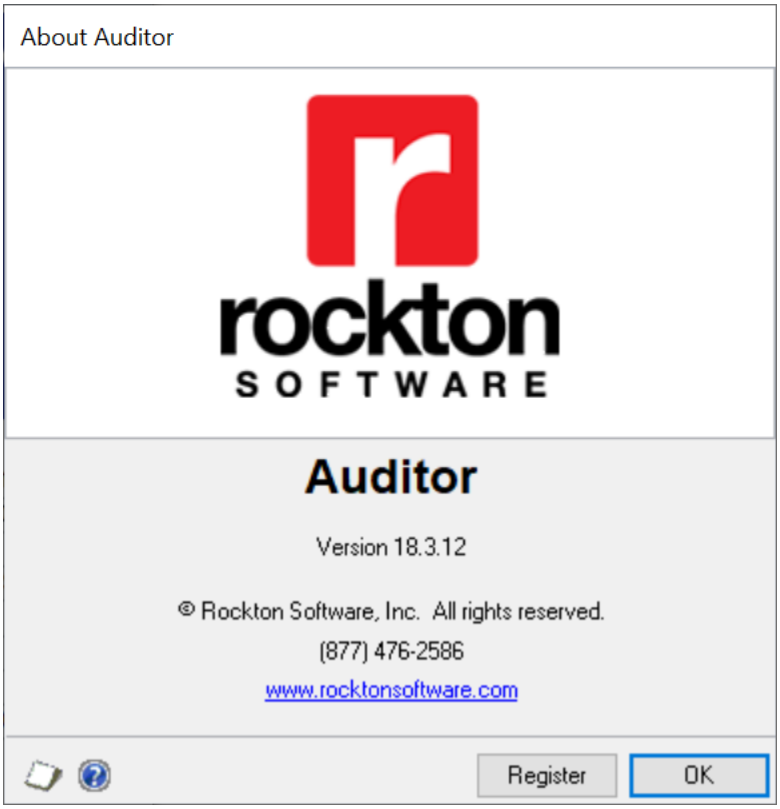
If a user is in the AUDITOR AUDITORS security role, they will not have access to the Auditor Import / Export window. This is true even if the user is also in the POWERUSER or any other security role.

Rockton Support and Troubleshooting

Overview

The windows in this section may be useful if you ever need to open a case with Rockton Software Support. We will give you specific instructions for accessing and using these windows if we need this information to assist in troubleshooting your issue.

About Auditor window



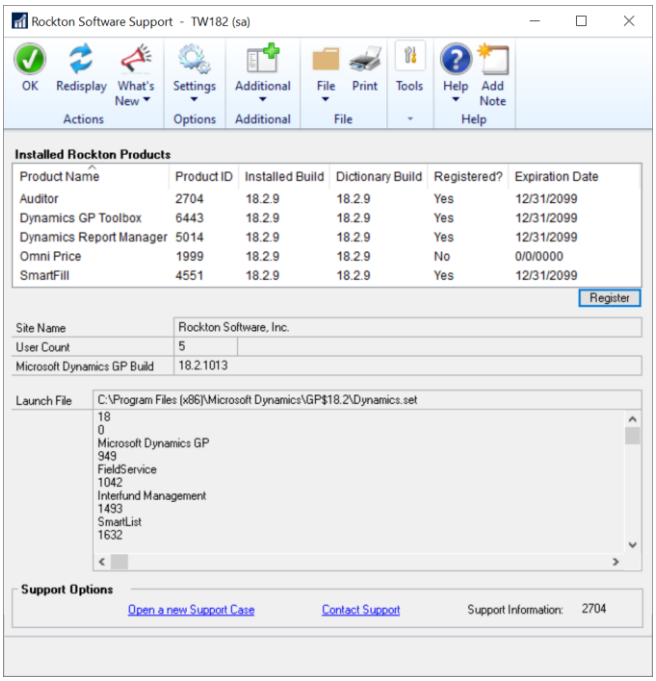
This window is accessible in one of two ways:

- From the Navigation Pane.
- Go to Help > About Microsoft Dynamics GP … From the Additional menu on this window, choose About Auditor.

Description

The About Auditor window shows the version of Auditor that you have loaded, along with the phone number to use to contact Rockton Software, and a link to our website. In addition, it also provides a convenient means of navigating to the Auditor Registration window.

Rockton Software Support window



This window can be opened by clicking the Help icon ( ) and then choosing Rockton Software Support from the drop-list.

Description

This window will mostly be used by Rockton Support to get some high-level information about your system to assist in troubleshooting problems. You may also find some of the information presented here to be useful in your own troubleshooting.

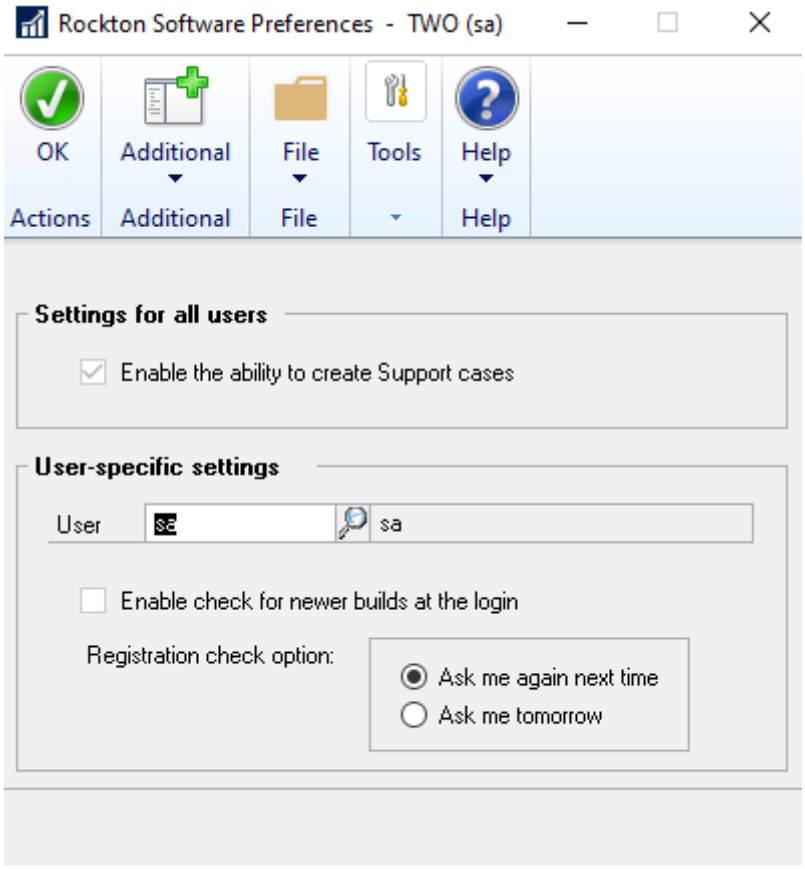
Clicking the What's New button will drop-down a list of the Rockton products that you currently have installed which also have What's New documents available. From this list, you can choose the product for which you want to see a list of new features in this build.

The Installed Rockton Products section will show you your registration information. The Installed Build displays the version in the setup table. The Dictionary Build displays the version installed on the workstation. You can also see if the product is registered and when the registration is set to expire.

If a product shows as not registered, select that product and then click the Register button to automatically attempt to register your products. If no registration exists, contact Rockton Software to resolve your registration issue.

Another important feature of the Rockton Software Support window is the Support Options section at the bottom of the window. You can create a support case by clicking the **Open a new Support Case** link. This will open a browser window that will take you to the Rockton Software Partner Portal, where you can enter details of your problem. Or, if you wish to speak to someone in support first, or do your own research about your situation, you can click the **Contact Support** link and your Internet browser will be opened to our Technical Support page. Here, you will find various options for support including Manuals, FAQs, How-To Videos, Support contact information as well as other options. You can also see the Controlling Product in the **Support Information** field. This information can be helpful to support when troubleshooting.

Rockton Software Preferences window



This window can be opened by clicking the Help icon (), choosing Rockton Software Support from the drop-list, and then clicking Settings and choosing Rockton Software Preferences.

Description

This window is used to assign specific preferences for Rockton Software products. Settings here will apply to all Rockton products you have installed. The window is broken into settings that apply to all users and settings that apply to specific users.

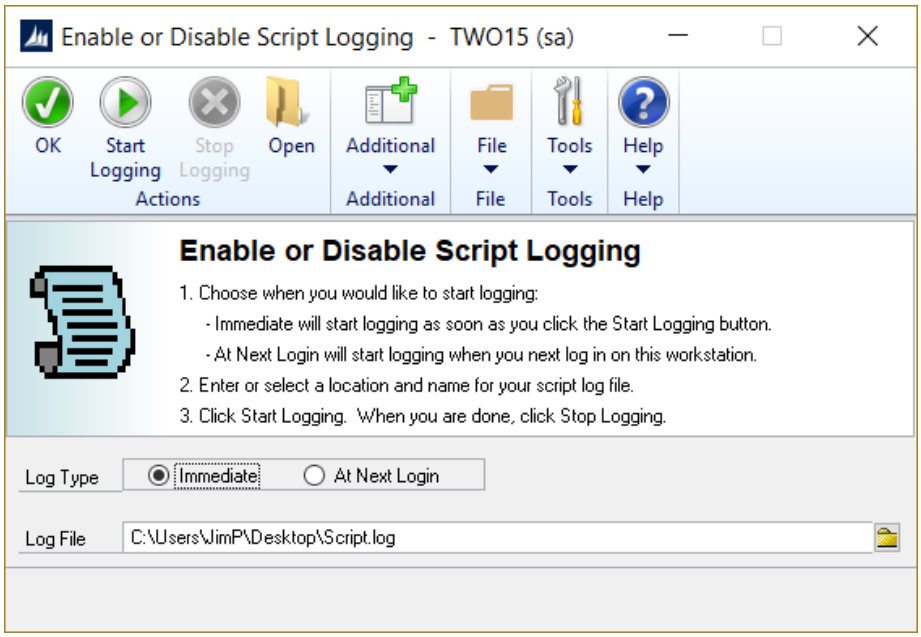
When the Enable the ability to create Support cases check box is marked, users can create a support case from the Rockton Software Support window. When this option is enabled, a hyperlink to Open a new Support Case is available in the Rockton Software Support window.

In the User-specific settings section, you can select a User and then mark the Enable check for newer builds at login. When marked and a user who is an administrator logs in, Rockton will check for any newer builds of the products installed. If the option is unmarked, no checks are made. It is recommended this option be marked for at least on Admin. user.

The Registration check option allows you to choose whether to ask next time or ask tomorrow when looking for registration.

Enable or Disable Script Logging window

Rockton Software Support may request that you use this window to help troubleshoot an issue.



You can get to this window by going to Microsoft Dynamics GP > Tools > Setup > Auditor > Auditor Setup. Then, from the Troubleshooting tab, choose Enable or Disable Script Logging.

Description

The Enable or Disable Script Logging window lets you create a special log file called a “script log”. This may be requested by Rockton Software Support if the case you have reported is a tricky one.

In the past, you would add the line “ScriptDebugger=TRUE” to your Dex.ini file, then log in to GP and use the Debug menu to create a script log. When you were done logging, you would need to set the ScriptDebugger setting to FALSE to suppress the Debug menu. This window lets you perform this task without needed to update the Dex.ini.

When you open the window, you may be asked to restart Dynamics GP. This will happen if the ScriptLogEnhanced Dex.ini setting is not present or is not set to TRUE. The window will add the setting for you, but it will require a restart of Dynamics GP.

You will usually be given detailed instructions for how to use this window by a Support representative, but the general process will be similar to the following:

1. This window requires that You may be prompted to add
2. Select either Immediate or At Next Login for Log Type.
3. Enter or select the name and location of the log file that you are going to create.
4. Perform whatever steps are necessary in Dynamics GP to get to a point immediately before you want to start capturing information in the log file.
5. Click the Start Logging button on this window.
6. Perform the steps that you want to log.
7. Click the Stop Logging button on this window.
8. Click the Open button to view the log file or email it to Rockton Software Support.

Appendix A

Audit Group Export File Format

The Group Maintenance window provides an Export capability that will create a text file containing the setup information for that Audit Group. This file can then be used to import this Audit Group information at this same or another site.

Note: Some data elements in the Export file contain the Database Name. So if you plan to Export into a different company, then you will need to edit this file and change all references to the Database Name to the appropriate value.

Each record in the Export file contains one data element, so there are no delimiters. The following diagram describes the general layout of the Export file:

< Group Definition >
    < Group Master Definition: RSAS019 >

< Group Table Master Definition: RSAS023 >

[Table Definitions – one set per Table Audit]
    < Table Master Definition: RSAS001 >
    < Table Primary Key Master Definition: RSAS009 >
    < Table Field Master Definition: RSAS002 >
    < Field Options Master Definition: RSAS024 >
    < Field Mappings Master Definition: RSAS025 >

< Group SQL Table Master Definition: RSAS028 >

[SQL Table Definitions – one set per SQL Table Audit]
    < SQL Table Master Definition: RSAS026 >
    < SQL Table Primary Key Master Definition: RSAS029 >
    < SQL Table Column Master Definition: RSAS027 >

< Group Form Master Definition: RSAS022 >

[Form Definitions – one set per Form Audit]
    < Form Master Definition: RSAS011 >
    < Window Field Master Definition: RSAS010 >
    < Field Options Master Definition: RSAS024 >
    < Field Mappings Master Definition: RSAS016 >

Table definitions (enclosed in < > in the above diagram) will have the following format:

Table Name
Number of Fields
Number of Records
Field Name { one per Field in this Table }

[Record Data – one set per record in this Table]
    Field Value { one per Field in this Table }

Appendix B

Typical Archive XML Format

The Table Archive/Purge window creates an archive XML file containing the information in the selected table. The format of that XML file for most tables is as follows:

<*TablePhysicalName*_ARCHIVE>
    <*TablePhysicalName*>
        <*Column1PhysicalName*>*value*</*Column1PhysicalName*>
        <*Column2PhysicalName*>*value*</*Column2PhysicalName*>
        etc.
    </*TablePhysicalName*>
</*TablePhysicalName*_ARCHIVE>

Audit Log Archive XML Format

The Audit Log is composed of two separate tables: RSA Audit Log Master (RSAS015) and RSA Audit Log Reference Master (RSAS031). The XML archive file created is as follows:

<RSAS015_ARCHIVE>
    <RSAS015>
        <*Column1PhysicalName*>*value*</*Column1PhysicalName*>
        <*Column2PhysicalName*>*value*</*Column2PhysicalName*>
        etc.
        <RSAS031_ARCHIVE>
            <*Column1PhysicalName*>*value*</*Column1PhysicalName*>
            <*Column2PhysicalName*>*value*</*Column2PhysicalName*>
            etc.
        </RSAS031_ARCHIVE>
    </RSAS015>
</RSAS015_ARCHIVE>

Approval Log Archive XML Format

The Approval Log is composed of two separate tables: RSES Approval Log Master (RSAS039) and RSES Approval Log Ref Master (RSAS044). The XML archive file created is as follows:

<RSAS039_ARCHIVE>
    <RSAS039>
        <*Column1PhysicalName*>*value*</*Column1PhysicalName*>
        <*Column2PhysicalName*>*value*</*Column2PhysicalName*>
        etc.
        <RSAS044_ARCHIVE>
            <*Column1PhysicalName*>*value*</*Column1PhysicalName*>
            <*Column2PhysicalName*>*value*</*Column2PhysicalName*>
            etc.
        </RSAS044_ARCHIVE>
    </RSAS039>
</RSAS039_ARCHIVE>

Appendix C

Example: Setting Up Related Audits

The following is a step by step example of how to enter setups so that you can view Checkbook audits from the Checkbook Maintenance window.

Setting up an Audit Group

In order to have audit data to view, we must first set up an Audit Group to log changes to Checkbook data. An Audit Group defines which form, table, or SQL table that we want to be audited when data is changed. In this example, we want to audit changes to the data in the Checkbook Master table. We will use a SQL table audit to do this.

1. In Microsoft Dynamics GP, click the Auditor toolbar icon ( ). Then choose Audit Groups.
2. In the Group Maintenance window, enter BANKING as the Group ID and Group Description.
3. Click the Add Audit button (+) and choose SQL Table Audit from the drop-list.
4. Since we want to create an audit on the Checkbook Master, type CM00100 in the Search field and then choose either the Enter or tab key.
5. From the results, highlight the CM00100 for the TWO database and then click the Select button.
6. In the Auditor SQL Table Maintenance window, we need to setup what options and fields we want to audit and receive audit results on. Mark the following three tracking options:
    - Track Adds
    - Track Deletes
    - Track Changes
7. From the Field Names, mark the Audit column checkboxes for the following field names:
    - DSCRIPTN
    - BANKID
    - CURNCYID
    - ACTINDEX
    - NXTCHNUM
    - Next_Deposit_Number
8. Click OK to save those changes.
9. Back on the Group Maintenance window, click Save. Then close the Group Maintenance window.

Setting up a Related Audit

You will now set up a Related Audit so that the audit information captured by the Audit Group defined above can be viewed directly from the Checkbook Maintenance window based on rules that you assign.

1. Go to Cards > Financial > Checkbook.
2. On the Checkbook Maintenance window, go to Additional > View Related Audits.
3. In the View Related Audits window, click the Rules button.
4. In the Related Audit Rules list, highlight Window 'Checkbook Maintenance' and click the Add Rule button (+) to create a new rule for this window.
5. In the Rule Setup window, click the Add Window Field Relationship button (+) to open the Window Field Relationship Setup window.
6. In the Window Field, type or select Checkbook ID.
7. From the Field List, type CHECKBOOK ID and then tab. Choose Yes when prompted to create the Field List.

Setting up a Field List

The Field List defines what variations exist for a field name across the system. For instance, the same field can be named one thing on a window and something entirely different in the physical table on the database. This is what the system will try to match in order to show audits on the View Related Audits window.

1. In the Field List Setup window, type CHEKBKID in the New Field Name box and then click the top Insert button.
2. Type Checkbook ID in the New Field Name box and click this same Insert button again. You will now have two Field Name Variations appearing in the Field List.
3. Click Save to close the Field List Setup window.
4. Click OK to close the Window Field Relationship Setup window.
5. Click Save to close the Rule Setup window.
6. You will now see the Rule that you have created on the Related Audit Rules Setup window.
7. Click OK to close the Related Audit Rules Setup window.
8. Finally, click OK to close the View Related Audits window.

Testing the Audit and Viewing Results

We can now test and verify that our audit information is working correctly by making changes to one of the fields we have chosen to audit from within our Audit Group.

1. Go to Cards > Financial > Checkbook. Select an existing Checkbook from the lookup.
2. In the Description field, enter a new description such as TEST, and then click the Save button. This action should have been saved to the Audit Log.
3. Select that same Checkbook ID again.
4. Go to Additional > View Related Audits. You should now see that the audit that was logged in step 2 is listed on the View Related Audits window.