Auditor
With E-Sign
For Dynamics GP 2010
Documentation dated August 29, 2014

8/29/2014

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.

7. BUSINESS OBJECTS LICENSING: You accept responsibility for complying with the licensing of the Crystal Report royalty-free runtime modules. Although they are installed by Rockton Software, you accept responsibility for determining if your site or environment can legally utilize the components by consulting with Business Objects or the current owner of Crystal Reports. Rockton Software is not responsible for licensing any Crystal Report component or software for any purpose related to the use of Auditor by you.

8. USAGE STATISTICS: Rockton Software will collect usage statistics of certain windows or features in this Rockton product. These statistics will be transmitted periodically to Rockton Software for the sole purpose of analyzing feature usage and future development planning. No personal data other than Site Name is attached to these statistics.

Rockton Software Auditor with E-Sign
Table of Contents

Rockton Software Auditor with E-Sign
Table of Contents (cont.)

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.

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: • Microsoft Windows Server 2012 x64 Essentials Edition or Standard Edition (requires Dynamics GP 2010 SP3) • Microsoft Windows Small Business Server 2011 Standard Edition with Premium Add-on • Microsoft Windows Server 2008 R2 x64 Standard Edition • Microsoft Windows Server 2008 Standard Edition SP 2 or later • Microsoft Windows Small Business Server 2008 Premium Edition SP 2 or later • Microsoft Windows Server 2003 R2 Standard Edition • Microsoft Windows Server 2003 Standard Edition SP 2 or later • Microsoft Windows Small Business Server 2003 R2 Premium Edition • Microsoft Windows Small Business Server 2003 Premium Edition SP 2 or later • Microsoft Windows Small Business Server 2003 R2 x32 Standard Edition (SQL 2005/2008 Express ONLY) • Microsoft Windows Small Business Server 2003 x32 Standard Edition SP 2 or later (SQL 2005/2008 Express ONLY)
Client Operating System	One of the following: • Microsoft Windows 8 Professional or Ultimate Editions (requires GP 2010 SP3) • Microsoft Windows 7 Professional or Ultimate Editions • Microsoft Windows Vista Business Edition SP2 or later • Microsoft Windows Vista Ultimate Edition SP2 or later • Microsoft Windows XP Professional SP 3 or later
Processor	1 Dual Core or 1 Single Core Processor 2.6 GHz or higher
Available hard disk space	5 Meg in the Dynamics GP install folder; 5 Meg in the DYNAMICS database
Minimum available RAM	2 GB (more recommended)
Microsoft SQL Server	One of the following: • Microsoft SQL Server 2012 - Standard or Express Editions (requires Hotfix KB 2654242 Version 11.00.1914 or later for Microsoft Dynamics GP 2010) • Microsoft SQL Server 2008 R2 - Standard, Workgroup or Express Editions • Microsoft SQL Server 2008 SP 1 or later - Standard, Workgroup or Express Editions • Microsoft SQL Server 2005 SP 3 or later - Standard, Workgroup or Express Editions
Microsoft Dynamics GP	One of the following: • Version 2010 with or without SP1, SP2, or SP3
Adobe	Adobe XI, X, 9.0, 8.0, 7.0, or 6.0

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, run the Auditor setup file (**AuditorSetup.exe)**.

   ! *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 window 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 the **Audit.cnk** file 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.

   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.

This completes 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 don't have a registration key, we recommend that you log into the Dynamics GP lesson company.

> ⚠ *If you are evaluating the software and do not yet have a registration key, this product will only work in the Dynamics GP lesson company. To obtain a registration key, 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.
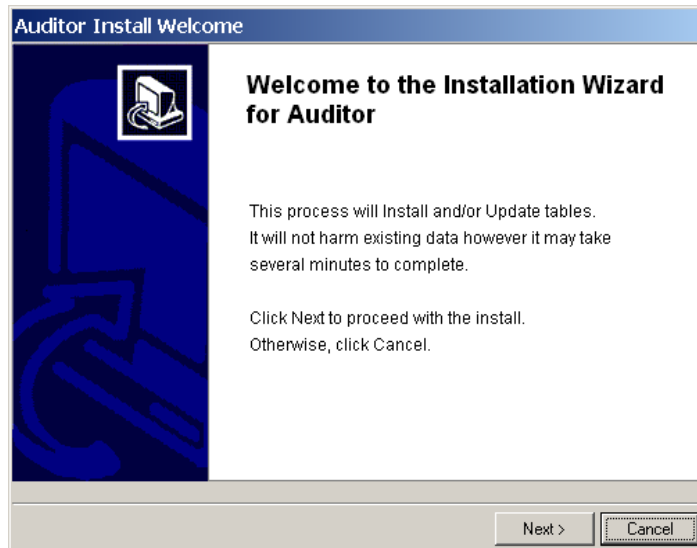
5. Click the Next button to review the License Agreement.

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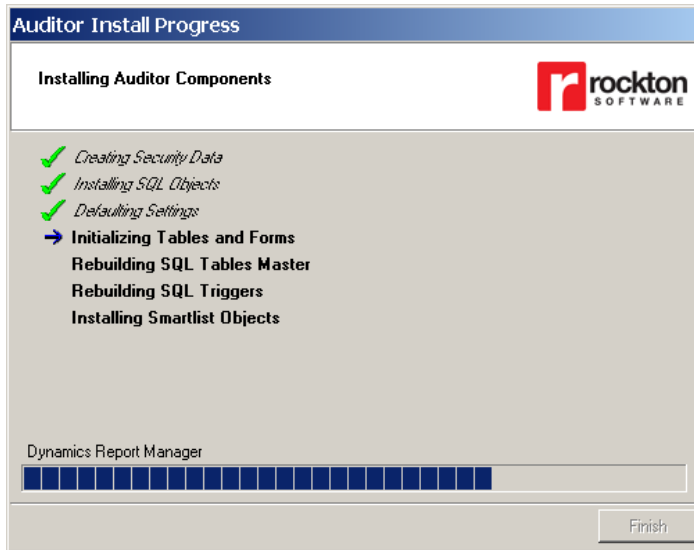
7. If you have Security Auditor installed and have Security Audits logged or you have created Segregation of Duties Groups, you will be allowed to Import from Security Auditor into Auditor at the end of the install.

⚠ *Security Auditor must be on at least version 10.0 to import the Security Audit Log and Segregation of Duties Groups. If you are on an earlier version of that product, you must first upgrade before using the import.*

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 entered a valid registration key, the following window will open:
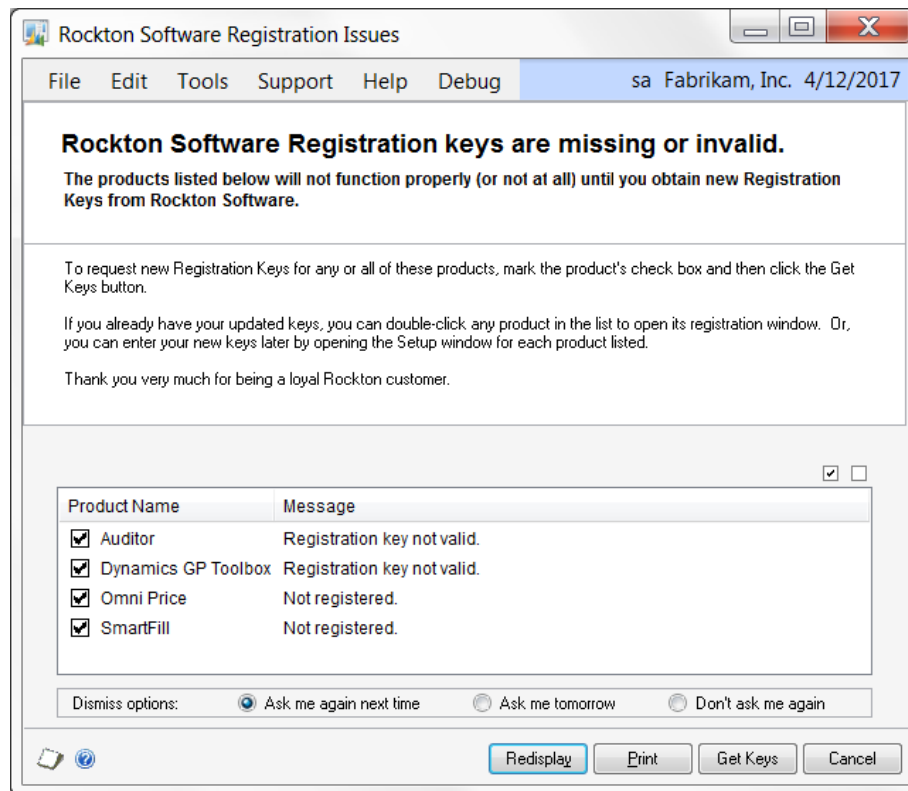
This will show any Rockton products that are not currently registered. If you wish, you can click the Get Keys button to have your registration keys loaded automatically.

If you wish to enter your registration keys manually, you can do so on the Auditor Setup window. Choose the Registration task and the Auditor Registration window will open. Carefully enter the Registration Key and press the OK Button.

10. In some cases, you may see this window:
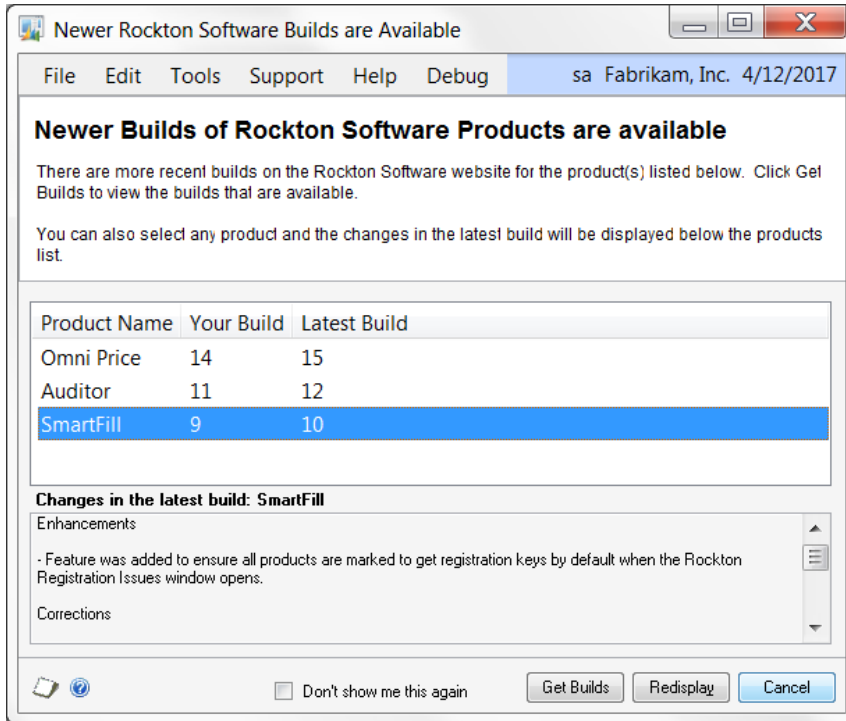
This will show any installed Rockton products for which there are newer builds available on our website. Click Get Builds to download and install any updates.

⚠ *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.*

This completes the installation process for the first workstation.

Auditor Security Settings

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

- AUDITOR ADMIN Security Role

  Used to set access to an Administrator of Auditor

- ADMIN_AUDITOR_01 Security Task

  Contains all windows necessary to setup and administer Auditor. Typical Users do not need to have access to these windows.

- DEFAULTUSER Security 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.

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 ReadMe.txt   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 ReadMe.txt   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 the rsaLogAudit and rsaUpdateMessageCenter stored procedures, which are located in the DYNAMICS database.
5. Drop the rsaDatabaseTableID scalar function, which is located in the DYNAMICS database.
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.

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.

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 using the procedure described below:

- 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.

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.

System 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 refer to these users as "System Administrators". This may also be abbreviated to Administrators, or just Admins.

Administrators are selected on the System Settings window in Auditor.

An Overview of Auditor

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.

An audit is a 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 has the ability to track so much information, you may want to consider that 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.

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 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 keys 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 keys 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 keys,

You can contact Rockton Software over the Internet to obtain new keys for the products listed. If you do not have any valid registration keys on file for any of the products listed, then you will be given temporary registration keys that will expire in about a month.

To retrieve your reg keys, simply mark the check box for each product that requires new keys, and then click the Get Keys button. This will automatically try to register each product selected. If keys cannot be obtained, you will see a message that indicates there was a problem. You can then click on that message in the list and your Internet browser will open, showing you details of what the problem was and how to resolve it.

You can also view or enter your keys manually by double-clicking each product in the list above. This will open the Registration window for that product.
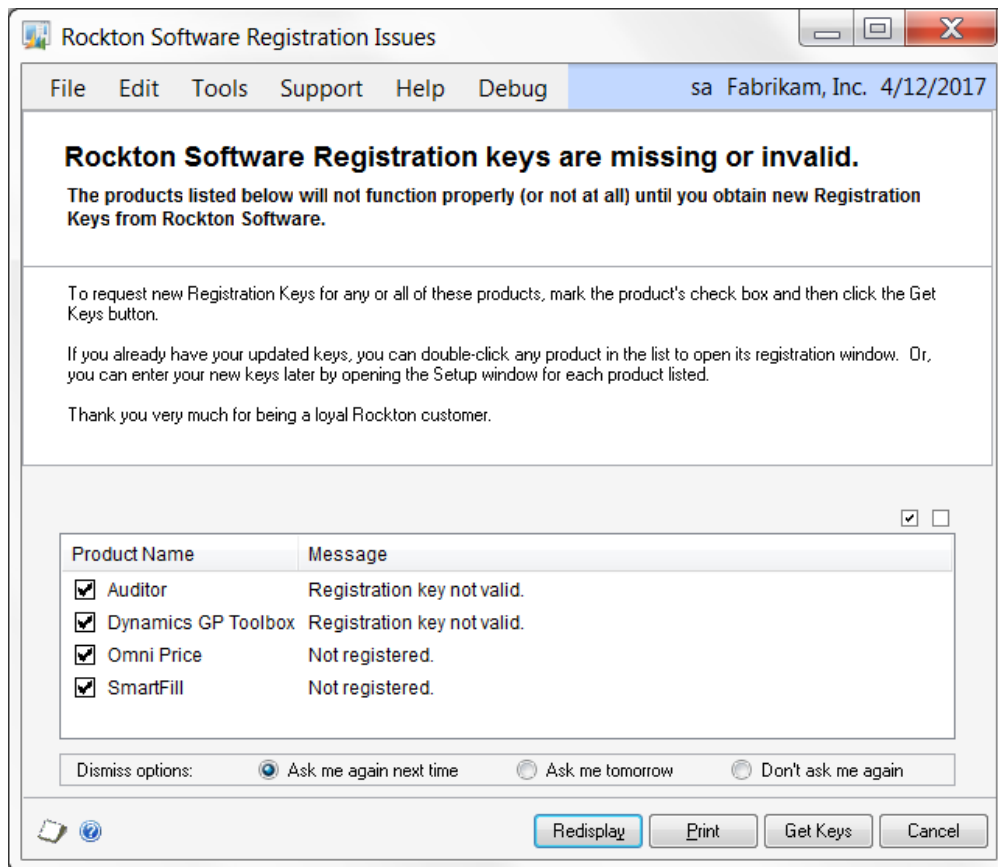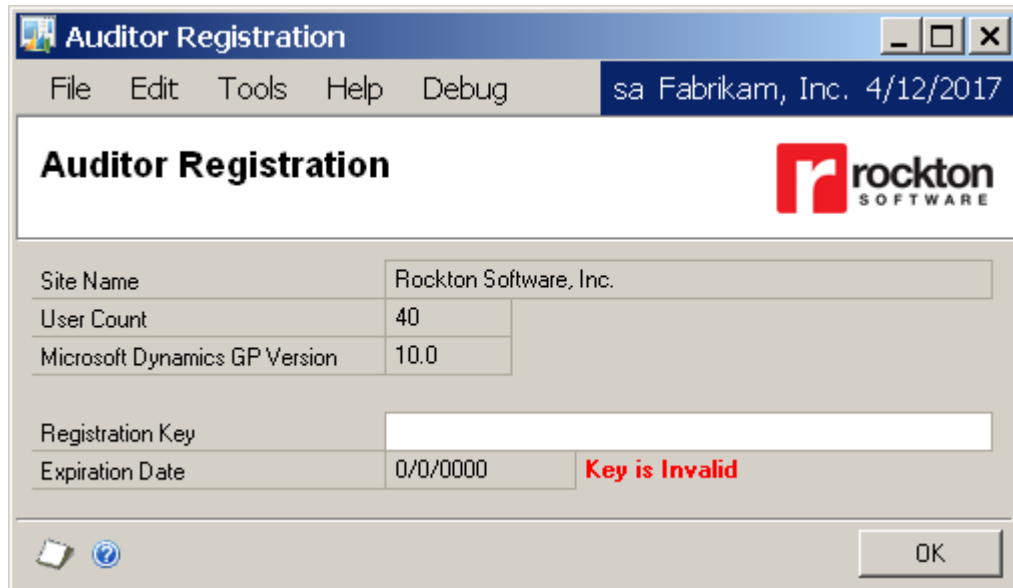
Auditor Registration window


This window is accessible in one of these ways:

- From the Navigation Pane.

- Go to Help > About Microsoft Dynamics GP… From the Extras menu, choose Additional > About Auditor. Then choose 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 choose the Registration task.

Description

The Auditor Registration window is where you enter your Registration Key. After entering your key, just tab off the Registration Key field. If your key is valid, a "Thank You" message will be displayed. If not, you will see the words **Key is Invalid** to the right of the Expiration Date.

If your key is invalid, first verify that you have not mistyped anything. If you received your keys in an email, it may be helpful to copy the keys from the email and paste them into the Registration Key field to avoid typing mistakes. If you still see this message, contact Rockton Support to verify that your Site Name, User Count and Dynamics GP version have not changed since you got your keys. If necessary we will generate new keys and resend them to you.

Newer Rockton Software Builds are Available window
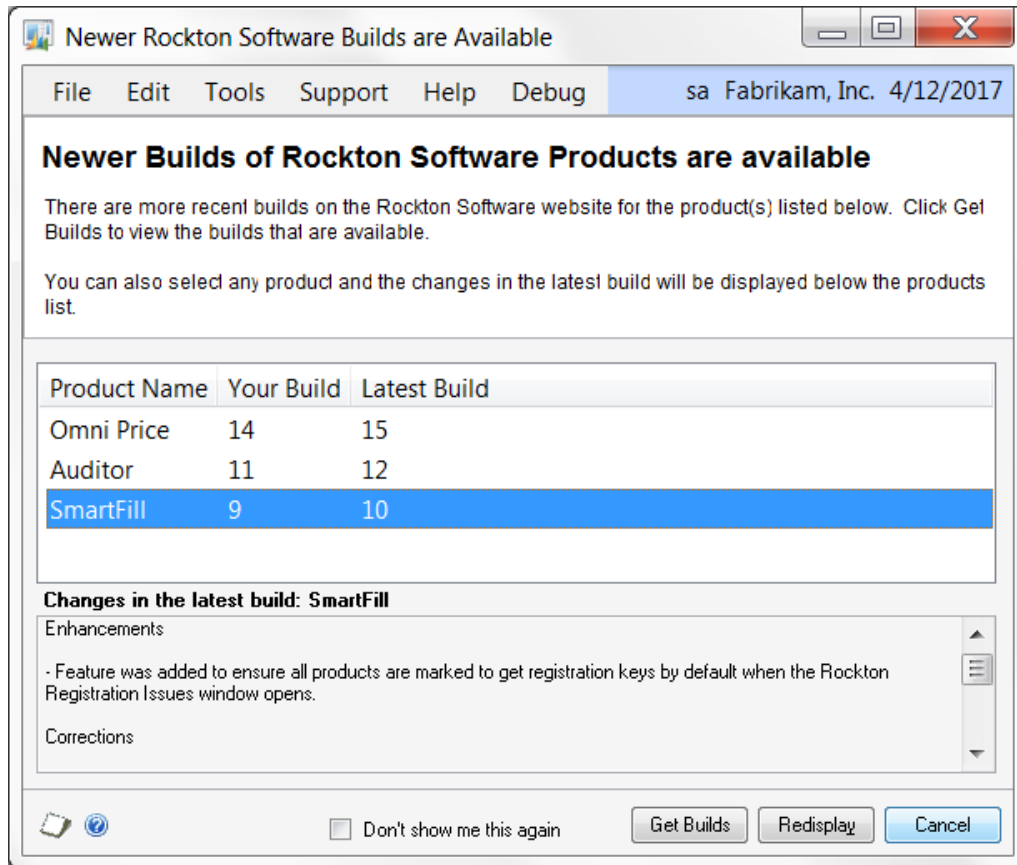
This window opens automatically when a System Administrator logs in if any Rockton products are found to have newer builds available for download on www.rocktonsoftware.com.
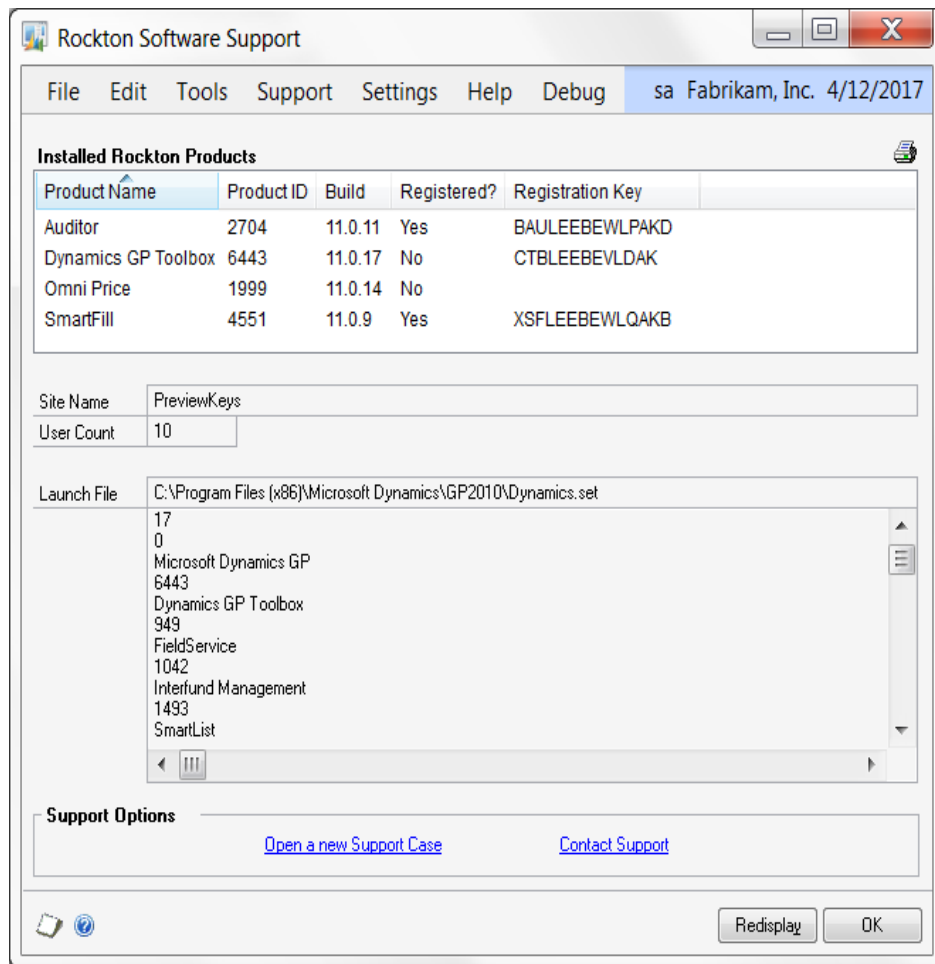
Description

Whenever an 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.

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.

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 over the Internet by clicking the **Open a new Support Case** link. This will open the Create Rockton Support Case window, 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.

Create Rockton Software Support Case window

This window is opened when you click the Open a new Support Case link at the bottom of the Rockton Software Support window.

Description

The Create Rockton Support Case window allows you to instantly open a new support case with Rockton Software. First, select the Product about which you have a question or problem. Then enter the rest of the information requested and click the Create button and your information will be transmitted to Rockton Software via the Internet. You can even include file attachments with the Add Attachment (**+**) button or remove them with the Remove Attachment button (✕).

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.
Audit/Approval Log Maintenance	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 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.
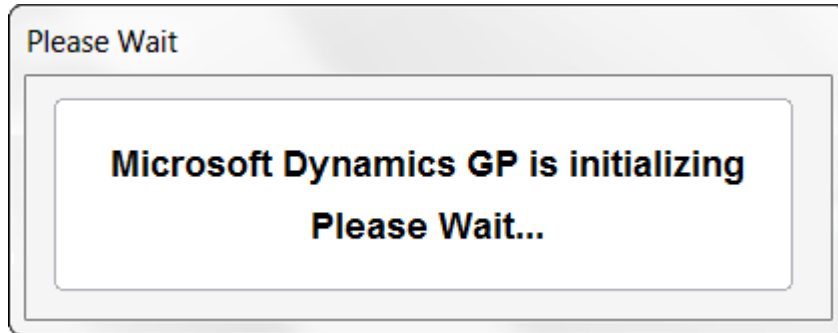
Task	Description
Add or Remove Smartlist Objects	Adds or removes the Audits and E-sign Approvals objects from SmartList.
Rebuild	Opens the Auditor Rebuild window where you can rebuild system tables or SQL objects.
Re-add Security Data	Adds Security Roles and Tasks for Auditor, if they have been deleted. **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.
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.
Debug 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.

Please Wait window

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

Description

The Please Wait window 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 window 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). Once Auditor is through initializing, the Please Wait window will close.

The Please Wait window 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 are equivalent. Therefore the Please Wait window is redundant.

Auditor System Settings window

This window allows you to manage System Administrators and E-Sign Approvers.
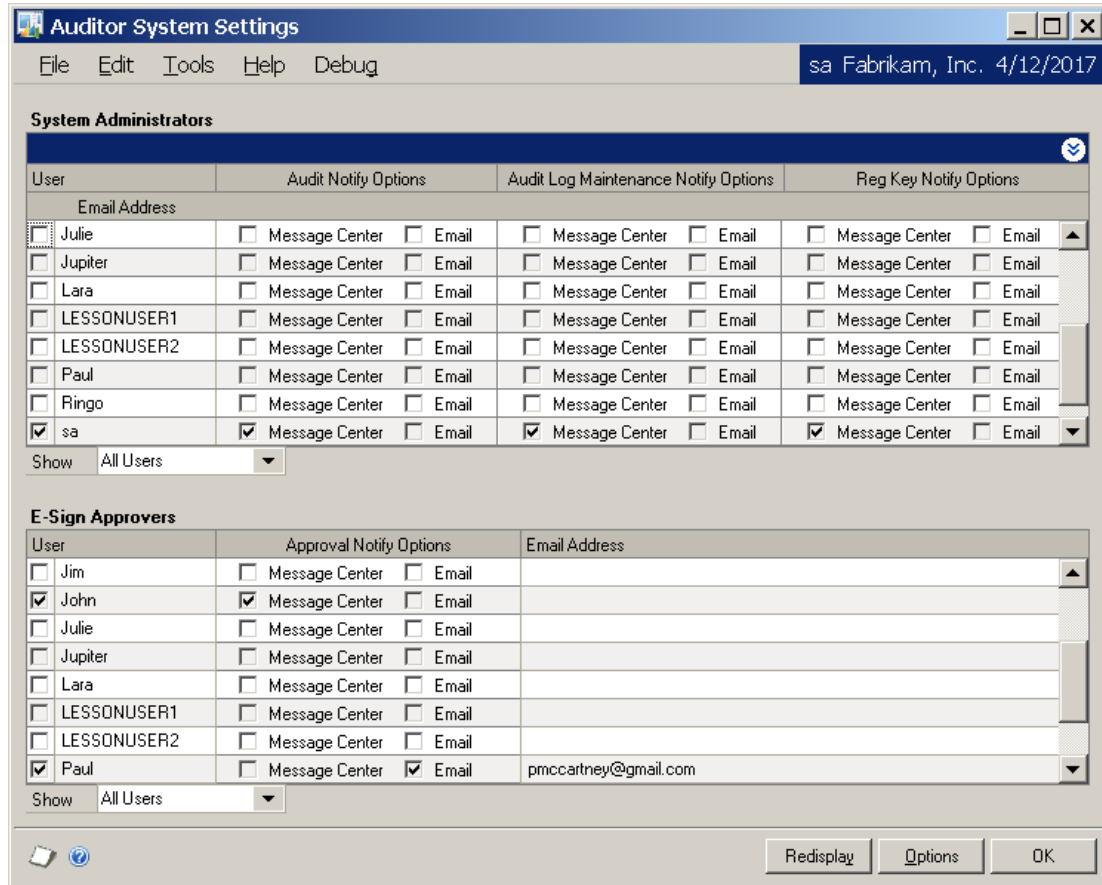
This window is accessible in one of these ways:

- 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 System Settings task.

Description

This window lets you specify which users in your system are System Administrators and which are E-Sign Approvers. System Administrations (or "Sys Admins" for short) can optionally be notified in the Message Center or by Email when certain events occur. E-Sign Approvers are the only Users in the system that can approve or deny changes made to fields that have E-Sign Signatures assigned to them. You can select multiple Sys Admins and E-Sign Approvers. It is OK for a User to be both.

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

> ⚠ *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	When you set up an audit, you have the option of notifying the Sys Admins when that particular audit happens. Selecting one of these options will notify this Sys Admin when these audits occur.
Audit Log Maintenance Notify	When the size of the Audit Log reaches the specified threshold, this Sys Admin will be notified. This notification will be sent to the Message Center only once per day for this Sys Admin.
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 Sys Admin will be notified. This notification will be sent to the Message Center only once per day for this Sys Admin.

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 Sys Admins,

Clicking the Options button opens the Auditor Options window.

Auditor Options window

Audit Log Maintenance Options

"Warn System 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 a System Administrator will, upon logging into Dynamics GP, receive a warning message notifying them that the log has exceeded this limit.

Message Center Options

"Warn System Administrators when Unread Messages exceed the Threshold" – Checking this box will let you specify the maximum number of unread messages in the Message Center before Sys Admins are notified. If this option is checked, any user marked as a Sys Admin 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" – Checking this box will prevent the Notification box that normally appears in the lower-right corner of the Dynamics GP window from being displayed.

"Open Message Center on login…" – This drop-down lists the options for when, or if, the Message Center should open after an 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.

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" – This option will cause 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.

"Do not allow SQL Table audits on SQL system databases" – This option causes the "Rebuild SQL Tables Master" process to skip the master, model and msdb databases. These databases will not show up in the list when you attempt to add a SQL Table audit.

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 System Administrators for all SQL Table audits" – This option controls whether or not a record is written to the Message Center for Sys Admins 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.

Miscellaneous Options

"Allow editing of Audit Notes" **–** This option lets users edit their notes in the Audit Inquiry window. Open the Audit Inquiry window from SmartList by double-clicking an audit. 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 audit is captured.

"Open Access window with Group Maintenance window" **–** This option 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.

Security Audit Options

"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.

It is not recommended to force 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. Doing so could 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. Open the Security Audit Inquiry window from SmartList by double-clicking a security audit. 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.

Import from Security Auditor window

This window allows you to import data and settings from Rockton's Security Auditor product.
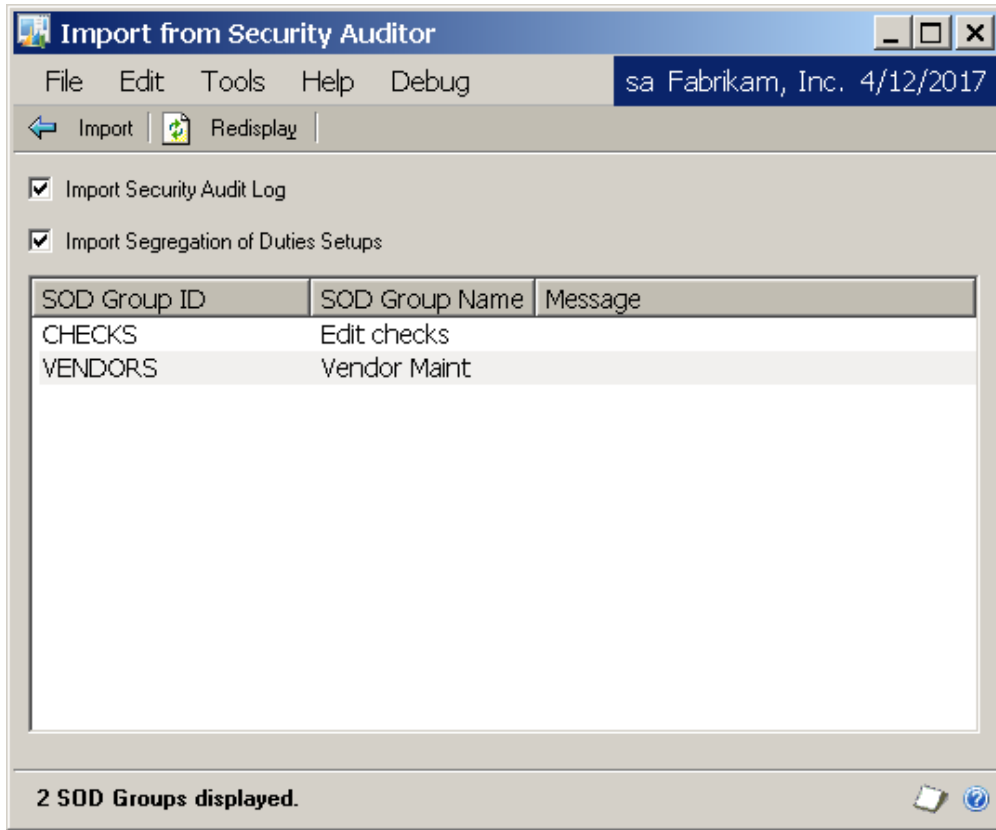
You can access this window by first opening the Auditor Setup window, then choosing the Import from Security Auditor task from the Setup tab.

Description

If you have previously used Rockton's Security Auditor product, then you may have Security Audits logged that you wish to keep. You may also have created Segregation of Duties Groups for that product. You can make these items available in Auditor as well by using the Import from Security Auditor window.

In order for this import process to function correctly, these conditions must be met:

- Five Security Auditor tables (RSSA001, RSSA002, RSSA004, RSSA015 and RSSA023) must exist on the DYNAMICS database
- The version of Security Auditor that is installed must be at least 10.0

Import Security Audit Log – If there are any records in the Security Audit Log table in Security Auditor (RSSA015), then this check box will be available. Check this box to load the contents of the Security Audit Log in Security Auditor into the one in Auditor.

> ⚠ *If you currently have any Security Audits logged in Auditor, then the Event IDs of the imported audits from Security Auditor will be reassigned so that there are no conflicts between the ones in Security Auditor and the ones that you currently have in Auditor.*

Import Segregation of Duties Setups – If there are any records in the Segregation of Duties tables in Security Auditor (RSSA002, RSSA004, RSSA023), then this check box will be available and any SOD Groups that have been defined in Security Auditor will be listed. Check this box to load all Segregation of Duties Groups and Exclusions in Security Auditor into Auditor.

⚠ *If the name of any of the SOD Groups listed matches the name of a SOD Group that has already been created in Auditor, then you will see "SOD Group already on file" in the Message column. You can still import these SOD Groups if you want to, but the SOD Group IDs and associated Exclusion IDs will automatically be made unique by adding a numeric suffix to the end of the name.*

Once you have made your selections, click the Import button and the selected components will be copied to Auditor. When you close this window, you will be presented with the Uninstall Security Auditor window.
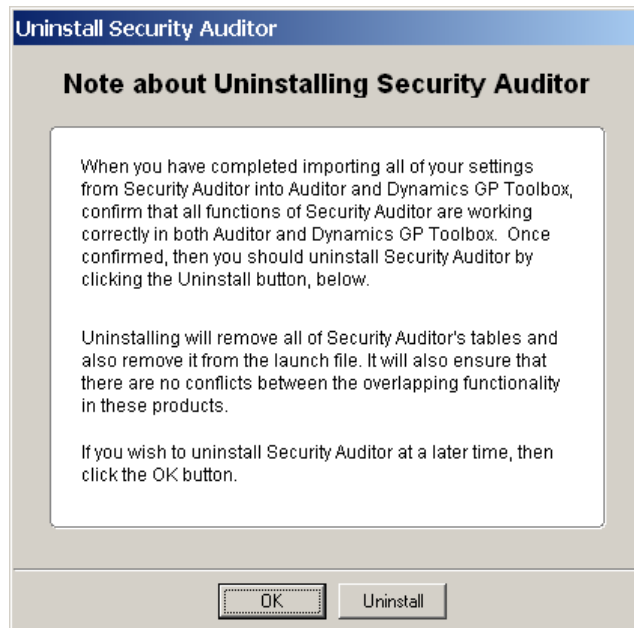
⚠ *All of the features of Rockton's Security Auditor product are now available in the Auditor and Dynamics GP Toolbox products.*

*It is recommended that you uninstall Security Auditor as soon as possible after you have copied over any data and settings into Auditor and, if applicable, Dynamics GP Toolbox. This will prevent any confusion that may occur due to the overlapping functionality between these products.*

If you are ready to uninstall Security Auditor at this time, click the Uninstall button. Otherwise click OK to close this window.

Auditor Import / Export window

This window allows you import or export data from Auditor.
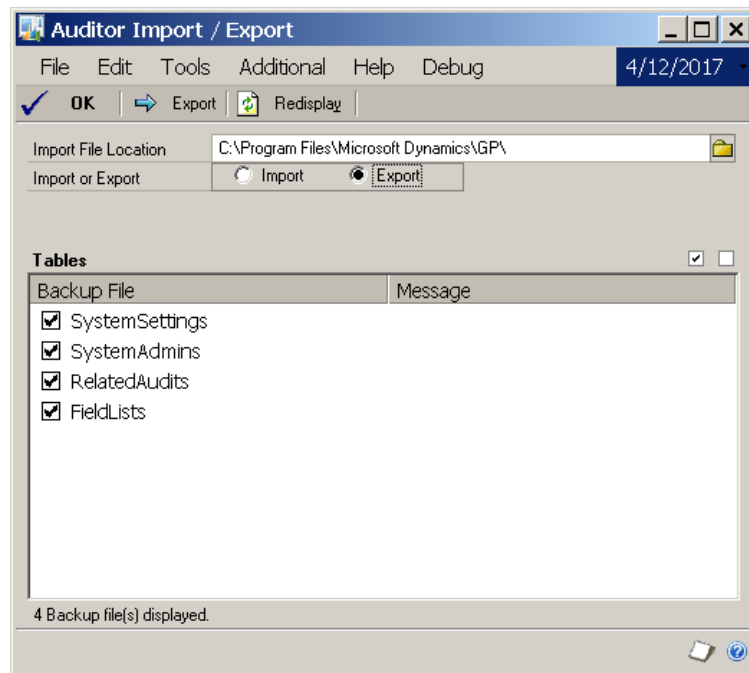
You can access this window by first opening the Auditor Setup window, then choosing the Import / Export task from the Setup tab.

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.

Auditor Rebuild window

This window allows you to rebuild system tables or SQL objects.
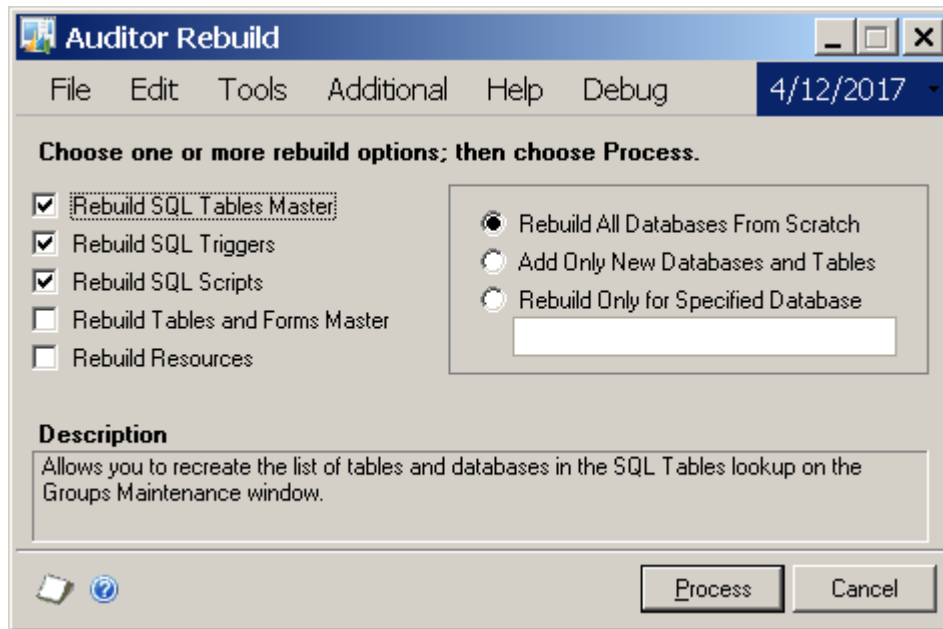
You can access this window by first opening the Auditor Setup window, then choosing the Rebuild task from the Troubleshooting tab.

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.
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.

Group Maintenance window

The Group Maintenance window is the main window from which you set up audits.
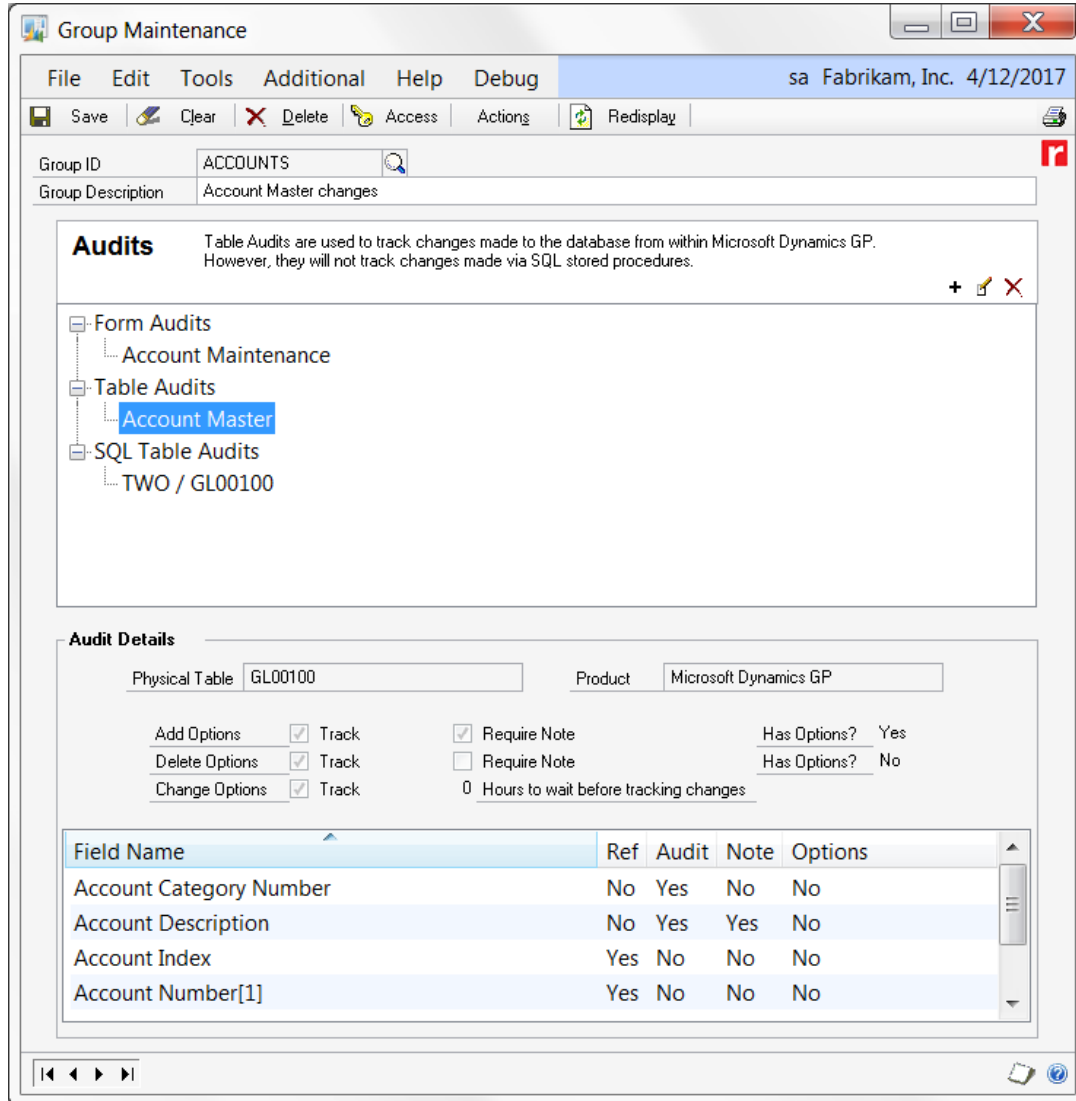
This window can be accessed in one of these ways:

- 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 start when setting up an audit. Audits of similar function or access are collected together in Audit Groups. For instance, you may want to have a Group for Receivables, and another for Payables. You can have an unlimited number of forms or tables in an Audit Group. Once a Group is configured, it can be exported to a text file to be sent to another site to be Imported using this window.

There are three types of audits: Form audits, Table audits and SQL Table audits. **Form** audits are used to track changes made on a Dynamics GP window. **Table** audits are

used when you desire to track changes made at the point that they are saved to the database. **SQL Table** audits also track database changes, but unlike Table audits, they work in 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 as a result of 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 one and 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, described separately later. The Actions button has three items in its drop-list: Import Group, Export Group, and Reconcile. The Reconcile option opens the same Reconcile window that you can access from the Auditor Setup window. The Import and Export options are described in the **Exporting and Importing Audit Groups** section below.

Using the Audits tree

The Audits tree at the top of the Group Maintenance window is where all of your audits are listed for a given Group. Immediately above the tree you will see a description area, which gives you a little bit of information about the audit type that you are currently working with. There are three "icon" buttons to the upper-right of the Audits tree: the Add Audit ✚, Edit Audit 🗹 and Delete Audit ✖ buttons are used to set up the individual audits in a Group.

The Add Audit button contains 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 maintenance window for that audit type will open. At this point, the audit has been added to the current Group. If you simply cancel off the audit's maintenance window, you will see that the audit is now listed in the Audits tree along with a warning icon ⚠. This indicates that you have not entered all of the necessary options for this audit to be considered 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.
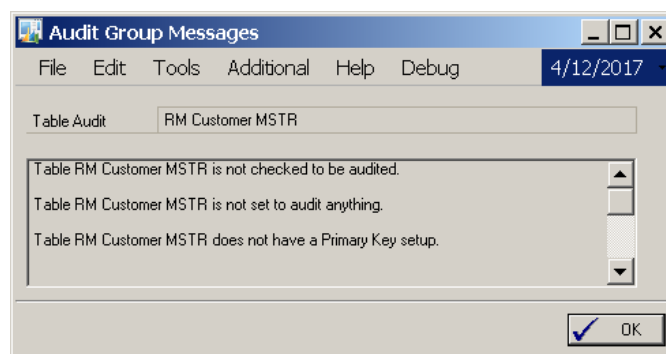
The Edit Audit and Delete Audit buttons require you to first select an audit in the Audits tree. The Edit button is equivalent to double-clicking an audit in the tree.

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.

Exporting and Importing Audit Groups

The Import Group and Export Group options on the Actions Button's drop-list allow you to save Audit Groups that you have set up and then Import them at a later time, or on another system.

To use the Export Group option, first enter or select an existing Audit Group on the Group Maintenance window. Then go to Actions > Export Group. This will open a dialog where you can choose where to save the exported Audit Group. Once you have selected the location of the exported group, and the name of the export file, 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.
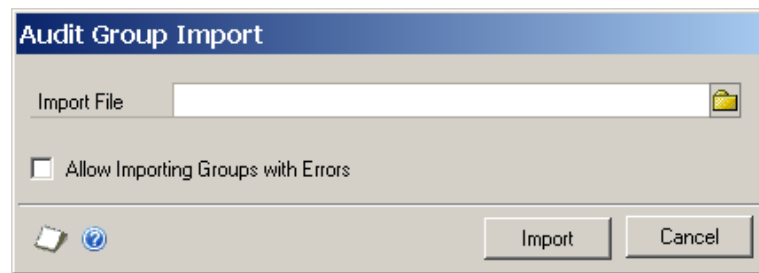
To import a previously exported Audit Group, first enter the Import File name and location, or select it by clicking on the Path button to the right of the Import File field.

Next, decide if you want to import this group whether or not it has errors in it. 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, then parts of that group may not be imported, depending upon whether or not you 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.

Audit Group Access window

The Group Access window lets you select the Users and Companies to which an Audit Group applies.
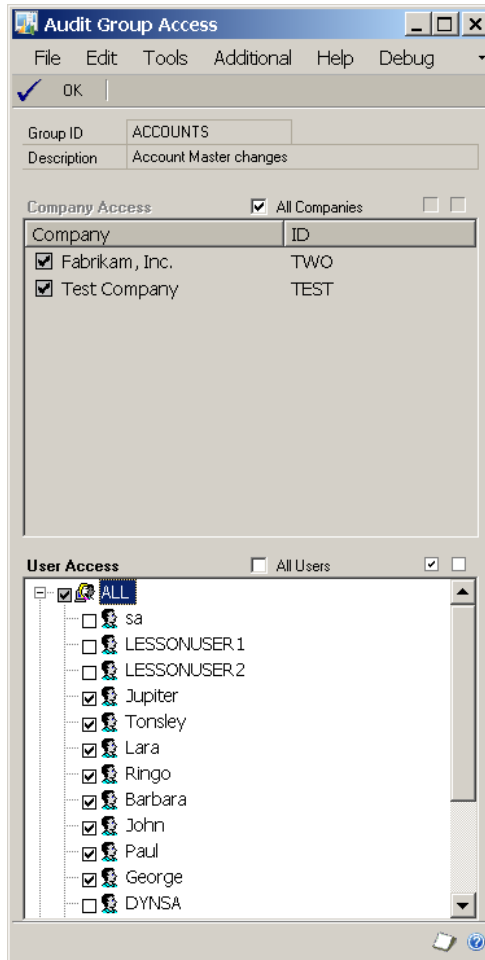
You can access this window in one of two ways:

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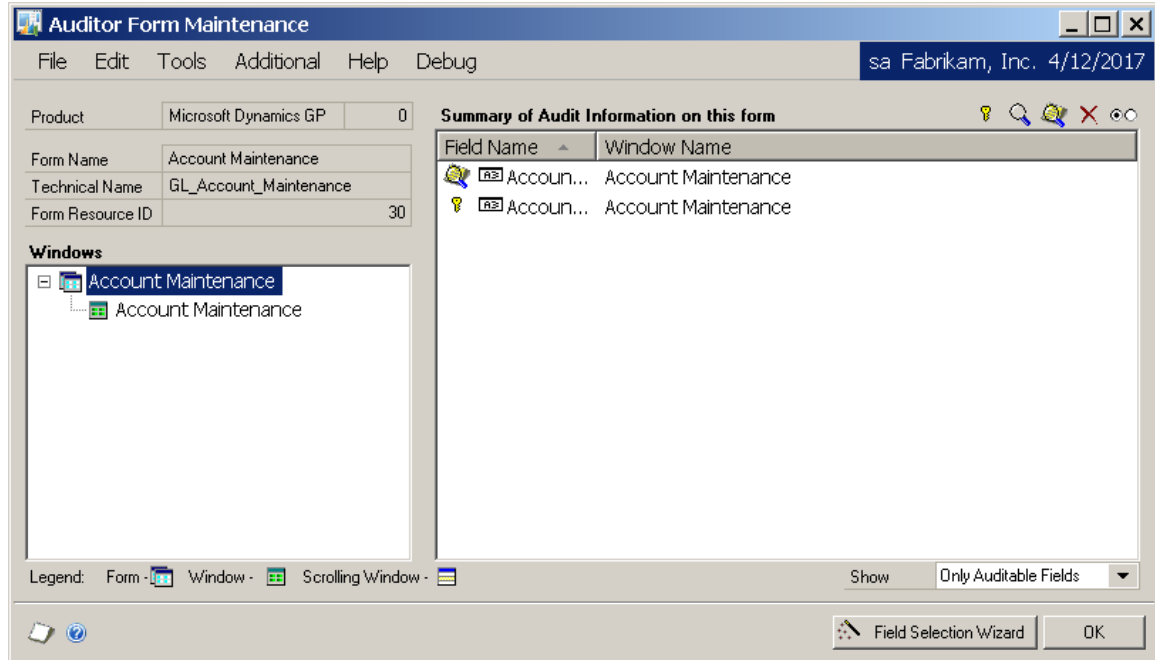
To get to this window, first open the Group Maintenance window. Then double-click one of the forms listed under the **Forms** node in the **Audits** tree.

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.

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.
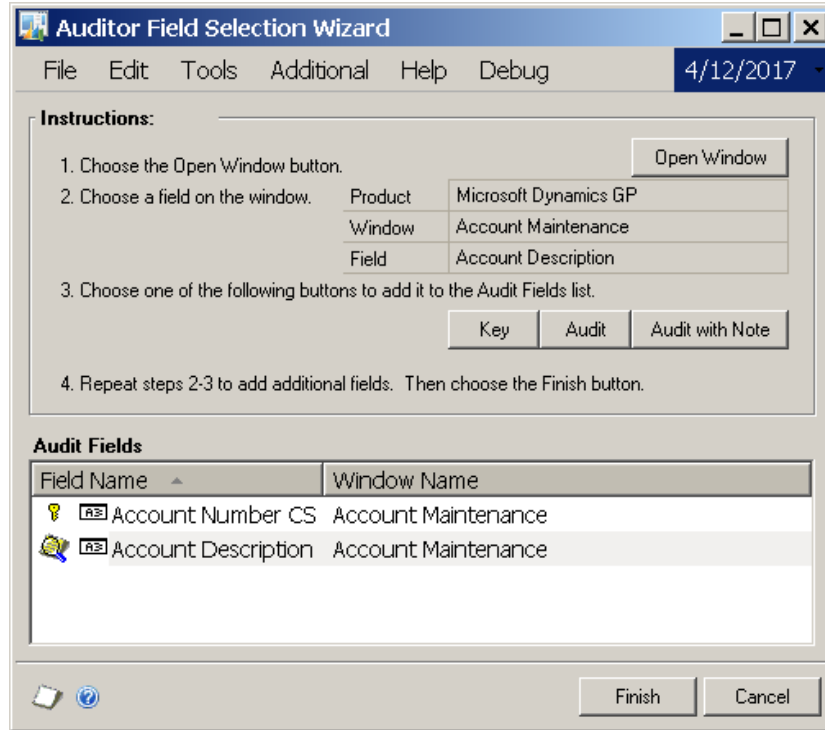
From the Field Selection Wizard window, press the Open Window button to open the window you are auditing. With this window open, click on a field that you want to audit. Notice that Product, Window and Field on the wizard window will change values to show the field that you have clicked.
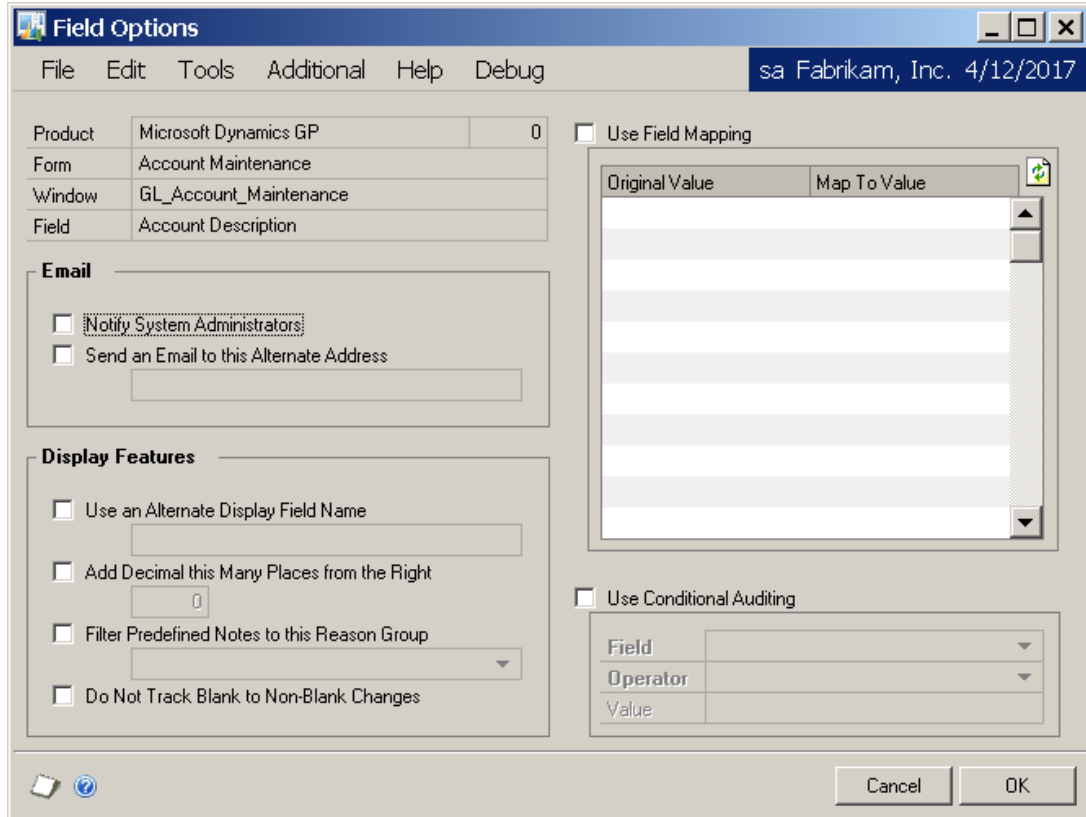
Now, press the Audit or Audit with Note button on the Auditor Field Selection Wizard window. You will see that this field is automatically added to the Audit Fields list. Continue this process until you have selected all of the fields that you want to audit.

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

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:

The following Options are available for auditing:

Option	Description
Notify the System Administrators	Choose this option to send an email to each System Administrators email address (as specified in the System Setting setup window) or to update the Message Center.
Send an Email to this Alternate Address	Choose this option and specify an email address to send a specific person 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, SOP Entry has an SOP Type that when audited appears as the numbers 1 through 5. You can map the value "1" to "Quote" and "2" to "Order" so that the audit log reflects more useful data.
Use Conditional Auditing	Choose this option to make an audit conditional. The condition listed must be true in order for an audit to occur. Specify the comparison field, the operator (equal or not equal) and the string value to compare the field to. If this expression evaluates to true during auditing, and audit will be captured.

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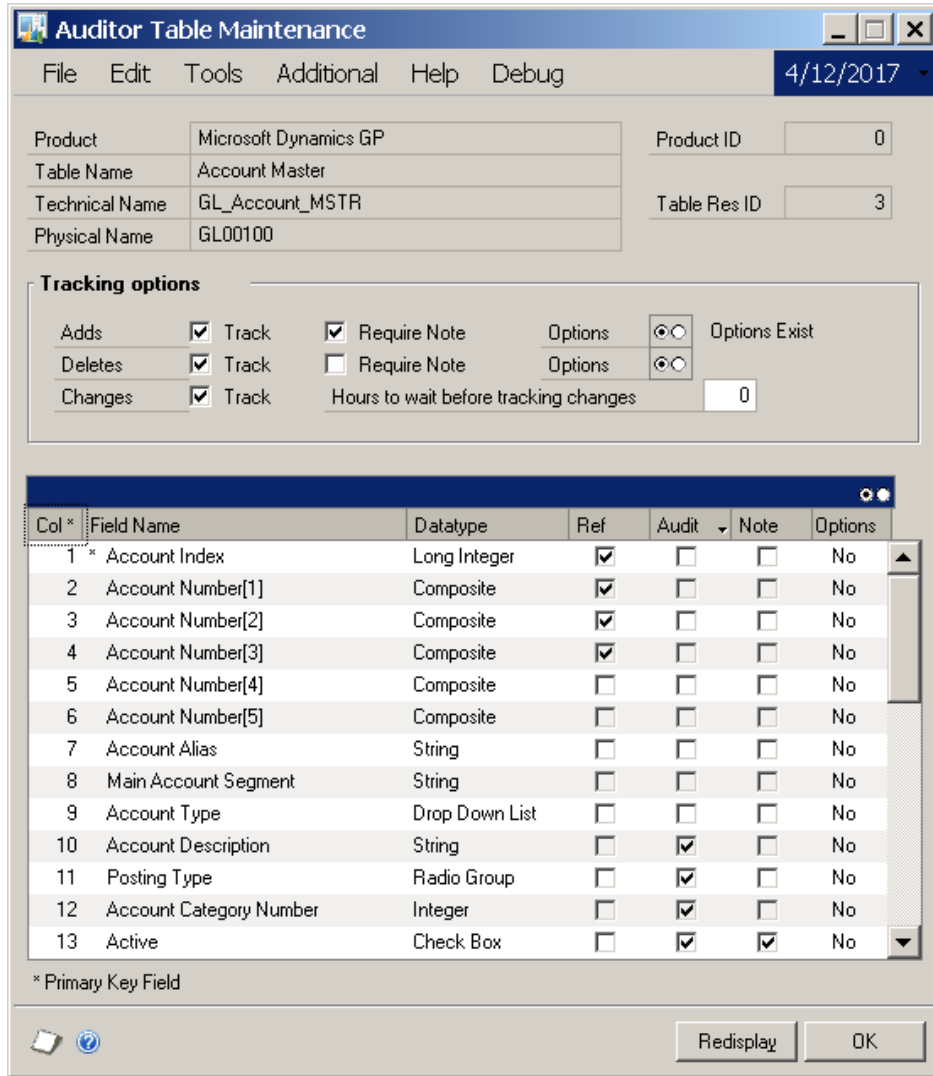
To get to this window, first open the Group Maintenance window. Then double-click one of the tables listed under the **Tables** node in the **Audits** tree.

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:

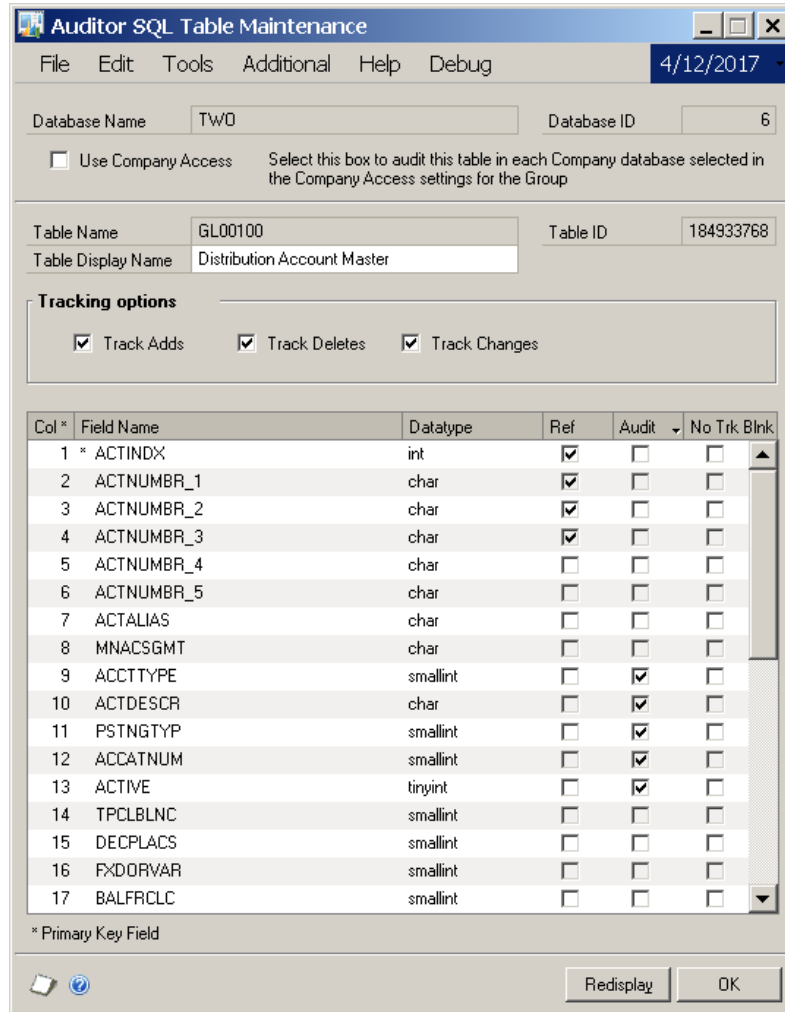| Option	Description
Track Adds	Check this option if you wish to audit when users add records to this table.
Track Deletes	Check this option to track deletions of records from this table.
Track Changes	Check this option to track specific field-level changes (which also must be selected in the field list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

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.

With SQL Table audits, the basic rule of thumb is, you cannot audit a table more than once in the same database. In order to prevent you from doing this, Auditor adheres to the following rules:

When checking Use Company Access on a 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 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.

Auditor Message Center window

The Auditor Message Center window is where Sys Admins and E-Sign Approvers are notified about system events.
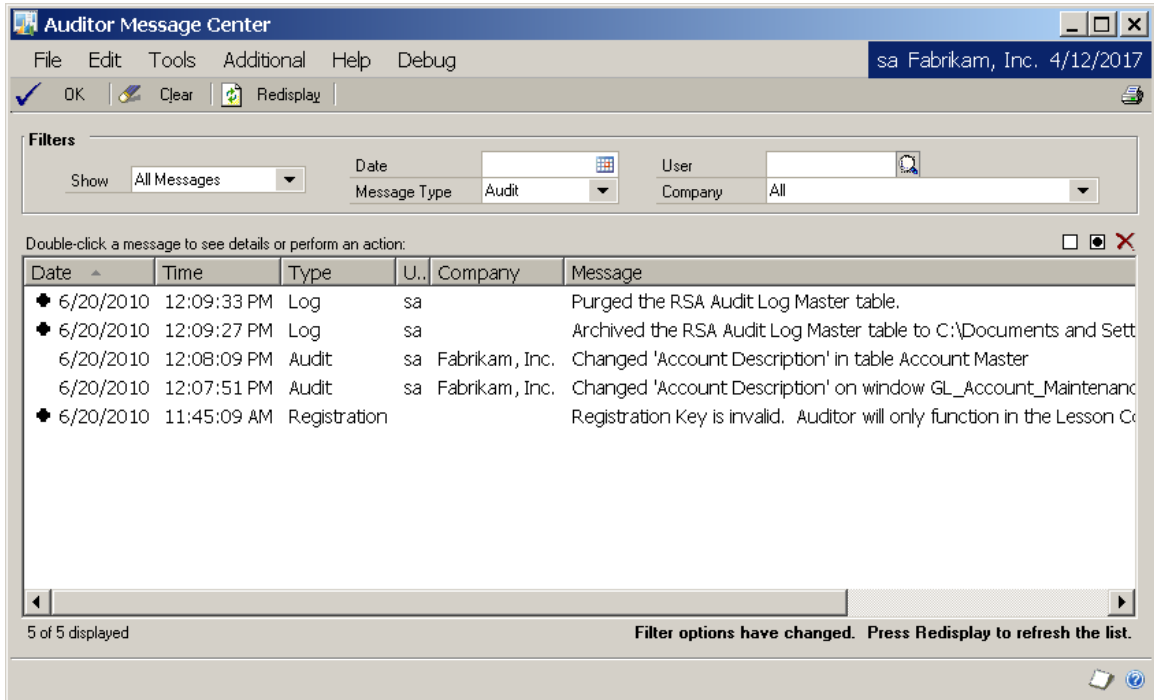
This window is accessible in one of these ways:

- 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 a Sys Admin or 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.

You can 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 Dynamics GP window:
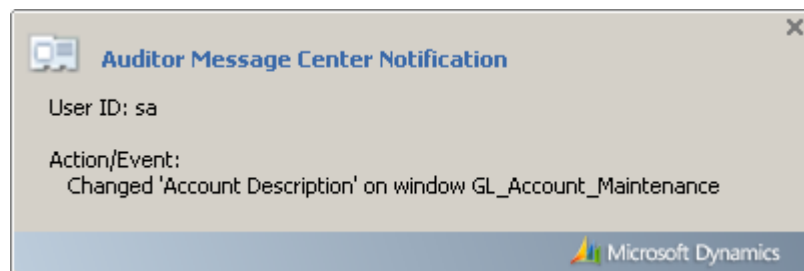

If there is User activity, then this Notification Box will appear for 15 seconds. If there is no User activity at the time that this box is displayed, then it will remain displayed until there is User activity.

If the Auditor Admin 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.

Reason Codes window

The Reason Codes window is where you set up common reasons for making system changes.
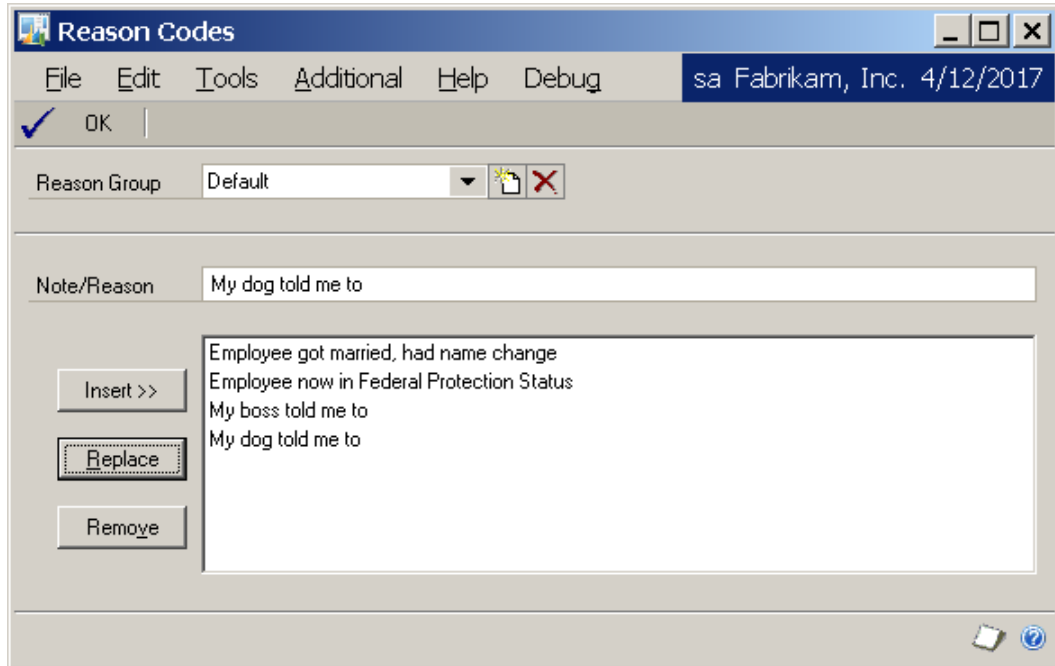
This window is accessible in one of these ways:

- 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.

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 will 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 Note Entry window will appear. It will specify the details of the change, and instruct the user, in bold, to enter the reason that they made the change.

The user can enter a Note or Reason by typing in freeform text into the note field. 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 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. However, 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 un-noted audits backed up.

The Note Entry window will display a status bar in the lower left explaining how many audits are left to be noted. Use the navigation buttons to see the outstanding un-noted audits. When all notes are completed, press the OK button.

Segregation of Duties Group Maintenance window

Segregation of Duties Group Maintenance is where you manage Segregation of Duties.
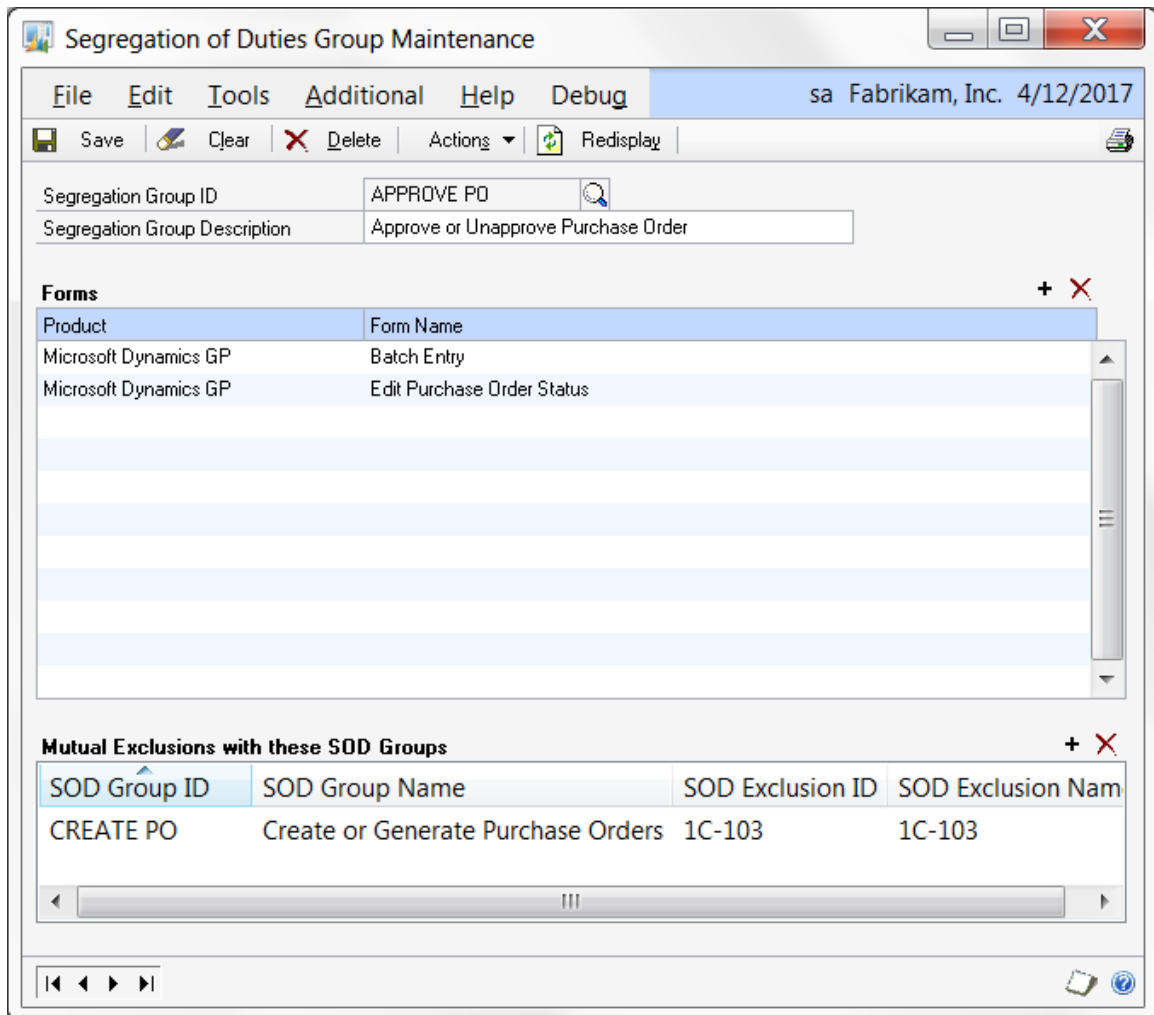
This window is accessible in one of these ways:

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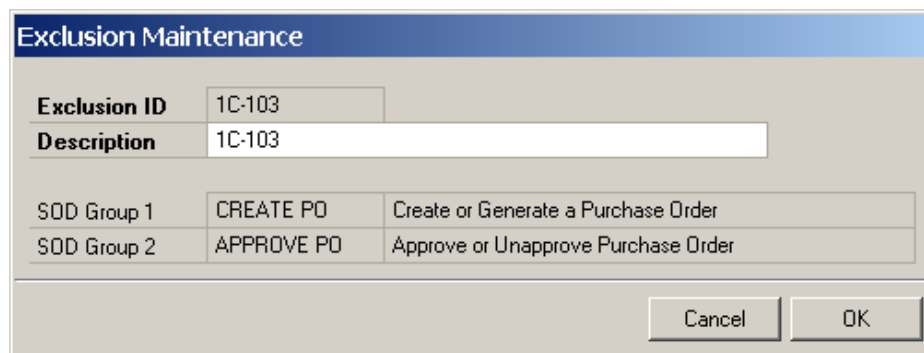
Once this SOD Group is created, you can make it mutually exclusive with other SOD Groups. This means that if a given user has security to any form in SOD Group 1, and then also has security to forms in SOD Group 2, a conflict is flagged.

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.

| Exclusion Maintenance		
Exclusion ID	1C-103	
Description	1C-103	
SOD Group 1	CREATE PO	Create or Generate a Purchase Order
SOD Group 2	APPROVE PO	Approve or Unapprove Purchase Order

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-".

View Related Audits window

This window lists all of the Audits related to whatever is displayed on the window that you are currently viewing.
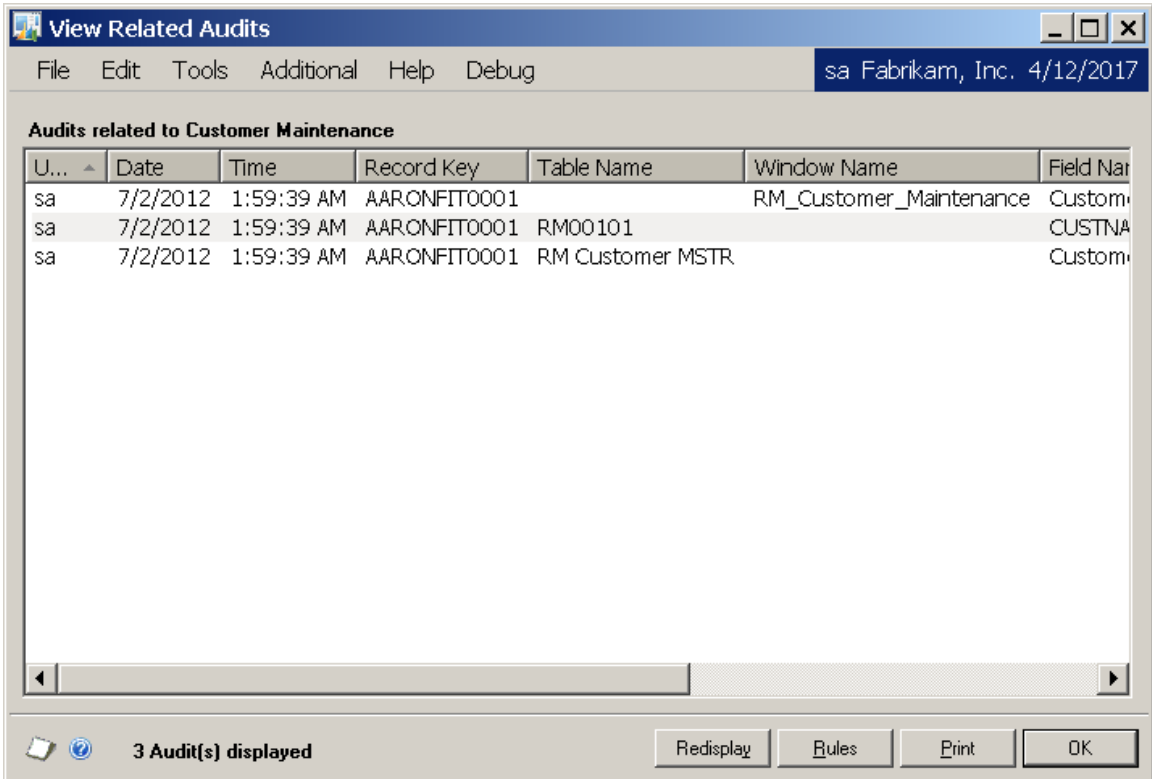
This window is accessed from the View Related Audits option on the Additional menu of almost any window in Dynamics GP.

Description

The Related Audits feature gives you the ability to see audits that have been captured for whatever 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.

Fortunately, we have provided setups for several of the most commonly-used entities in the system; so those will be enabled for you automatically. However, because we have used a flexible, rule-based setup, we have allowed you to turn on this functionality for virtually any window in Dynamics GP.

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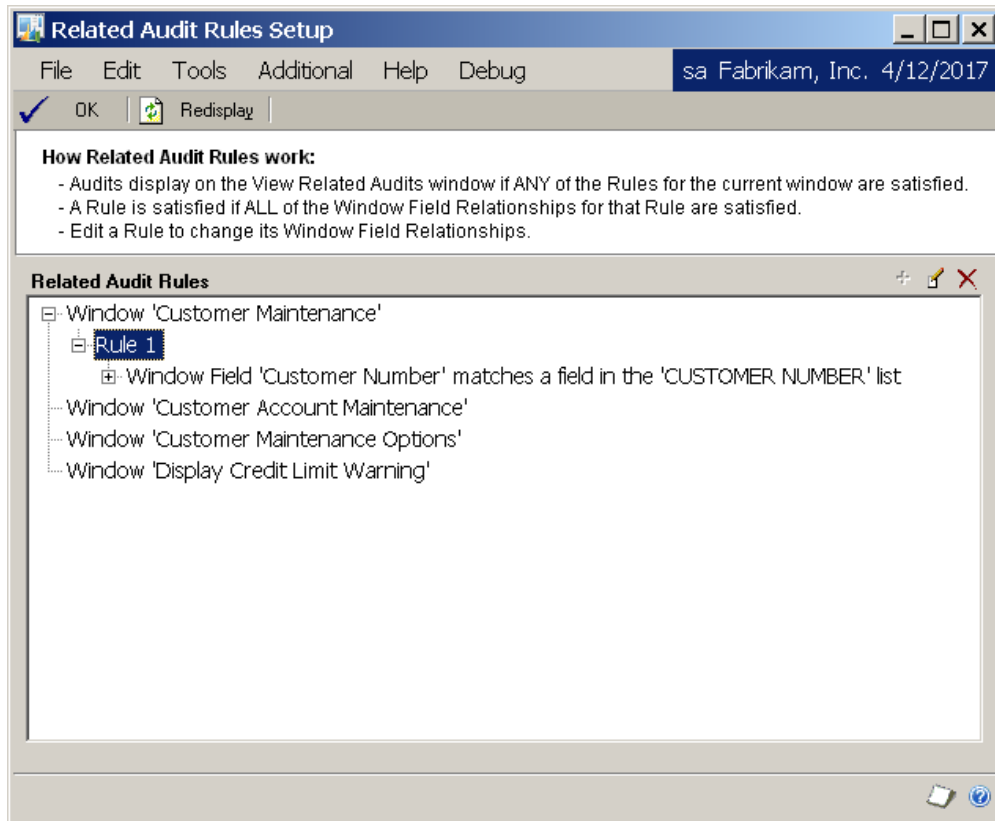
This window opens when you click the Rules button on the View Related Audits window.

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 admin, 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 admin, 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.
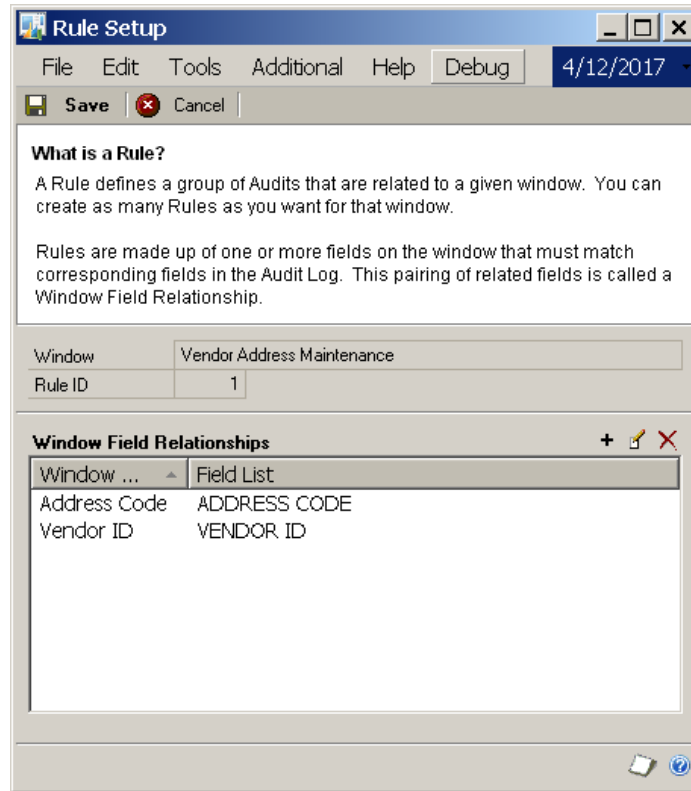
This window is accessible in one of these ways:

- 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 window is where you manage all of the Field Lists in Auditor.
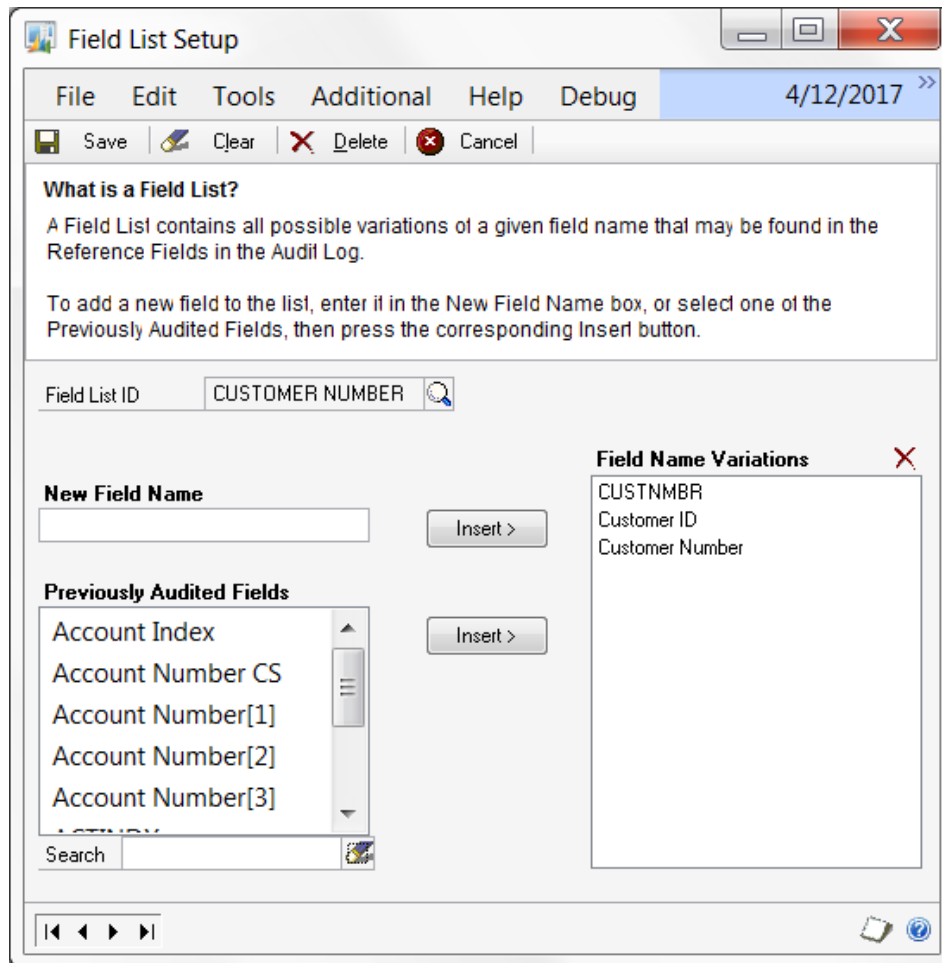
This window is accessible in one of these ways:

- 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, however. The Previously Audited Fields box lists all of the Reference Fields that appear on any audit in the Audit Log. You can use the Search field below the list box to narrow down the list to only those containing a certain value. This may me much easier than trying to come up with these variations on your own. You can then select one or more fields from the list box and add them to the Field List by clicking the bottom Insert button.
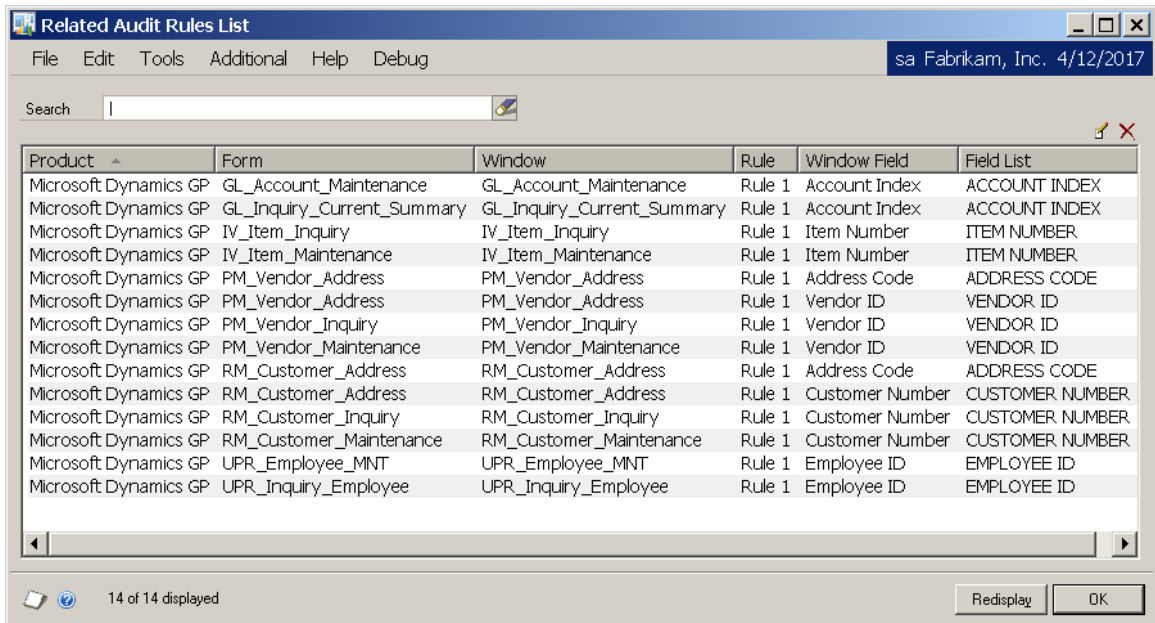
You can also remove a field from the Field List by selecting it in the Field Name Variations list box and clicking the Remove Field Name from Field List button (✕).

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.

Note Entry 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 Table Archive/Purge window

The Auditor Table Archive/Purge window is used to purge or archive Audit and E-sign Approval Log records.
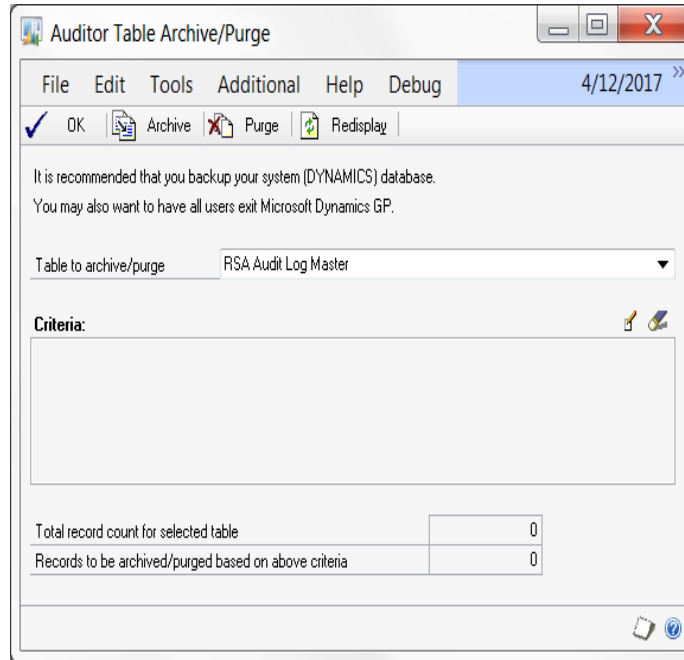
This window is accessible in one of these ways:

- 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 Audit/Approval Log Maintenance task.

Description

The Audit Log is contained in the RSAS015 and RSAS031 tables, the E-Sign Approval Log is contained in the RSAS039 table and the Security Audit Log is contained in the RSAS045 table. All are in the DYNAMICS database. Over time, these logs can grow quite large. The purpose of this window is to permanently archive and purge these files.

You can see the number of records that are in the selected log, and then define a query to select records for purging and/or archiving to XML. Pressing the Edit Criteria button ( ) will open an interactive tool for defining a query to act on the log file. You can filter which records you want to archive using this tool. Once you have done this, you will see the number of log records that match your query in the 'Records to be archived/purged based on above criteria' field. If you need help with this feature, please contact Rockton *Software or your reseller for support.*

You can use the Auditor Options window to notify Sys Admins when a specified threshold is reached.

Once you press the Purge button, the selected records will be deleted from the log file and cannot be recovered without a proper restore.

We recommend that you first export the records to XML using the Archive button or perform a backup to permanently archive the DYNAMICS database before purging a log.

Audit Reporting using SmartList
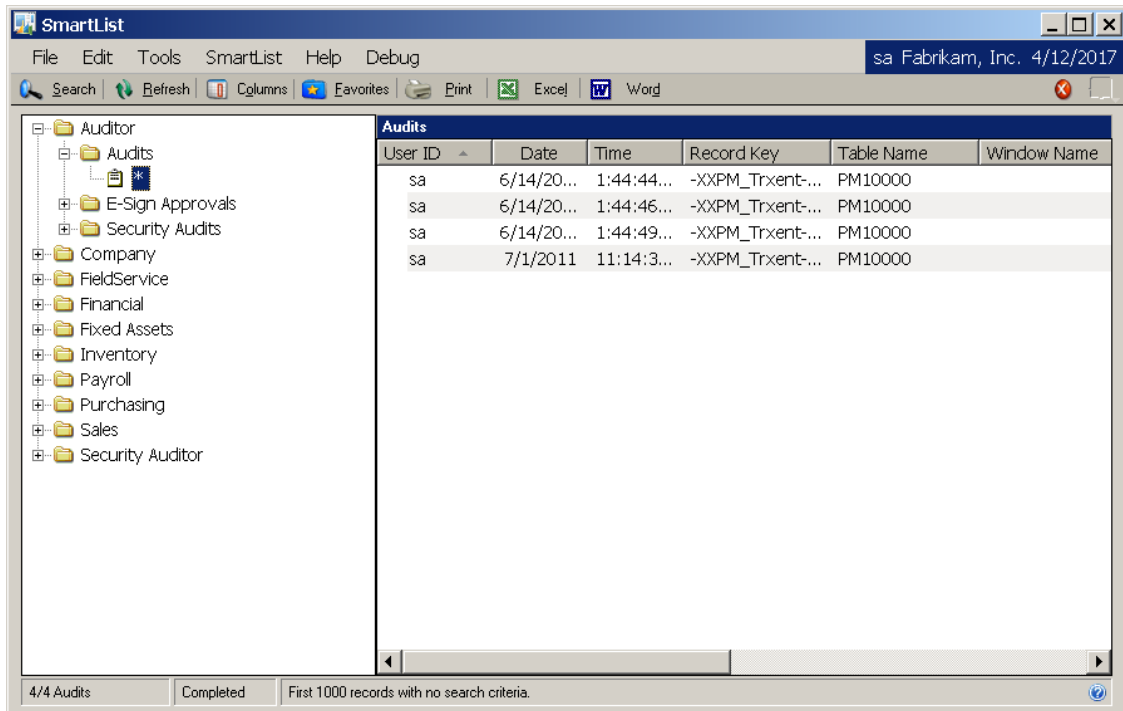
To get to this window, go to Microsoft Dynamics GP > SmartList, or press the SmartList icon on the Microsoft Dynamics GP toolbar.

Description

All system audits are tracked in two tables in the system database, and can be reported using Smartlist. Smartlist is the only built-in way of directly viewing audits. Using the features of Smartlist, you can filter and sort your audits and export them to Word or Excel for further evaluation. You can also double-click on and 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.

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

- Audits - RSAS015 and RSAS031 tables

- E-Sign Approvals – RSAS039 table

- Security Audits – RSAS045 table

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.

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 to which Users and Companies 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 allows you to simply open the window where you want to assign the Signature, click on the appropriate field, and then click an Assign Signature button on the Wizard window.

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

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.
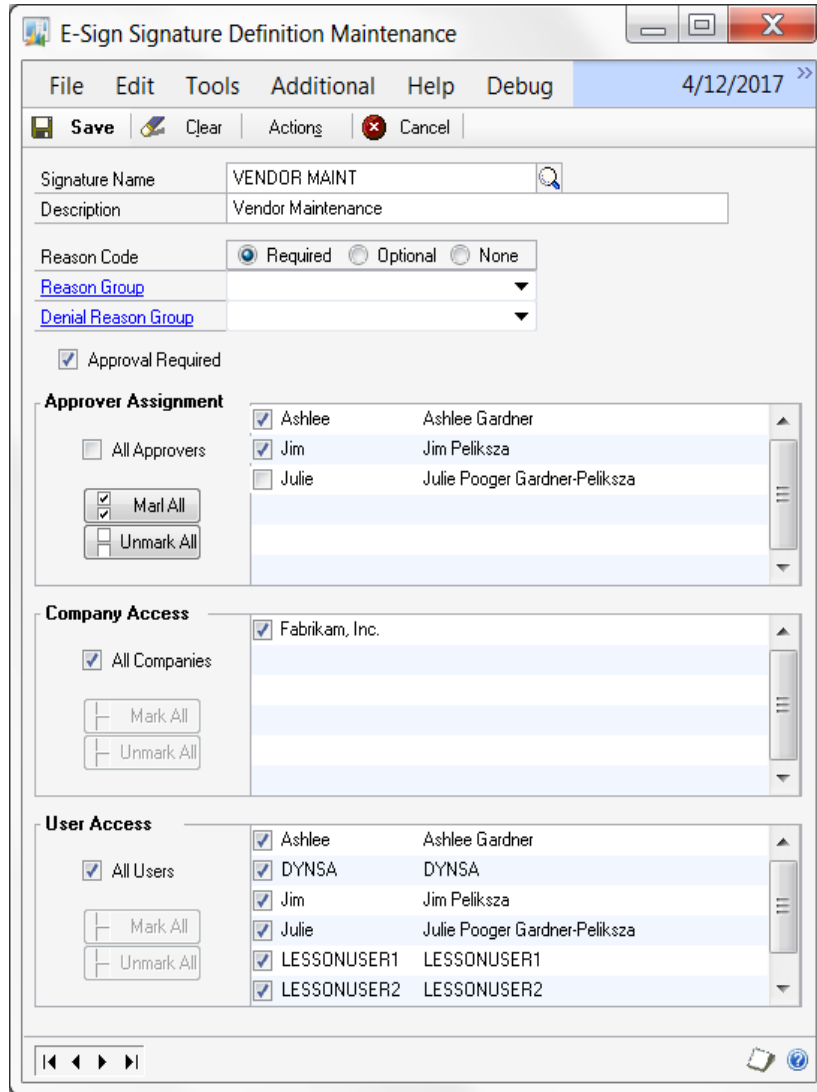
This window is accessible in one of these ways:

- 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.

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.
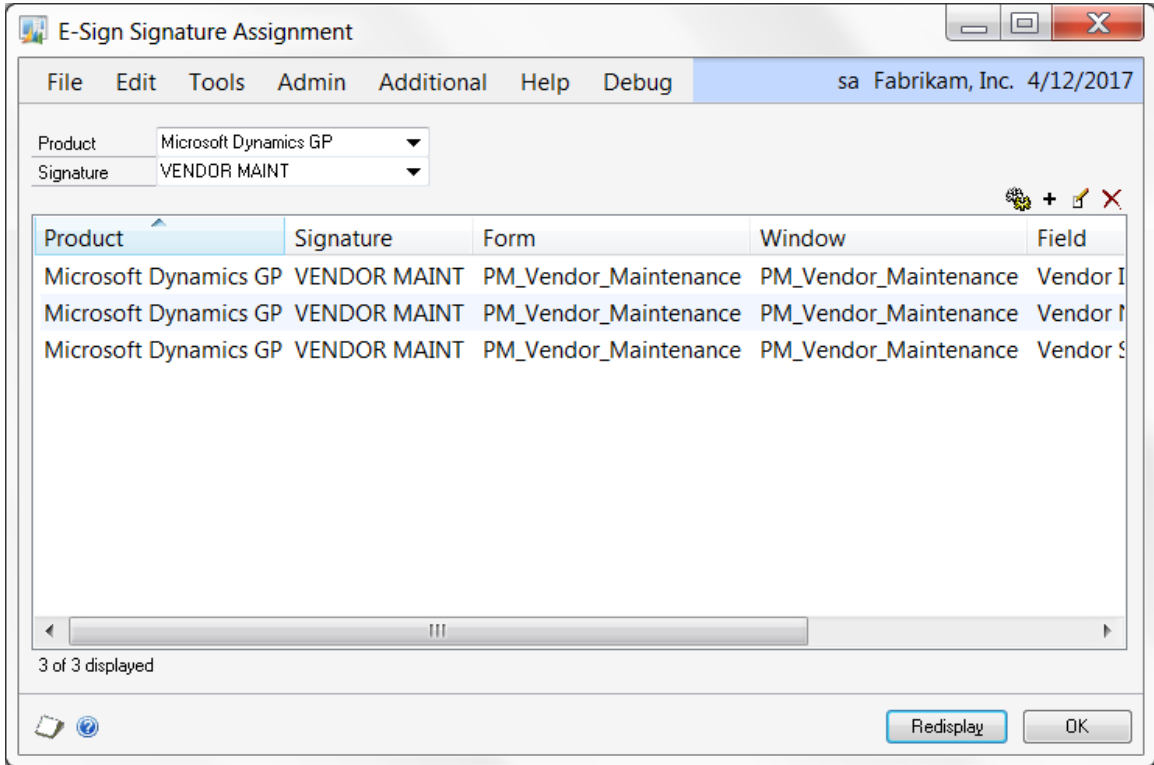
This window is accessible in one of these ways:

- 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 fields to which it applies.

Working with Signature Assignments

To assign a Signature to a window field, first click the Add Assignment button (**+**) to open the E-Sign Assign Signature window.

1. The first step is to select the Signature that you would like to assign. In this case, we will choose the **VENDOR CONTACT** Signature from the drop-down. This will automatically move us to Step 2.

2. You will now specify the window to which you want to assign the VENDOR CONTACT Signature selected in Step 1. You do this by simply opening that window the way you normally would. In this case, we will open the Vendor Maintenance window. You will notice that the Product, Form and Window information will fill in automatically and we will move to Step 3.

You may find that you need to open more than one window in order to get to the one that you want to assign. You will be moved to Step 3 immediately after opening the first window, but you can continue opening other windows and the Product, Form and Window information will fill in accordingly. Once you get to the window that you want to work with, you can continue to Step 3.

Step 1: Select Signature

Signature: VENDOR CONTACT

Step 2: Open window

Open the window where you want the Signature to be assigned.

Product: **Microsoft Dynamics GP**
Form: **PM_Vendor_Maintenance**
Window: **PM_Vendor_Maintenance**

Step 3: Select Signature Field

Choose a field on that window, then click Select to select it.

Field: **Vendor Contact**

[Assign]

3. We now need to specify the field to which you want to assign the VENDOR CONTACT Signature. This is done by simply moving the cursor to that field. In this case we will move the cursor to the **Contact** field. Then we will click Step 3's Assign button to move to Step 4.

You may notice that the Assign button in Step 3 has now changed to a Clear button. The Clear button allows you to "un-assign" the field that you initially chose and move back to Step 3 to choose a new field to which to assign the Signature.

4. In this final step, we will choose the field or fields on the window that we want to use to indicate what entity is being changed. These identifying fields are called Key Fields. In this example, we are assigning a Signature to the changing of the Contact field. So we need to select appropriate Key Fields that will indicate which Vendor it is we are changing.

To do this, you will move your cursor to a field that you want to use as a Key Field, then click the Add Key button (**+**). You will see the Key Field appear in the list at the bottom of the window. Repeat this process for each Key Field that you want to specify.

In the example above, we have chosen to use the Vendor ID and the Vendor Name fields to identify the Vendor being changed. You will see these values displayed when you look at the Approvals Log in Smartlist.

5. Once we have chosen all of our Key Fields, the Signature Assignment is complete. Click the Finish button to save the Signature Assignment. You should see a message indicating that the Signature was assigned successfully. The process for assigning this Signature is now complete.

Other Signature Assignment Functions

To remove a Signature Assignment, highlight it in the list and 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 a window where you can change the Form, Window or Field Name manually. In addition, you can change the Key Fields that have been assigned. Typically, we do not recommend using this window, however you may be asked to do so by Rockton Support.

The Actions button contains options for manually registering and unregistering the triggers that enable the Signature Assignments. Again, this is not something that you would normally need to do unless requested by Rockton Support.

E-Sign Approval Needed window

The E-Sign Approval Needed window is where a User requests approval 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.

Description

This window will open after a User makes a change to a field that has a 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 change will be undone.

Enter or select the Requestor's GP 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.

Enter or select an Approver for this change in the Approver field. Choosing the lookup will give you a list of all valid Approvers for this Signature.

The Approval Process

There are two options for obtaining approval for a system change. The simplest option is to click the Approve button. This 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.

The simple 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. 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 lower-left corner of the window. 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. A more detailed description of the E-Sign Pending Approval Requests window follows later in this document.

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.

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.

E-Sign Signature Needed window

The E-Sign Signature Needed window 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.

Description

Similar to the E-Sign Approval Needed window previously discussed, this window will open after a User makes a change to a field that has a Signature Assignment. However this window will open if the Signature Definition does not have the Approval Required option set.

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

E-Sign Pending Approval Requests window

The E-Sign Pending Approval Requests window is where you can see changes that currently need your approval.
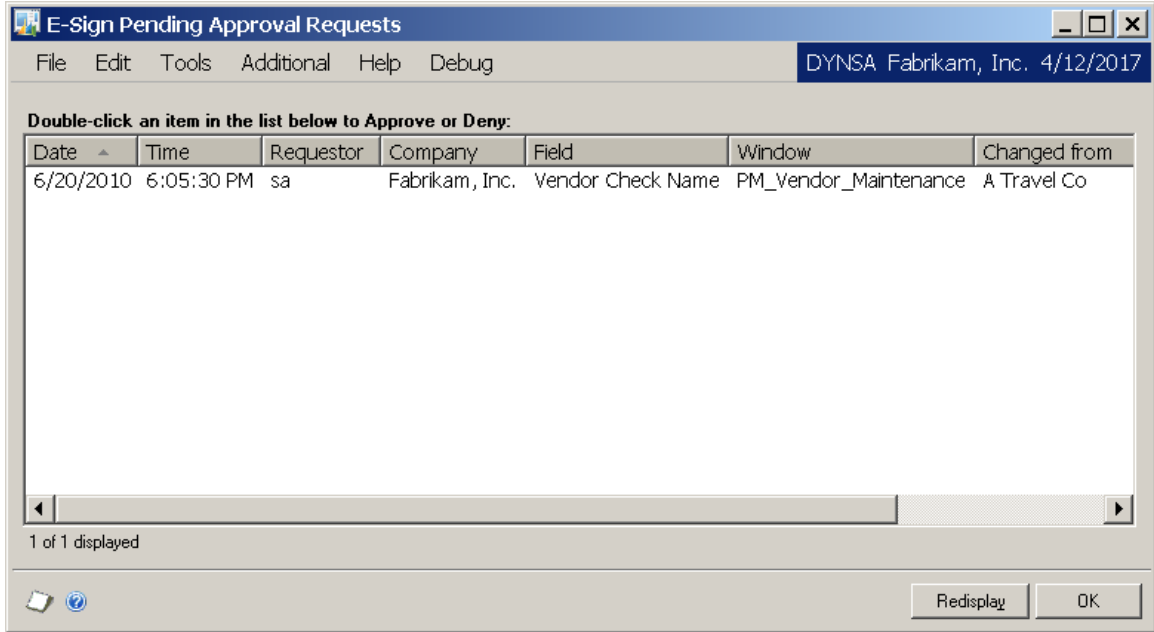
This window will open automatically for Approvers that have pending approval requests.
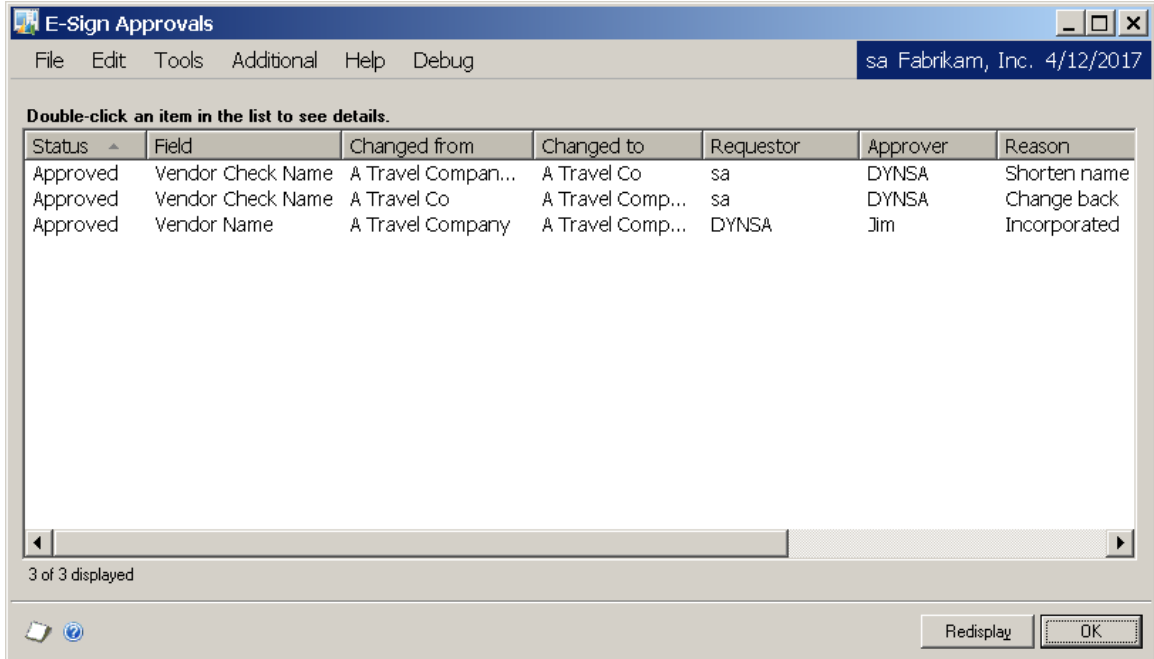
Description

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 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.

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

Audit Log Archive XML Format

The Audit Log Maintenance window provides an archive capability that will create an XML file containing the information in the Audit Log Master (RSAS015) table. The following is the format of that file:

<CompanyID>	CMPANYID
<ProductID>	PRODID
<ProductName>	PRODNAME
<AuditType>	RSA_Audit_Type
<FieldNote>	RSA_CB_Field_Note
<Date>	RSA_Date
<EventID>	RSA_Event_ID
<EventType>	RSA_Event_Type
<FieldName>	RSA_Field_Name
<FieldNote>	RSA_Field_Note
<NewValue>	RSA_Field_Value_String
<OldValue>	RSA_Field_Value_StrOld
<FormID>	RSA_Form_ID
<FormName>	RSA_Form_Name
<FormTechName>	RSA_Form_Technical_Name
<RecordKey>	RSA_Record_Key_String
<TableID>	RSA_Table_ID
<TableName>	RSA_Table_Name
<TablePhysName>	RSA_Table_Physical_Name
<TableTechName>	RSA_Table_Technical_Name
<Time>	RSA_Time
<WindowName>	RSA_Window_Name
<WindowTechName>	RSA_Window_Technical_Nam
<UserID>	USERID

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 (r). 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.