Administration User's Guide

This is a publication of Momentive Software.

Version 2026.1

© 2026 Momentive Software Holdco, LLC. All rights reserved.

Momentive Software™ and all respective logos are trademarks or registered trademarks of Momentive Software Holdco, LLC, and its affiliates.

Contents

Chapter 1: Introducing the Administration Module 1

Chapter 2: Organizations 2

Open Organization 2

New Organization 2

New Organization Wizard - Organization Name Panel 3

New Organization Wizard - Organization Main Address Panel 3

New Organization Wizard - Functional Currency Panel 4

New Organization Wizard - Fiscal Year-End Panel 5

New Organization Wizard - Account Segments Panel 6

New Organization Wizard - Modules Panel 10

New Organization Wizard - Field Lengths Panel 11

New Organization Wizard - Security Panel 12

New Organization Wizard - Finish Panel 12

Organization Information 13

Organization Information - Organization Tab 13

Organization Information - Address Tab 15

Organization Information - Segments Tab 17

Organization Information - Modules Tab 18

Organization Information - Field Lengths Tab 18

Organization Information - Electronic Filing Tab 20

Organization Information - Email Setup tab 21

Organization Preferences 33

Organization Preferences - Processing Tab 33

Organization Preferences - Entry Dates Tab 38

Organization Preferences - Session Tab 40

Organization Preferences - Document Number Tab 41

Chapter 3: User and Group Security 42
Maintain Users 42
Maintain Users Buttons 46
Rename User ID 46
Password 47
Maintain Groups 47
Maintain Groups Buttons 49
Copy Groups 49
Set Up System Menus 50
Copy System Security 52
Set Up Organization Menus 53
Copy Organization Security 56
Comparing System and Organization Security Menus 57
Audit Trails 58
System Audit 58
Summary Organization Audit 60

Chapter 4: Advanced Security 64
Set Up Account Level Segments 64
Set Up Account Level Security 66
Copy Account Level Security 68
Account Level Security on Transactions 68
Account Level Security on Reports 70
When Security Changes Take Affect 72
Updating Account Level Security 73
Set Up Database Encryption 74
Advanced Audit Trails 80
Advanced Organization Audit 80
Set Up Advanced Organization Audit 85

Chapter 5: Adding New Modules 90
Activate License - Owned Tab 90
Activate License - Evaluation Tab 91
Add a Module 93
Add a Module Wizard - Module Panel 93
Add a Module Wizard - Field Lengths Panel 95
Add a Module Wizard - Security Panel 95
Add a Module Wizard - Finish Panel 96

Chapter 6: Attachments 97
Set Up Locations 97
Set Up Categories 98
Set Up Categories Example 98
Set Up Categories Buttons 99

Chapter 7: User Defined Fields 100
Set Up User Defined Fields 100
Set Up User Defined Fields - Setup Tab 100
Set Up User Defined Fields - Transaction Sources Tab 105
Set Up UDF Default Sources 107
Flow-Thru Scenarios 109
A/P Flow-Thru 113
A/R Flow-Thru 114

Chapter 8: Alerts 115
Set Up Alerts 115
Set Up Alerts - Setup Tab 115
Set Up Alerts - Preview Tab 118
Set Up Alerts - Assign Tab 121

Copy Alerts Setup 122
Alerts Activity Log 123

Chapter 9: Grant Administration 125
Set Up Grant Administration Module 125

Chapter 10: Utilities 126
Backup 126
Backing Up Databases 127
Restore 129
Compress 130
Data Integrity Checks 130
Description of Individual Integrity Checks 132

Chapter 11: System Activity 139
Manage Concurrent Users 139
Manage Services 141
Set Maintenance Mode 143
Current Activity 143
System Menu Buttons 145
System Preferences 146
Windows Authentication 148

Chapter 12: Table Structure 150
Default Table Structure 150
Default Table Structure Buttons 153

Chapter 13: History 155
Consolidate Transaction History 155

Remove Payroll History 156

Chapter 14: Administration Reporting 157

Security List 157

User Information List 161

Group Information List 162

Account Level Security List 163

Advanced Organization Audit List 165

User Defined Fields List 167

UDF Default Sources List 170

Currency List 171

Index 173

Chapter 1: Introducing the Administration Module

The Administration module is intended for the MIP Fund Accounting system administrator. It includes detailed information about setting up users, establishing security, and entering organization/system specific data. The *Getting Started* guide contains information about analyzing and setting up your chart of accounts. It also provides forms that guide you through the organization creation process.

To Use This System

1. First, the MIP Fund Accounting system must be installed. Administration is required to run the system.
2. **The first time you log on to the system, enter NPS in the User box.** The user ID NPS initially has no password and has full security rights to all systems. Once your own user ID is created by the Administrator (Security>Maintain Users), go back and establish a password for NPS.
3. Once the Administration module is accessed, create a new organization using File>New Organization.
4. After selecting the new organization using File>Open Organization, all of the menu selections become available for all the modules that you have installed and added to the system.
5. There are Checklists available for setting up this system and its processes. Please refer to the online help (Help>Contents and Index>Reference) for specific menu selections, checklists, and common questions.

Chapter 2: Organizations

Open Organization

Access this form with Administrative user rights using File>Open Organization.

Use this form to open an organization in which to access. If you are currently working in an organization, opening a different organization closes the active organization.

If this is your first time logging on, enter NPS in the User box. The user ID NPS initially has no password, and has full security rights to all systems and sample data. Once you create your own user ID (Security>Maintain Users), go back and establish a password for NPS.

User Information

- **User:** Enter your User ID.
- **Password:** Enter the User's password.

Password requirements:

- Include at least one uppercase and one lowercase letter
- Include at least one number
- Cannot contain spaces at the beginning or end
- Cannot be one of the last 6 passwords used

Select an Organization: Specify the organization name you want to open. By default, the system displays the name of the last organization database opened.

Tip: If you try to open an organization database and you receive a message indicating that you currently have no rights for the database, you must log on as user *Admin* in order to register the database. If you do not know the password for user *Admin*, contact your system administrator.

New Organization

Access this wizard with Administrative user rights using File>New Organization.

Use this wizard to quickly set up a new organization.

New Organization Wizard - Organization Name Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel to assign a name to the organization you are setting up. After completing all panels of the wizard, click the Finish button. The system creates a database with the same name as the organization name.

Nonprofit Online Users

Your organization name will automatically be prefixed with your Organizational Unit identifier as part of the New Organization Wizard process. This helps identify your database in the Private Cloud environment. For more information, see Nonprofit Online.

Fields

What is the name of your organization?: Enter a unique name for the new organization. This name appears in the heading of reports. Note that when entering an organization name, you should avoid the use of symbols, such as | " / \ : * ? ; < > [ ] ' and #.

Tips:

- You can change the organization name later, using the Organization>Organization Information>Organization tab.
- The *Getting Started* guide contains information about analyzing your chart of accounts structure.

New Organization Wizard - Organization Main Address Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel of the wizard to enter the address and other pertinent information about the organization.

Fields

Address, City, State/Province, Postal Code, Country: Enter the main address for the organization you designated on the previous panel. This address appears on disbursement checks, statements, and other forms. It can contain up to three lines of text.

Voice, FAX: Enter the voice and FAX telephone numbers for the designated organization. These numbers appear on any reports that include this type of information.

Email, Web Site: If applicable, enter the email address and website URL address for the active organization. This data appears on any reports that include this type of information.

Tips:

- You can edit this information later, using the Organization>Organization Information>Address tab.
- The *Getting Started* guide contains information about analyzing your chart of accounts structure.

New Organization Wizard - Functional Currency Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel to select the primary currency to use for this organization. You can choose from many types of currency, such as the US Dollar, Euro, Pound Sterling, Yen, or Mexican Peso.

- If the Multicurrency module is *not* installed, this will be the only currency the organization can use to operate.
- If the Multicurrency module is installed, this will be the primary reporting currency. That is, the currency in which exchange rate gains and losses are recorded. Other currencies can be used once the Multicurrency module is added, if necessary, (Organization>Add a Module) and the currencies are set up (Organization>Set Up Modules>Multicurrency).

Once the wizard is finalized, the currency formatting can be specified using the Organization>Currency Setup form. You can set up different currency formatting for each currency type used in the system. To determine the decimal and grouping symbols used in reports, with Administrative user rights, use the Organization>Currency Setup form. Other decimal and grouping symbols (such as the period and comma), found throughout the system, follow the computer's regional settings (Start>Settings>Control Panel>Regional Options). All non-currency numbers follow the computer's regional settings.

Multicurrency and Payroll Users

If you have installed both the Multicurrency and Payroll modules, you must select a functional currency of USD (US Dollar).

Fields

What is your functional currency?: Select a currency type from the drop-down list. This is the primary currency that will be used throughout the organization. Once you complete this wizard, the functional currency cannot be changed.

New Organization Wizard - Fiscal Year-End Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel to enter a fiscal year-end date, the organization's Federal and State Tax Identification numbers, and select your IRS Tax Form Preference.

The fiscal year-end date defines the current fiscal year (including fiscal month end and day date end) in which you are operating. This date is automatically increased by one year each time you run the annual close process (Activities>Close Fiscal Year). The year that you enter is the first fiscal year you can close for the current organization; however, you can enter transactions for any number of previous fiscal years.

Fields

What is your fiscal year-end?: Enter the last day of the fiscal year for which you are entering transactions. This date cannot be changed after the organization is created.

What is your Federal Tax Identification Number?: Select FEIN or Foreign and enter the federal tax identification number for this organization. You are not required to enter an ID here; instead, you can enter it at a later time, using the Organization>Organization Information>Organization tab. When FEIN is selected, the system will mask the tax ID for Aatrix® reporting, using the following format ##-####### and limits the number of digits to nine.

What is your State for 1099 Withholding?: Select your state from the drop-down list. You are not required to enter your state on this panel; instead, you can enter it at a later time, using the Organization>Organization Information>Organization tab.

What is your State Tax Identification Number?: Enter your state tax identification number for the 1099 State Withholding Information. You are required to enter your state tax identification number on this panel if you entered a State for 1099 Withholding on this panel. If you did not enter your State for 1099 Withholding on this panel, you are not required to enter your state tax identification number here either; instead, you can enter it at a later time, using the Organization>Organization Information>Organization tab.

What is your IRS Tax Form Preference for this organization?: Select the organization's IRS tax form preference. Once your organization is created, you can switch between any form using the Organization tab (Organization>Organization Information). 990 line numbers assignments will need to be entered using the Maintain>Chart of Accounts form.

- **Form 990EZ:** Select the 990 form version that you want to report for this organization.
- **Form 990:** Select the 990 form version that you want to report for this organization.
- **Government - N/A:** Select Government N/A if you are not required to submit a 990 form.

Tips:

- Once you enter the fiscal year-end date here, the system calculates the first day of the fiscal year, and displays it in the "Warn Prior To" column on the Organization>Organization Preferences - Entry Dates Tab. Consequently, users are warned if they try to enter a transaction for the previous fiscal year. However, please note that the Close Fiscal Year process (Activities>Close Fiscal Year) does not update the entry dates specified on the Organization Preferences form.
- The *Getting Started* guide contains information about analyzing your chart of accounts structure.

New Organization Wizard - Account Segments Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel to enter your chart of accounts segment structure and to define the properties for each segment, or modify these selections. The system automatically displays suggested default segments. You can accept these segments, create your own, or delete all of them, except GL. However, the suggest default segment structure provided–GL, Fund, Sub Acct 1, Sub Acct 2, and Restriction–generally accommodates most organizations' needs to generate proper financial statement formats, making it easier to produce financial statements (Reports>Financial Statements) and the Reports>990 Worksheet.

Be sure to thoroughly analyze your reporting requirements before you enter and save your chart of accounts segment structure. The system gives you full reporting capabilities for each segment created.

Note: A segment's properties cannot be added, deleted, or modified after the completion of this wizard. You can, however, change the names, function assignments, and the order of the segments, using the Organization>Organization Information - Segments Tab.

Allocation Management Users

In order to create an organization which includes the Allocation Management module, you must create at least two segments-General Ledger and another segment.

Fields

Note: To activate each new row in the table, enter information in one of the columns (such as, enter "3" in the Seq. column).

Sequence (Seq.): The number that you enter here designates the order in which segments appear for transaction entry. The sequence does not affect the order that the segments appear on reports; you control that when you print reports.

Name: Enter a name to identify each account segment. Remember, the Segment Name is only a title. The segment's behavior is determined by its associated Type. If accepting the default segments provided, the segment name should be modified to meet the organization's unique needs. For example, instead of using Sub Acct 1, you might change it to Location.

Type: The following is an explanation of each segment type:

- GL (General Ledger) - This segment type is used for classification of assets, liabilities, revenues, and expenditures. It is required, and you can only have one GL segment. (This is the only segment type that is required in every organization's account structure.)
- Fund - This segment type is used for recording transactions by fund (where fund is a self-balancing, separate set of books). It is optional, and you can only have one Fund segment in an organization's account structure.
- BAL (Balancing) - This segment type is used for transactions, such as, departments, grants, and programs, where you want debits to equal credits for each related code.
- NBAL (Non-Balancing) - This optional segment type is used for classification of transactions, such as, departments and programs, where you do not require that debits equal credits for each related code. Non-Balancing segments are used in situations where an organization needs to track Revenues and Expenditures, but not balance sheet accounts.
- RES (Restrictions) - This optional segment type is used to classify activity according to ASC 958 (FAS 117 superseded) classifications—unrestricted, temporarily restricted, or permanently restricted. ASC 958: Unrestricted (funds without donor restrictions) or Restricted (funds with donor restrictions).

Character Type: This defines the character set you want to use when naming account codes for each segment (Maintain>Chart of Accounts Codes). We suggest that you consider the person entering transactions when you assign segment Character Types—numbers are more easily and quickly entered than alphabetic characters. The table below shows each character type and which characters are valid for that type.

Character Type	Valid Characters
Numeric	Numbers 0-9 only
Alphabetic	Letters A-Z only (upper and lowercase)
Alphanumeric	0-9, A-Z, and punctuation (except the invalid characters: | " [ ] ' %)

Length: This defines the maximum number of characters allowed when naming account codes for each segment. Since you want to accommodate all the codes required, consider your future needs when making choices here.

Function: Select a function of N/A (Not Applicable), PGM (Program), FND (Function), or RES (Restriction) for each segment. Only one segment can be assigned PGM, FND, or RES. All other segments must be assigned N/A. The system automatically assigns the function for the default segments; you can accept the system selections or change them.

The function is used later when setting up account codes (Maintain>Chart of Accounts Codes). Essentially, this code is used to determine the list of designation codes available on the Chart of Accounts Codes form. They are used primarily for 990 reporting.

By flagging a segment with a functional designation, the system will be able to associate that segment with pre-defined sets of grouping categories commonly used in financial and tax reporting. Function codes must be assigned in order to run the system's default financial statements and for reporting form 990.

- If a segment is set up with a function of PGM, it can be assigned a designation of Program Expenses, Fundraising Expenses, or Management & General Expenses. Use Maintain>Chart of Accounts Codes>Setup tab to assign one of these designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations.
- The system uses the PGM segment to identify the segment that will be used to group Program Service revenue for 990 Part VIII Line 2 items, as well as the Functional expenses in Part IV.

- If a segment is set up with a function of RES, it can be assigned a designation of FAS 117: Unrestricted (funds without donor restrictions), Temporarily Restricted, or Permanently Restricted and ASC 958: Unrestricted (funds without donor restrictions) or Restricted (funds with donor restrictions). Use Maintain>Chart of Accounts Codes>Setup tab to assign one of these designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations.
- If a segment is set up with a function of FND, it can be assigned a designation of N/A or a fund designation code you created using the Reports>Assign Report Groups. Use Maintain>Chart of Accounts Codes>Setup tab to assign one of these designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations.
- The General Ledger segment always has a function of N/A because the system defined GL designations are only applicable to the GL Segment and there can only be one GL segment per organization. It can be assigned any designation available for the N/A Function. Use Maintain>Chart of Accounts Codes>Setup tab to assign one of the available designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations. For more information about N/A Functions, see Chart of Account Code Designations.

Tips:

- The *Getting Started* guide contains information about analyzing your chart of accounts structure.
- When you are adding segments to this table, you may want to start with the Type drop-down list, so you can first choose each new segment's type, then designate its other properties.

New Organization Wizard - Account Segments Example

Say, for example, that you are a non-profit organization setting up your system. You have analyzed your report requirements and determined you need to report to external funding sources by grant, and to internal management by department. You have both a general operating fund and a grant fund; and need to produce ASC 958 (FAS 117 superseded) reports.

Set up your segments as follows:

Segment Name	Segment Type
Fund	Fund
General Ledger	General Ledger

Segment Name	Segment Type
Grant	Balancing
Department	Nonbalancing
ASC 958 (FAS 117 superseded)	Restrictions

With this setup, your organization works the following way:

- Debits must equal credits for all Funds entered during transaction entry. This is a system requirement for all Fund segments.
- Because you have designated ASC 958 (FAS 117 superseded) as a Restrictions segment, a Restrictions code is required for each line of your transactions for General Ledger account types Revenues, Expenditures, and Net Assets/Equity.
- Because you have designated Grant as a Balancing segment, debits must equal credits for all Grants entered during transaction entry. This means a Grant code is required for each line of your transactions, regardless of whether the General Ledger account for the line affects revenues/expenditures or assets/liabilities.

Note: Generally, do not designate a segment as Balancing unless you need to produce Balance Sheets for each of the related codes; codes for both Balancing and Non-balancing segments are always required with revenue- and expenditure-type General Ledger accounts.

New Organization Wizard - Modules Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel to designate which modules you want to use with this organization. By default, the system places a check mark next to all available modules (that is, all modules that are authorized by your activation code).

Allocation Management Users

In order to create an organization which includes the Allocation Management module, you must create at least two segments-General Ledger and another segment on the Account Segments panel. If you only created one segment (General Ledger), clear Allocation Management on the Modules panel.

Payroll Link Users

In order to create Timesheets and process Payroll, the HR Management module must be installed.

Fields

Which modules will be used by this organization?: This panel displays a list of modules you are licensed to use as designated by your current activation code. Select the modules you want to use with the organization. After you set up your organization, you can add modules to it later using the Organization>Add a Module wizard.

The General Ledger module is not available for selection since it is required to operate the system.

New Organization Wizard - Field Lengths Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel to view and/or alter the default field lengths for the organization. The lengths entered here indicate the maximum number of characters allowed for various elements within your organization.

Note: The field lengths cannot be changed after the organization is created.

Fields

Module: The system displays the customizable fields for the modules you installed.

Category: The system displays the category assigned to this field, such as Title or ID.

Field Name: The system displays the name of the field, as it appears in the system.

Field Length: Either change the length, or accept the default for each of the fields listed in the table.

Tips:

- If you create an organization with a Vendor ID length of less than 10 characters, you cannot use the "UNASSIGNED" Vendor ID. This ID was designed so you can enter purchase orders to generate encumbrances with an unknown Vendor ID. For more information about using this ID, see Maintain>Accounts Payable>Vendors - Vendor Tab.
- It is a good idea to evaluate your needs, and shorten and lengthen fields as appropriate. For example, you might want to enter distribution codes that are longer than 12 characters, or you may want to limit G/L transaction descriptions to less than 60 characters.
- The Document Number must be 14 character or longer in order to be consolidated (Organization>Consolidate Transaction History).
- The list displays all of the customizable field lengths for this organization. Fields not listed are not customizable.
- The *Getting Started* guide contains information about analyzing your chart of accounts structure.

New Organization Wizard - Security Panel

Access this panel with Administrative user rights using File>New Organization.

Use this panel to confirm that all security rights have been granted to the current user for the organization in which you are creating. The current user is the user name you entered when logging on to the system.

You also need to assign security rights to other users (Security>Set Up Organization Menus) before they can access this organization.

New Organization Wizard - Finish Panel

Access this panel with Administrative user rights using File>New Organization.

Use this final panel to review all selections you made while setting up this organization, including the organization and server names, segments, installed modules, and field lengths.

When you click the Finish button, a database is created; you can begin using your new organization. The system names the database, by defaulting to the same name as the organization, which you entered on the first panel of this wizard.

Tips:

- If you need to make changes before you click Finish, use the Back button to move back to the appropriate panel and make the necessary changes.
- You can print the information for this organization by right-clicking (in the area where the organization properties are listed) and selecting "Print."
- You can only change the following information once you finalize your organization:

Information	Where it can be changed
Organization Name, Tax ID Numbers, IRS Tax Form Preference	Organization>Organization Information>Organization tab
Organization Address	Organization>Organization Information>Address tab
Segment Sequence, Segment Names, Function	Organization>Organization Information>Segments tab
Available Modules	Organization>Add a Module

Organization Information

Use this form to review and/or edit setup options for the active organization. Note that many setup options (such as fiscal year-end, segment types, and segment lengths) cannot be edited. When you enter information on this form, it is available in the system the next time a user opens the active organization. The organization must be closed before making any changes to it.

Organization Information - Organization Tab

Access this tab with Administrative user rights using Organization>Organization Information.

Use this tab to edit the Name, Federal Tax ID, or 1099 State Withholding information assigned to the active organization. You can also use this tab to set an organization to be used specifically for testing purposes.

Fields

Name: If you want to change the name of the active organization, enter the new name here. The name listed here was assigned to this organization when it was created (File>New Organization).

Note that when entering an organization name, you should avoid the use of symbols, such as | " / \ : * ? ; < > [ ] ' and #.

Server: The system displays the name of the server in which you are running.

Database: The system displays the database name for the active organization.

Currency: The system displays the primary or functional currency assigned to the active organization.

Fiscal Year-end: The system displays the active organization's fiscal year.

The Server name, Database name, Currency, and Fiscal Year-end date are *display* only. These items, which were designated when the organization was created (File>New Organization), cannot be changed.

This is a test organization for testing and new feature beta purposes: Select this option if you'd like the organization you're currently working in to be used for testing purposes only. Any changes made in this test organization will not affect your live production data.

Note: The new test organization settings will only take effect after you log out and back in to MIP.

Once you log back into MIP and have the test organization selected, you will receive a pop-up message that allows you to select a different organization or proceed with using the test organization.

TEST **TEST** **TEST** will display in the header next to the organization name to indicate that you're working in a test organization.

Federal Tax ID: Select FEIN or Foreign. Then enter or edit the federal tax identification number for this organization. If this number was already assigned (File>New Organization), the system displays it for you. When FEIN is selected, the system will mask the tax ID for Aatrix® reporting, using the following format ##-####### and limits the number of digits to nine.

Note: If the Federal Tax ID number is displayed but you select the other option button, the system will remove the number. You will need to click the Undo button or re-enter the Federal Tax Identification Number.

1099 State Withholding Information: This is the organization's default State and State Tax ID number. If you intend to withhold state or local taxes on 1099 distributions, enter your organization's default State and State Tax ID and for each Vendor, select the *Issue 1099 for this Vendor* check box on the Maintain>Accounts Payable>Vendors>1099 Information form. (See Important Notes about 1099s.)

- **State:** Select the organization's state from the drop-down list.
- **State Tax ID:** Enter the organization's state tax identification number.

IRS Tax Form Preference Form 990EZ, Form 990, Government - N/A: Select the organization's IRS tax form preference. Select Government N/A if you are not required to submit a 990 form. Or select the 990 form version that you want to report. Form 990 Line Numbers are assigned using the Maintain>Chart of Accounts form. You must manually enter the 990 Line Number assignments, the first time Form 990 is selected. It is recommended to review the 990 form line number assignments for each 990 form version using the Chart of Accounts List Report (Reports>Lists>Chart of Accounts). This would ensure that any modifications made to the line number assignments are reflected correctly in the selected tax form.

Tips:

- When setting up security for users (Security>Set Up Organization Menus), we recommend you limit access to this form to include only system administrator-type users.
- The State Tax ID is required by several states as a means to get self-employed workers to pay state tax. This also aids in tracking income for alimony and child support. This ID may not be required in all states, but it is still a good idea to complete it. Some states use the FEIN as the State Tax ID. You should contact your state tax commission to determine what they require.
- If an individual vendor needs the state and state tax ID to be different for the 1099 State Withholding, this default can be replaced for the vendor using the Maintain Vendors>1099 Information tab. Ensure that the *Issue 1099 for this Vendor* check box is selected and complete the Organization State Withholding section including the Override State Withholding check box.
- Upon upgrade, if 2007 Form 990 Line Numbers were already assigned, the Form 990EZ is selected. Those assignments can be converted to the Form 990EZ Line Numbers. It is recommended to review the 990 form line number assignments for each 990 form version using the Chart of Accounts List Report (Reports>Lists>Chart of Accounts). This would ensure that any modifications made to the line number assignments are reflected correctly in the selected tax form.

Organization Information - Address Tab

Access this tab with Administrative user rights using Organization>Organization Information.

Use this tab to enter or modify the active organization's Main Address information. Use the "Printed Address" (page 16) button to override the main address and have it printed in a different format.

Fields

Main Address: The system displays the information entered when the organization was created (File>New Organization); however, it can be edited here.

- **Address, City, ST/Province, Postal Code, Country:** Enter the street or post office address for the active organization. The address you enter here appears on disbursement checks, statements, and other forms. The address can contain multiple lines of text.
- **Voice, FAX:** Enter the telephone and FAX numbers for the active organization. These numbers appear on any reports that include this type of information.
- **Email, Web Site:** Enter the email and website URL addresses for the active organization. This data appears on any reports that include this type of information.

Printed Address

Access this form using:

Maintain>Accounts Payable>Vendors>Addresses tab>Check Address button>**Printed Address button**; Purchase Order Address button>**Printed Address button**; **Printed Main Address button**;

Maintain>Accounts Receivable>Customers>Addresses tab>Services Address button>**Printed Address button**; Shipping Address button>**Printed Shipping button**; **Printed Billing button**;

Maintain>Purchase Orders>Address Codes>Address Codes tab>**Printed Address button**; or

Organization>Organization Information>Address tab>**Printed Address button**.

Use this form to override the printed format of the main address. This is helpful, if for example, the main address is in US postal mail format, but it must be printed in German postal mail format. Use the Update and Reset buttons to update or reset the address to the default settings.

Fields

Address Format: Use the Address, City, State/Province, Country, and Postal Code buttons to reorganize the structure of the address for printing. Additional information can be entered as well.

Printed Address: The system displays the main address. This is how the address will be printed on the form. If you modify the Address Format using the buttons, this field refreshes with your changes.

However, if you enter text into the Address Format, you must click the Update button to refresh this field and see how the address will be printed.

Organization Information - Segments Tab

Access this tab with Administrative user rights using Organization>Organization Information.

Use this tab to rename segments, change the segment sequence, and change the functional designation. The system also displays the segment properties (Type, Character Type, and Length) on this tab; however, these properties cannot be changed.

Data Consolidation Users

When a consolidated organization is created by the Administrator (File>New Consolidated Organization), the system automatically generates a CO (Consolidate) Type segment. Consequently, if the current organization is a consolidated organization, the system displays the CO segment on the Segments tab.

Fields

Seq.: This column designates the order in which segments appear in the system for transaction entry. (The sequence you enter here does not affect the order that the segments appear on reports; you control that order when you print reports.)

Name: This column designates the account segment's name. Segment names are used when you enter codes and transactions.

Type: The system displays the segment type. The system offers the following segment types when you are setting up a new organization: Fund, General Ledger, Balancing, Non-Balancing, or Restrictions.

Character Type: The system displays the character type.

Length: The system displays the maximum number of characters allowed for certain fields.

Function: Select a function of N/A (Not Applicable), PGM (Program), FND (Fund), or RES (Restriction) for each segment. Only one segment can be assigned PGM, FND, or RES. All other segments must be assigned N/A.

- If a segment is set up with a function of PGM, it can be assigned a designation of Program Expenses, Fundraising Expenses, or Management & General Expenses. Use Maintain>Chart of

- Accounts Codes>Setup tab to assign one of these designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations.
- If a segment is set up with a function of RES, it can be assigned a designation of Unrestricted or Restricted. Use Maintain>Chart of Accounts Codes>Setup tab to assign one of these designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations.
- If a segment is set up with a function of FND, it can be assigned a designation of N/A or any designation codes you create using the Reports>Assign Report Groups. Use Maintain>Chart of Accounts Codes>Setup tab to assign one of these designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations.
- The General Ledger segment always has a function of N/A. It can be assigned any designation available for the N/A Function. Use Maintain>Chart of Accounts Codes>Setup tab to assign one of the available designations to an account code, or use Reports>Assign Report Groups to assign multiple account codes to one of these designations. For more information about N/A Functions, see Chart of Account Code Designations.

Tip: The segments listed here—and their properties—were entered when this organization was created (File>New Organization).

Organization Information - Modules Tab

Access this tab with Administrative user rights using Organization>Organization Information.

Use this tab to review the modules that are a part of the active organization.

You cannot use this tab to add modules to an organization. When this organization was created (File>New Organization), its modules were assigned. To add more modules, use the Organization>Add a Module wizard. For more information, see "Add a Module Wizard - Module Panel" (page 93). This allows you to add any of your licensed modules to this organization.

Organization Information - Field Lengths Tab

Access this tab with Administrative user rights using Organization>Organization Information.

Use this tab to view the Field Lengths that were designated when the active organization was created (File>New Organization). You cannot change an organization's field lengths; the fields lengths remain the length specified when the organization was created.

Organization Information - Electronic Filing Tab

Access this tab with Administrative user rights using Organization>Organization Information

Use this tab to enter the organization's electronic filing information.

Fields

Contact Information: Enter the appropriate contact information for this organization.

- **Preferred Method of Notification:** Enter how the contact prefers to be notified: P (Postal Service) or E (Email).
- **Name:** Enter the person to be contacted by the Social Security Administration concerning processing problems.
- **Email:** Enter the contact's email address if "E" was selected as the Preferred Method of Notification.
- **FAX:** Enter the contact's fax number, if appropriate.
- **Personal Identification Number:** Enter the organization's personal identification number. This number can be obtained from your taxing authority.

Business Terminated This Year: Select this check box if the business ceased operations during the current tax year.

Other Federal Tax ID Used This Year: Enter any other federal tax ID used for the organization during the tax year.

Third Party Sick Pay Payer: Select this check box if your organization pays sick pay for another organization.

Income Tax Withheld by Third Party Payer: Enter the total federal income tax withheld by third parties (generally insurance companies) from sick or disability payments made to your employees.

Organization Information - Email Setup tab

Access this tab with Administrative user rights using Organization>Organization Information.

Use this tab to enter the information required to send emails from MIP Accounting. You will configure the SMTP (Simple Mail Transfer Protocol) connection for real-time alert notices and emailing forms and reports from the system.

Note: We recommend referring to your IT Technician or System Administrator for help completing the SMTP information.

Email Configuration

Select one of the Email Configuration options for sending emails from the system:

- Use SMTP for all email functions (sending emails and using automated email tools).
- Use Office 365 to send emails. Use SMTP for automated email tools.

Note: Office 365 only supports manual email functions, such as emailing vouchers or invoices. If you want to use automated email functions in MIP Classic (such as Alerts or Report Binder Scheduler), you must set up a standard SMTP connection ***in addition*** to Office 365.

SMTP Connection Setup

SMTP is an Internet standard for email transmission across Internet Protocol (IP) networks. Complete the SMTP settings for sending emails from the system. If you encounter difficulties, you should contact your email client's customer support department.

For steps on how to complete the SMTP setup for a standard service, Gmail, Yahoo, or Office 365, see "Configuring SMTP" (page 31).

For some common topics to help you set up your SMTP server, see "Setting Up SMTP" (page 23).

- **Server:** Enter the server name of the SMTP service used to process outgoing email, for example, SMTP.gmail.com.

- **Port:** Enter the port that accepts outgoing email requests. This port number should match the port configured on your SMTP service. By default, the system displays 25 as the port number.
- **Enable SMTP over Transport Layer Security (STARTTLS):** If your SMTP service supports SSL (Secure Sockets Layer), select this check box to securely send email notifications. TLS is a way of changing data into code as it travels across the internet; so that the data will be secure and private. It is recommended that you securely send your information via email; otherwise, the SMTP service sends all email as cleartext, which is not secure. We recommend selecting this check box; otherwise, your emails are not secure and data will be emailed as cleartext which is not secure.
- **Use Custom Credentials:** If your SMTP service requires authentication, select this check box to enter the credentials to connect to the SMTP service.
  - **Username, Password:** Enter the user name and password associated with the SMTP service.

Important! If using Custom Credentials, the Username must match the “From” email address used by the Administrator on the Options>System Preferences for Alerts, Maintain>Email Template for the Accounts Receivable Invoice, Maintain>Payroll>Email Template for the Payroll Voucher formats, and Reports>Report Binder>Set Up Scheduler Email for the Report Binder Scheduler. You cannot use a Username with a someone else's email address when the Use Custom Credentials check box is selected. Everything must match the system.
We recommended that the Organization create a general organization email account for everyone to use.

Test SMTP Connection: The From and To addresses will be used when the **Send Test Email** button is clicked. It is recommended that you test the SMTP Connection to make sure the information was set up correctly.

- **From:** Enter an email address to test where the email is coming from. If the email fails, this is the address that will receive the failure notification.
- **To:** Enter an email address to test where the email will be received. If the email is successful, this is the address that will receive the test email.
- **Send Test Email:** Click this button to test the email connection.

Note: We recommended that you keep a From and To email address to verify the connections. If these email address fields are left blank, when the *Send Test Email* button is selected, the system will only verify that the Server, Port, and User and Password fields have information but a test email will not be sent when the automated processes are performed.

Notes:

- Open Maintain>Email Templates to create default email preferences for your A/R Invoices. This includes entering a default “From” email address for your invoices.
- Report Binders do not use default email preferences; however, each binder must have a defined email distribution list. Use Reports>Report Binder - Set Up Scheduler Email to enter email addresses.
- After your Administrator has installed the Alert Server and entered your SMTP information into the Organization Information>Email Setup tab, they will need to set up a default From Email address using Options>System Preferences and select the Real-time Notices Email and/or In-product check boxes on the Set Up Alerts form (Organization>Set Up Alerts).
- After you have set up SMTP Email and created default Email Templates, you can then decided which customers you want to receive invoices by email using the Maintain>Accounts Receivable>Customers>Email tab.

Setting Up SMTP

Below are some topics to help you set up your SMTP Server.

Steps to locate your Email Server information if using Microsoft Outlook 2010, 2013, or 2016

- Close Microsoft Outlook 2010, 2013, or 2016.
- In Control Panel, click or double-click Mail. (You may need to click the **View by:** drop-down list and select *Large icons* or *Small icons*):
- The Mail Setup - Outlook form displays, click E-mail Accounts.
- On the Email tab, the Name and Type displays. The Name is the user name of the person whose Outlook is being viewed. The Type is the Server that is being used for Email. This could be Microsoft Exchange, POP3/SMTP, or IMAP.

- a. If Microsoft Exchange or IMAP is used, contact your IT department or ISP (Internet Service Provider) and find out your SMTP Server information.
- b. If SMTP is used, copy and paste the Server Name into the MIP Accounting system using Organization>Organization Information>Email Setup tab

Steps to locate your Email Server information if using Microsoft Outlook 2007

- Open Microsoft Outlook 2007.
- Select Tools>Account Settings. The Account Settings form displays.
- On the Email tab, the Name and Type displays. The Name is the user name of the person whose Outlook is being viewed. The Type is the Server that is being used for Email. This could be Microsoft Exchange, POP3/SMTP, or IMAP.
  - a. If Microsoft Exchange or IMAP is used, contact your IT department or ISP (Internet Service Provider) and find out your SMTP Server information.
  - b. If SMTP is used, copy and paste the Server Name into the MIP Accounting system using Organization>Organization Information>Email Setup tab.

Using SMTP for Real-time Alert Notices

If you want to alert users with Real-time email or in-product notices, your Administrator will need to complete the Alert Server (IIS) installation and set up the Email Setup tab using the Organization>Organization Information form; before setting up Alerts.

Before setting up the SMTP connection information, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.
- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?
- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?

- If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.

- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google GMail and AOL accounts can be used as an IMAP account.

After you have installed the Alert Server and entered your SMTP information into the Organization>Organization Information>Email Setup tab, you will need to set up a default From Email address using Options>System Preferences and select the Real-time Notices Email and/or In-product check boxes on your Set Up Alerts form (Organization>Set Up Alerts).

For more information on SMTP, see "Configuring SMTP" (page 31).

Using SMTP to Email Report as PDF File

If you use Email Report as PDF File on reports, the Administrator will need to set up the Email Setup tab using the Organization>Organization Information form.

Before this can be set up, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.
- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?
- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?
  - If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.
- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google GMail and AOL accounts can be used as an IMAP account.

After you have entered your SMTP information into the Organization>Organization Information>Email Setup tab, every time you use Email Report as PDF File on a report, you will need to enter the To and From email addresses, Subject, and Message (Reports>{Any report}> Email Report as PDF File).

For more information on SMTP, see "Configuring SMTP" (page 31).

Using SMTP to group reports together to be emailed as a PDF File

If you use Reports>Report Binder to group reports together and then click Email Report as PDF File , the Administrator will need to set up the Email Setup tab using the Organization>Organization Information form.

Before this can be set up, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.
- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?
- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?
  - If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.
- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google GMail and AOL accounts can be used as an IMAP account.

After you have entered your SMTP information into the Organization>Organization Information>Email Setup tab, every time you use Email Report as PDF File on a group of reports, you will need to enter the To and From email addresses, Subject, and Message (Reports>Report Bindger> Email Report as PDF File).

For more information on SMTP, see "Configuring SMTP" (page 31).

Using SMTP to schedule a group of reports to be emailed

If you want to schedule a group of reports to be emailed, the Administrator will need to set up the Email Setup tab using the Organization>Organization Information form.

Before this can be set up, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.
- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?
- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?
  - If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.
- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google Gmail and AOL accounts can be used as an IMAP account.

For more information on SMTP, see "Configuring SMTP" (page 31).

Using SMTP to send A/P Electronic Payment notifications to Vendors

If a vendor has requested to receive their A/P electronic payment notification via email, your Administrator will need to set up the Email Setup tab using the Organization>Organization Information form.

Before setting up the SMTP connection information, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.

- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?
- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?
  - If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.
- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google GMail and AOL accounts can be used as an IMAP account.

After you have entered your SMTP information into the Organization>Organization Information>Email Setup tab, you will need to check the Send Payment Notification Email to EFT Vendors and enter a general message (Organization>Set Up Modules>Electronic Funds Transfer - Email tab) and enter the Payment Information Email Address for each vendor (Maintain>Accounts Payable>Vendors>Payments and Terms tab). A notification is sent after the electronic payment file is processed using Activities>Accounts Payable>Create/Send A/P Electronic Payments.

For more information on SMTP, see "Configuring SMTP" (page 31).

Using SMTP to email Direct Deposit Vouchers to Employees

If an employee has requested to receive their pay stub via email, instead of or in addition to printing, your Administrator will need to set up the Email Setup tab using the Organization>Organization Information form; before setting up the Email Templates and Employee Information emails.

Before setting up the SMTP connection information, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.

- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?
- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?
  - If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.
- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google GMail and AOL accounts can be used as an IMAP account.

After you have entered your SMTP information into the Organization>Organization Information>Email Setup tab, you will need to set up a default Email Template for both your Voucher (Maintain>Payroll>Email Templates) and select the Email check box, enter the email address, and accept the <Default> Template for Vouchers for each employee (Maintain>Payroll>Employee Information>Email tab).

For more information on SMTP, see "Configuring SMTP" (page 31).

Using SMTP to email A/R Customer Invoices or Statements

If a customer has requested to receive their A/R invoices or statements via email, instead of or in addition to printing, your Administrator will need to set up the Email Setup tab using the Organization>Organization Information form; before setting up the Email Templates and Customers Email tab.

Before setting up the SMTP connection information, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.

- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?
- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?
  - If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.
- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google GMail and AOL accounts can be used as an IMAP account.

After you have entered your SMTP information into the Organization>Organization Information>Email Setup tab, you will need to set up a default Email Template for both your A/R Invoices and Customer Statements (Maintain>Email Templates) and select the Email check box, enter the email address, and accept the <Default> Template for Invoices and/or Customer Statements for each customer (Maintain>Accounts Receivable>Customers>Email tab).

For more information on SMTP, see "Configuring SMTP" (page 31).

Using SMTP to send status notifications to Requisition Users

If you want the system to send emails to users notifying them about the status of certain requisitions, the Administrator will need to set up the Email Setup tab using the Organization>Organization Information form.

Before this can be set up, you will need to know the answers to the following questions:

- What type of Server does the organization use to send email? Microsoft Exchange, POP3/SMTP, and IMAP.
- If POP3/SMTP server is used:
  - What is the Logon Information: User Name and Password?
  - Is it required to logon using Secure Password Authentication (SPA)?

- If Microsoft Exchange server is used:
  - Is your exchange server an SMTP Server? If so, do you have an IT person who could help with connecting to it?
  - If the Exchange Server is not an SMTP Server, Outlook (client) uses Exchange Server (server) to send emails, you should contact your Internet Service Provider or email administrator to ask if your account has access to an SMTP Server.
- An IMAP account is an enhanced type of email account that provides multiple mail folders on a mail server. Both Google GMail and AOL accounts can be used as an IMAP account.

After you have entered your SMTP information into the Organization>Organization Information>Email Setup tab, you will need to set up the Requisition Email Options (Organization>Set Up Modules>Electronic Requisitions and set up requisition users email options (Security>Requisitions>Set Up Requisition Users - Email tab).

For more information on SMTP, see "Configuring SMTP" (page 31).

Configuring SMTP

The following steps show how to complete the SMTP setup for a standard service, Gmail, Yahoo, or Office 365. If you encounter difficulties, you should contact your email client's customer support department.

Standard SMTP Settings:

To set up a typical SMTP service with Administrative user rights, complete the following steps:

1. Select Organization>Organization Information>Email Setup tab.
2. Enter the SMTP server name.
3. For the Port, accept the default of 25.
4. If your SMTP service supports SSL, select this check box to securely send email notifications. If this check box is not selected, the SMTP service sends all email as cleartext, which is not secure.
5. If your SMTP service needs authentication, select the Custom credentials check box and enter your user name and password. You will need to enter this user's email address in all the associated "From" email address fields.
6. Click the Save button.

7. It is recommended that you enter a From and To email address, and click the Send Test Email button to test the SMTP connection is set up correctly. These addresses will be used when the **Send Test Email** button is clicked; to test that your connection is set up correctly.

Gmail Settings:

To set up a Gmail SMTP service with Administrative user rights, complete the following steps:

1. Select Organization>Organization Information>Email Setup tab.
2. Enter the SMTP server name for Gmail: smtp.gmail.com.
3. For the Port, enter 587.
4. Select the check box to Enable SMTP over Transport Layer Security (STARTTLS). This will securely send email notifications. If this check box is not selected, the SMTP service sends all email as cleartext, which is not secure.
5. Select the Use Custom Credentials check box and enter your Gmail user name (including "@gmail.com") and password. You will need to enter this user's email address in all the associated "From" email address fields.
6. Click the Save button.
7. It is recommended that you enter a From and To email address and click the Send Test Email button to test the SMTP connection is set up correctly. These addresses will be used when the **Send Test Email** button is clicked; to test that your connection is set up correctly.

Yahoo Settings:

To set up a Yahoo SMTP service with Administrative user rights, complete the following steps:

1. Select Organization>Organization Information>Email Setup tab.
2. Enter the SMTP server name for Yahoo, smtp.mail.yahoo.com.
3. For the Port, enter 587.
4. Do NOT select to Enable SMTP over Transport Layer Security.
5. Select the Use Custom Credentials box and enter your Yahoo user name (including "@yahoo.com") and password. You will need to enter this user's email address in all the associated "From" email address fields.
6. Click the Save button.

7. It is recommended that you enter a From and To email address and click the Send Test Email button to test the SMTP connection is set up correctly. These addresses will be used when the **Send Test Email** button is clicked; to test that your connection is set up correctly.

Office 365 Settings:

To set up Office 365 emailing with Administrative user rights, complete the following steps:

1. Select Organization>Organization Information>Email Setup tab.
2. Select the "Office 365" option.
3. Send a test email under "Test SMTP Connection".
4. A window will open for you to log into your Office 365 account. Enter your Office 365 account information and sign in. The email address you select will appear as the "From:" address for any emails sent using MIP automated email functions.

Note: Office 365 only supports manual email functions, such as emailing vouchers or invoices. If you want to use automated email functions in MIP Classic (such as Alerts or Report Binder Scheduler), you must set up a standard SMTP connection ***in addition*** to Office 365.

Organization Preferences

Use this form to set up the following transaction entry options:

- posting status
- valid/invalid codes
- entry date warnings
- session and document ID values

Once you save them here, they are in effect when you enter transactions in the system.

Organization Preferences - Processing Tab

Access this tab with Administrative user rights using Organization>Organization Preferences.

Use this tab to select the transaction Processing Mode you want to use for the current organization. You can also activate the Documentation ID control, summarize transaction entries, and transfer assets to Sage Fixed Assets.

You can also specify whether you want to set up Account Code Combinations. Account Code Combinations affect transaction entry in the system; they create additional safeguards against transaction entry error. When you set up account code combinations, the system makes sure the proper combinations are enforced during transaction entry. Users cannot enter invalid combinations.

If you select the Valid Account Combinations option, you cannot enter transactions until you have specified which combinations are valid. Use Maintain>Account Code Combinations to set up valid account code combinations.

Fields

Processing Mode Batch, On-Line, Combined: Select a processing mode, which will determine the posting status available for transaction entry sessions in the MIP Accounting system. You can change the processing mode at any time, as long as transaction entry is not in progress.

Enable Document ID Control: Select this check box to allow multiple users in different sessions to auto increment document IDs.

Summarize Transaction Entries: Select this check box to combine the detail transaction lines in the Transactions>Transaction Entry forms. The lines are summarized after clicking Use Offsets or when using the Use Distribution Code process. The system automatically summarizes all system generated, fixed assets, and allocation transactions, regardless if this box is selected.

Account Code Combinations Options: Account code combinations allow you to specify which codes are valid or invalid with other codes during transaction entry.

- Leave the default selected—No Account Combinations—if you do not want to set up account code combinations in the MIP Accounting system.
- If you want to use account code combinations, specify whether they are valid or invalid combinations. You then need to set up the combinations in the MIP Accounting system (Maintain>Account Code Combinations), in order for the Transaction Entry forms to function properly.

Account Code Combinations Segments: Select the segments to be used in the valid or invalid account code combinations. If used, your account combinations must include at least two segments and you can have as many as nine.

Remember, the more segments you include in the account combinations, the more time is required to set up the account combinations. Therefore, plan carefully before deciding which segments to include in your account combinations.

Verify Account Code Combinations during Setup, Transaction Entry, and Processing: Select this check box to activate account code combinations in the MIP Accounting system. The system then checks for proper account code combinations during setup, transaction entry, and processing. Consequently, this affects system generated checks. It also affects entries created during the Allocation Management (JVA), A/R Billing (ARB), and Fixed Assets (JVD) processes. Please note that this feature does not apply to any Budget transactions. Note that if you use account code combinations, this box is rarely, if ever, cleared.

Transfer to Sage Fixed Assets: Use this group box to set up the features for transferring your assets to Sage Fixed Assets. The Sage Fixed Assets product must be installed in order to select the database and unit. These fields are only available if the organization's functional currency is USD (US Dollar).

- **Enable Sage Fixed Assets Quick Entry:** Clear this check box if you do not want to enable the Sage Fixed Assets Quick Entry feature. If it is selected, the system activates the following forms:
  - Transactions>Enter Cash Disbursement>Sage Fixed Assets Quick Entry
  - Transactions>Accounts Payable>Enter A/P Invoices>Sage Fixed Assets Quick Entry
  - Activities>Check Writing>Write Checks>Sage Fixed Assets Quick Entry
  - Activities>Accounts Payable>Transfer to Sage Fixed Assets
- **Database, Organization Unit:** Select an existing Sage Fixed Assets database or accept <default>. Select a unit name to serve as the default when you transfer assets (Activities>Accounts Payable>Transfer to Sage Fixed Assets). You can select a different unit when you transfer.

Tips:

- When you enter information on this form, it is available in the MIP Accounting system the next time a user opens the active organization. If you want to make changes to an organization that is currently open, the organization must be closed before you can make the changes.
- Currency fields follow the formatting of the organization's functional currency. The functional currency was determined when the organization was created (File>New Organization>Functional Currency panel).

Auto-Increment Feature

As the Administrator, you can set up the auto-increment feature so that it can be used in many forms throughout the system. Simply press the + key to have the system automatically display the next available number.

- To set up the numbers for this feature during transaction entry, use Organization>Organization Preferences.
- To set up the numbers for this feature when creating requisitions, use Organization>Set Up Modules>Requisitions.
- To set up the numbers for this feature when creating purchase orders, use Organization>Set Up Modules>Purchase Orders.

If you enter an entry that ends with an alpha character, the auto-increment will append it with the number 001 and then increment that number. For example, enter "A7C" as the last purchase order number and when you press the + key, the system will display A7C001 - then A7C002, and so on.

Account Code Combinations Setup

As the Administrator, using the account code combinations feature (which you select on the Organization Preferences form) is entirely optional. If you have a relatively simple accounting structure and a low probability of entry error, you may elect not to use the feature.

However, if you elect to use account combinations, choose the approach that is easier to set up and maintain. In other words, if most of the account combinations you can create with your account structure are valid, choose to set up invalid combinations. If most of the account combinations are invalid, set up valid combinations.

Indicate the following information on the Organization Preferences>Processing tab:

- Whether you want to use no account code combinations, valid combinations, or invalid combinations.
- Which segments comprise account code combinations (note that you are limited to 9 segments for account code combinations).
- Whether you want the system to "Verify Account Combinations".

You can change the selections you make on this tab at any time. However, if you set up account code combinations, then change the selection to "No Account Combinations," the account code combinations that you set up are deleted.

Instead, you can disable, or temporarily turn off the account code combinations you have set up by clearing the Verify Account Combinations box. Remember to turn the verification process back on when you are ready to activate account code combinations again.

Processing Mode Options

The Processing Mode option that you select (on the Organization Preferences form) determines which posting status is available for transaction entry sessions in the MIP Accounting system. Below you will find the Processing Mode options:

- If you select **Batch** processing mode, you can choose a status of Batch-To Post or Batch-To Suspend posting in the MIP Accounting system.
- If you select **On-line** processing mode, you can only choose a status of On-line posting in the MIP Accounting system.
- If you select **Combined** processing mode, you can choose any of the three posting statuses: Batch-To Post, Batch-To Suspend, or On-line posting in the MIP Accounting system.

Consider this when choosing a processing mode:

- *Do you want to give your transaction entry personnel the ability to both enter and post a transaction?* If not, then you might want to select Batch as your processing mode, and limit personnel to the Transactions menu (Security>Set Up Organization Menus).
- *Do you have a need for up-to-the-minute account balances?* If so, choose On-line or Combined as your processing mode.

There are three posting statuses in the MIP Accounting system. Here is how you post them:

- Batch-To Post sessions are posted using Activities>Manage Sessions>Post Transactions.
- Batch-To Suspend sessions are suspended and cannot be posted until you change them to either Batch-To Post or On-line Posting.
- On-line Posting sessions are posted as they are entered.

Budget and Payroll Users

The transactions created in the Payroll module, as well as those created using Activities>Budget Worksheet, are always processed in Batch mode, regardless of which processing mode is selected on the Organization Preferences form.

Order Entry Users

The transactions created using Activities>Accounts Receivable>Customer Returns and Sales Order Fulfillment; and Activities>Purchase Orders>Process Receipts and Adjust Receipts; are always processed in On-line mode, regardless of which processing mode is selected on the Organization Preferences form.

Organization Preferences - Entry Dates Tab

Access this tab with Administrative user rights using Organization>Organization Preferences.

Use this tab to create warnings and limits for transaction entry in the system. When you enter a date here, the system warns or prohibits users when they try to enter transactions with an Effective Date that is outside the specified date.

Prohibit and Warn dates do not apply to the following forms, since they automatically generate entries:

- A/P System Generated Checks and Vouchers (Activities>Check Writing>Write Checks or Void Checks/Vouchers/Invoices or Activities>Accounts Payable>Pay Selected A/P Invoices)
- A/R System Generated Invoices (Transactions>Accounts Receivable>Edit A/R Invoices
- Receipt Writing (Activities>Receipt Writing)
- System Close Year End (Activities>Close Fiscal Year)

Fields

Transaction: The system displays all transaction entry forms that require a document date or an effective date.

Prohibit Prior To: Enter a date, or use the calendar control to select a new date. During transaction entry, if you enter an Effective Date that is prior to the date in this column, the system displays an error message and does not allow the transaction to be entered.

Warn Prior To: Enter a date, or use the calendar control to select a date. During transaction entry, if you enter an Effective Date that is prior to the date in this column, the system gives you a warning, but still allows you to enter the transaction.

By default, the Prohibit/Warn Prior To date is the first day of the fiscal year that was specified when the organization was created (File>New Organization). Consequently, users are warned if they try to enter a transaction for the previous fiscal year. However, you can change or delete these default dates.

Warn After: Enter a date, or use the calendar control to select a date. During transaction entry, if you enter an Effective Date that is after the date in this column, the system gives you a warning, but still allows you to enter the transaction.

By default, this date is the last day of the fiscal year that was specified when the organization was created (File>New Organization). Consequently, users are warned if they try to enter a transaction for the previous fiscal year. However, you can change or delete these default dates.

Prohibit After: Enter a date, or use the calendar control to select a date. During transaction entry, if you enter an Effective Date that is after the date in this column, the system displays an error message and does not allow the transaction to be entered.

Tips:

- For Void Checks, the system uses the "New Effective Date" or the "Original Effective Date" when checking for the Prohibit and Warn dates entered on this tab.
- For the dates you enter on this tab to be effective, the Prohibit Prior To date should be the earliest date entered in one row. Similarly, the Prohibit After date should be the latest date entered in one row.
- Once you have created your organization, remember to keep these dates current.
- The Close Fiscal Year and the updated database process (Activities>Close Fiscal Year) updates the entry dates on this tab.

Organization Preferences - Session Tab

Access this tab with Administrative user rights using Organization>Organization Preferences.

Use this tab to view or change the Last Session ID number used for each transaction type (such as, Cash Disbursements and Journal Vouchers) in the MIP Accounting system.

Fields

Transaction: The system displays certain transaction entry types that require a Session ID.

Last Session ID: This column lists the Last Session ID number that was used on each transaction entry Session form in the MIP Accounting system.

The numbers listed here are the basis for the auto-increment feature, which is available on Session forms in the MIP Accounting system. If a cell is left blank, the default auto-increment number of 001 is used.

To use the auto-increment feature, simply press the "+" key when your cursor is in an empty Session ID box. The system automatically enters the next available Session ID—that is, one number larger than the numbers listed on this tab—and updates the number listed on this tab.

Tip: Refer to the "Organization Preferences - Document Number Tab" (page 41) for information on using the auto-increment feature during transaction entry.

Organization Preferences - Document Number Tab

Access this tab with Administrative user rights using Organization>Organization Preferences.

Use this tab to view or change the Last Document Number used for some transaction types (such as Cash Receipts and Journal Vouchers) and system generated Edit Payroll type checks in the Payroll module.

Fields

Transaction: The system displays certain transaction entry types that require a document number.

Last Document Number: This column lists the last document number. The numbers listed are available on some document forms in the system and the system generated Edit Payroll type checks in the Payroll module. In order for the system to keep track of the Last Document Number, the "Enable Document ID Control" check box must be selected on the Processing tab. If this check box is not selected, the system disregards any numbers entered here.

Tip: You can set the Last Used Check Number for General Ledger type cash accounts (used when printing checks, such as Transactions>Enter Cash Disbursements, Transaction>Accounts Payable>Enter Manual A/P Checks, and Activities>Check Writing>Write Checks) using the Maintain>Chart of Accounts Codes form.

Chapter 3: User and Group Security

Maintain Users

Access this form with Administrative user rights using Security>Maintain Users.

Use this form to perform one of the following tasks:

- Enter a new user;
- Change an existing user's status, name, email address, organizations, and/or password;
- Limit a user's access to balances and reports (if Executive View User is installed);
- Hold a Requisitions license for a user (if Electronic Requisitions is installed); and
- Delete a user from all organizations.

Once a user is created, it is available (in the User ID drop-down list on the Maintain Users form) for the active organization and any existing organizations. In order to apply this user to an organization, select the User ID then move the active organization over to the Selected Items box. The user can be denied access to an organization by moving the organization back to the Available Items box. When you enter new users, you are adding them to all organizations in the Selected Items box.

A new user does not have any security rights. Therefore, you need to set up its security in each organization using Security>Set Up System Menus and Set Up Organization Menus, respectively. Use the Set Up System Menus form to assign rights to Backup, Restore, and so on. Use the Set Up Organization Menus form to assign access to Administration, Accounting, and Payroll (if applicable) menu selections in which you want new users to have access.

Human Resource Management Users

Click the Change Password button to assign a new password or change an existing password for both MIP and HR Management systems. Select the HR Management User check box to grant users access to the HR Management module. It is only available if the Human Resource Management and Payroll modules are installed. When an MIP user, with the HR Management User check box selected, status is made Inactive, that user's access in HR Management will also change to "No Access."

Nonprofit Online Users

In order to change your password, press Ctrl+Alt+End on your keyboard, and select “Change a password.” See Nonprofit Online.

Fields

NPS Training Organization (NTO): This is a training organization provided to all customers using MIP. Therefore, all users of MIP have access to this database and it cannot be removed. Users are granted full access to this training organization.

User ID: Enter or select a unique ID that represents the user being added or modified. We recommend limiting your entry to strictly alphabetic characters (A through Z) or numeric characters (0 through 9), and avoid using symbols.

Status: Specify the status of the User ID. When creating a new ID, accept the default status, A (Active), or select I (Inactive) from the drop-down list. A status of discontinued is not available on this form. Note that inactive users cannot log on to the system.

User Name: Enter the user name, such as First, Middle, and Last Name

Email: Enter the user's email address, if applicable.

Executive View User: Select this check box to indicate that a user only has executive view rights. This option only displays if the Executive View module is installed.

An Executive View user only has access to reports, balances (Activities>Display Balances), and budget worksheets (Activities>Budget Worksheet). Therefore, the system only displays those menu items on the Security>Set Up Organization Menus form. With executive view, you can assign an unlimited number of users; however, you are limited to the number of licenses purchased for the Executive View User (as determined by your Activation Code). This user is independent from the number of concurrent users logged on to the system. (Concurrent users are the number of simultaneous users accessing the program; which is based on the number of users purchased with the software license.)

Requisition User: Select this check box to hold a license for this user in the Electronic Requisitions module. Remember to enter the user name specified here when logging on to Electronic Requisitions. This option only displays if the Electronic Requisitions module is installed.

HR Management User: Select this check box to indicate that a user has rights to the HR Management module. This option only displays if the Human Resource Management and Payroll modules are installed.

Organization ID Available Items, Selected Items: In the Available Items box, select the organization ID to be applied to the user, and then click the Mover (>) to move the item to the Selected Items box. The Available Items box displays all registered organization IDs.

Tips:

- To print a list of users and other data entered on this form, use Reports>Lists>User Information and Reports>Lists>Security.
- We recommend that you create all organizations (File>New Organization) before creating users on this form.
- An organization does not have to be open in order to add users.
- The system provides a default user—whose user ID is "NPS"—with the sample organization "NTO." User NPS is initially assigned no password, but we recommend assigning it a unique password and use it as the System Administrator ID.
  If you decide to require passwords for your users (Options>System Preferences), a password must be added for the user NPS (and any other existing users) or the NTO database cannot be accessed.
- A user is required to enter that password every time they open the system.
- User IDs and user names are significant for two reasons:
  - First, you must set up security (Security>Set Up System Menus and Set Up Organization Menus) on the basis of User ID.
  - Second, the system tracks and logs system activity by User ID. This provides an audit trail of activity for later use.
- When setting up security for users (Security>Set Up System Menus and Set Up Organization Menus), limit access to this form to include only system administrator-type users.
- If a user is deleted, it is removed from all organizations, not just the active organization.
- To change the email address of the person logged on to the system, use Options>User Preferences.
- When adding a module, the current user is granted all rights for the new module in the active organization.
  - Remember to open each organization and add the module and security rights for each user. Use Security>Maintain Groups to expedite this process.
  - When an organization is created or a module is added to an active organization, the system automatically assigns the organization-related security to the user who is currently logged on.

- A user must be assigned to an organization before their Organization Security rights can be modified.
- An Executive View User can be included in Groups. Even if you are part of a group with access to various forms, you will still be limited to what you can use.
- A user can be set up as a regular user, changed to an executive view user (by selecting Executive View User), and back to a regular user (by clearing Executive View User) without losing their original rights.

Password requirements:

- Include at least one uppercase and one lowercase letter
- Include at least one number
- Cannot contain spaces at the beginning or end
- Cannot be one of the last 6 passwords used

Maintain Users Buttons

	Rename User ID: Use this button to change the ID for an existing user.
	Import Windows Authentication User: Use this button to import individual users from your network. This button is only available if the Use Windows Authentication check box was selected by the Administrator on the Options>System Preferences form.
	Change Password: Use this button to add or change the password for a user.

Rename User ID

Access this form with Administrative user rights using Security>Maintain Users> Rename User ID.

Use this form to rename a User ID. This would be helpful if, for example, an employee changed her name through marriage.

Fields

Current User ID: Select an existing user from the drop-down list.

New User ID: Enter a new, unique user ID name. The Drop-Down Lookup displays existing User IDs that are already in use and cannot be used. We recommend using all numeric IDs. Numeric IDs are generally easier and faster to enter during transaction entry. We also recommend limiting your entry to strictly alphabetic characters (A through Z) or numeric characters (0 through 9), and avoiding the use of symbols.

Password

Access this form with Administrative user rights using the Security>Maintain Users or Options>User Preferences>Change Password button.

Use this form to assign a new password or change an existing password. A password can also be changed using either Security>Maintain Users or Options>User Preferences.

Nonprofit Online Users

In order to change your password, press Ctrl+Alt+End on your keyboard, and select “Change a password.” See Nonprofit Online

Fields

Old Password: Enter the user's existing password, so it can be changed to a new password.

New Password: Enter a new password. The system displays asterisks as it is entered.

Confirm: Retype the new password to confirm it.

Password requirements:

- Include at least one uppercase and one lowercase letter
- Include at least one number
- Cannot contain spaces at the beginning or end
- Cannot be one of the last 6 passwords used

Maintain Groups

Access this form with Administrative user rights using Security>Maintain Groups.

Use this form to set up or edit a group of users in the active organization only (the organization currently open).

Then, use Security>Set Up Organization Menus to set up organization security for the group and its users. For example, suppose you have 10 A/P clerks who have the same rights. You can set up a group, called "A/P Clerks" that includes all 10 clerks. Then, set up rights for the group (Security>Set Up Organization Menus). That way, you do not have to go set up the same rights 10 times.

Nonprofit Online Users

MIP manages the creation and deletion of user accounts through Active Directory. Please contact Customer Support via web ticket, chat, or phone. See contact information and support hours on the Support Resources page. For more information, see Nonprofit Online.

Fields

Group ID: Enter an ID for the new group being created.

Group Name: Enter a group name for the associated ID.

User ID Available Items, Selected Items: In the Available Items box, select an *active* user ID to be applied to the group, and then click the Mover (>) to move the item to the Selected Items box. The Available Items box displays all user IDs to be included in the new group.

Tips:

- To print a list of users or groups and other data which entered on this form, use Reports>Lists>Group Information, User Information, and Security.
- Click Copy to make a copy of a group and its users.
- We recommend using all numeric IDs. Numeric IDs are generally easier and faster to enter during transaction entry. Otherwise, we recommend at least limiting your entry to strictly alphabetic characters (A through Z) or numeric characters (0 through 9), and avoiding the use of symbols, such as: | " [ ] ' ; #.
- Groups are not used on the Security>Set Up System Menus form.
- Groups can only contain users; not other groups.
- Groups cannot log on to the system.
- If a group is deleted, it is only removed from the active organization.
- When setting up security for groups (Security>Set Up Organization Menus), we recommend limiting access to this form to include only system administrator-type users.

Maintain Groups Buttons

	Copy Groups: Use this button to copy groups and their users.
	Import Windows Authentication Groups: Use this button to import groups and their users from your network. This button is only available if the Use Windows Authentication check box was selected by the Administrator on the Options>System Preferences form.

Copy Groups

Access this form with Administrative user rights using Security>Maintain Groups> Copy.

Use this form to copy groups and their users. This process does not copy their security. Use Security>Set Up Organization Menus to copy the organization security for a group and its users.

Fields

Copy From Group ID: Select the existing group ID that you want to copy.

Copy To Group ID, Name: Enter the ID and name for the new group. The Drop-Down Lookup displays existing Group IDs that are already in use and cannot be used again. We recommend using all numeric Names. Numeric names are generally easier and faster to enter during transaction entry. We also recommend limiting your entry to strictly alphabetic characters (A through Z) or numeric characters (0 through 9), and avoiding the use of symbols.

Set Up System Menus

Access this form with Administrative user rights using Security>Set Up System Menus.

Use this form to grant system security rights to a specific user. Rights are assigned to the selected user for the active organization (the organization currently open).

System rights are limited to areas that are not organization-specific. Therefore, the MIP Accountingsystem is not available, and rights can only be granted to the Administration menus that apply to the NPSSQLSYS database.

System security rights include all menu selections in the File, System, and Options menus. The Security, Organization, and Reports menus are limited to the following menu selections:

- Security>Maintain Users and Set Up System Menus
- Organization>Default Table Structure
- Reports>Lists>User Information

Note: A user has no rights in an organization until you open the organization and assign the rights using Security>Set Up Organization Menus.

Fields

ID: Select an existing user from the drop-down list. The user was created on the Security>Maintain Users form.

Set Up Menus Box: This box displays the MIP Accounting menus specific to system administrator-type users.

Double-click on an item—or single-click on the plus (+) sign next to the item—to expand the outline. When an item has been expanded, the plus (+) sign becomes a minus (-) sign. To collapse an item, simply double-click its name, or single-click the minus sign.

To the right of each item, the system displays the letters V, E, D, A, and P. These letters indicate which rights the user has for that particular menu selection. They appear black if all of the sub-levels are assigned, and gray if only some of the sub-levels are assigned. The letters do not appear at all if none of the sub-levels are assigned. The rights are abbreviated as outlined below.

Rights: Highlight a menu selection in the Set Up Menus box, then select the check boxes to grant the user various rights.

- **View Existing Records:** This option allows the user to open and review a previously entered item,
- **Edit Existing Records:** This option allows the user to change information for a previously entered item,
- **Delete Existing Records:** This option allows the user to delete a previously entered item, thus removing it from the database,
- **Add New Records:** This option allows the user to enter new items, and
- **Process Records:** This option allows the user to perform a process.

Description: The system displays a description of each menu selection, as it is highlighted.

Tips:

- To print a list of users and other data which entered on this form, use Reports>Lists>Security List and Reports>Lists>User Information List.
- Groups are not available on this form.
- An organization does not have to be open in order to grant system rights.
- Click Copy to make a copy of a user's system security to be used for a different user.
- To remove all rights for a user, select each menu selection and then clear all check boxes, or delete the user using Security>Maintain Users.
- Some rights depend on other rights; the system automatically selects or clears options. For example, if you select the Edit check box, the system selects the View check box too.
- Be sure to limit the right to set up security to appropriate users. Otherwise, a user can gain unauthorized access by simply changing his own security rights.
- You can assign rights to a main menu to give the user rights to all of those menus' selections. For example, if you select System and assign rights, those rights are applied to all available menu selections in the System menu.
- A user cannot be added using this form. Use Security>Maintain Users to add a new user.

Copy System Security

Access this form with Administrative user rights using Security>Set Up System Menus> Copy.

Use this form to copy the system security rights for the selected user to a different user.

Fields

Copy From User ID: Select an existing user ID that you want to copy.

Copy To User ID: Select an existing ID for the user that has the same security settings as the Copy From User ID.

Set Up Organization Menus

Access this form with Administrative user rights using Security>Set Up Organization Menus.

Use this form to set up security rights for a user or group in the active organization (the organization currently open). This form allows rights to be granted to organization-specific menus. A user has no rights in an organization until you open the organization and assign the rights on this form.

If a user is selected that is part of a group and the Display All Rights check box is selected, the Set Up Menus box includes both the user's individual and group rights—referred to as cumulative rights. Cumulative rights are security rights assigned to a group and to a user within the group, that are combined with no precedence.

Note: If the user selected is not a part of a group and the Display All Rights check box is selected, you will not be able to edit the security rights because the system cannot save your selections.

Executive View Users

If you logged on as an Executive View user, the system only displays the Display Balances and Reports menus along with Budget Worksheets.

Fields

Type: Either select "User" or "Group" to determine if the system should display a list of users or groups in the ID drop-down list.

ID: Select a user or group in which to assign organization rights.

- If "User" is selected in the Type box, the drop-down contains existing users in the active organization.
- If "Group" is selected in the Type box, the drop-down contains existing groups for the active organization.

All groups were created using Security>Maintain Groups, while users were created using Security>Maintain Users.

Display All Rights: For Type *User*, select this check box to display all of the user's individual rights at the same time, including the rights for any groups in which they belong. Note that the Rights check boxes are not available for editing and the Save button is disabled.

Note: If "Group" is the Type, this check box is not available, however, the Rights check boxes are available; making the security rights editable.

Set Up Menus Box: This box displays the MIP Fund Accounting menus.

- Double-click on an item–or single-click on the plus (+) sign next to the item–to expand the outline. When an item has been expanded, the plus (+) sign becomes a minus (-) sign. To collapse an item, simply double-click its name, or single-click the minus sign.
- To the right of each item, the system displays the letters V,E, D, A, P, and S. These letters indicate which rights the user has for a particular menu selection. The letters appear black if all of the sub-levels are assigned, and gray if only some of the sub-levels are assigned. The letters do not appear at all if none of the sub-levels are assigned. The rights are abbreviated as outlined below.

Rights: Highlight a menu selection in the Set Up Menus box, then select the check boxes to grant the user or group (depending on what was selected in the Type box) various rights.

- **View Existing Records:** Allows the user/group to open and review a previously entered item.
- **Edit Existing Records:** Allows the user/group to change information for a previously entered item.
- **Delete Existing Records:** Allows the user/group to delete a previously entered item, thus removing it from the database.
- **Add New Records:** Allows the user/group to enter new items.
- **Process Records:** Allows the user/group to perform a process, such as Close Fiscal Year.
- **Display Sensitive Data:** Allows the user/group to view fields that contain sensitive information, such as, bank account numbers and social security numbers, in the Maintain>Vendors and Maintain>Payroll>Employee Information forms, and related reports. Note that the associated module must be owned and added to your system, in order to grant these rights.
  - If the Display Sensitive Data check box is not selected, the sensitive data field will display the last one to three number of characters, preceded with asterisks. Unless the number of characters is eight or greater in length, then the last four digits display. For example an eight-digit bank account number will display as ********, a nine-digit social security number will display as ***-**-0000, and a 7-digit bank account number will display as ****099.

Important! Note that when adding user rights for the Maintain>Payroll>Employee Information menu, the *Display Sensitive Data* check box is automatically selected. If you clear the *Display Sensitive Data* check box, the system will automatically clear the **Add New Records** check box as well. So that the user or group will not be able to add New Records. You will need to select the **Add New Records** check box ***after*** selecting the **Display Sensitive Data** check box.

Description: The system displays a description of each menu selection, as it is highlighted.

Group Assignments: The system automatically displays any groups in which the selected user is a member (if appropriate).

- When you click on a menu selection within the outline, the Group Assignments box will display actual group rights (VEDAPS), if the menu selection is part of a group.
- If the menu selection is not assigned to a group, the system simply continues to display the groups in which the user is a member.

Tips:

- To print a list of users or groups and other data which entered on this form, use Reports>Lists>Security, User Information, and Group Information.
- Click Copy to make a copy of the group or user's organization security to be used for a different group or user.
- Assign system-specific security rights using Security>Set Up System Menus.
- To remove all rights for a user, select each menu selection and then clear all check boxes, or delete the user using Security>Maintain Users.
- Some rights depend on other rights; the system automatically selects or clear options. For example, if you select the Edit check box, the system selects the View check box too.
- Be sure to limit the right to set up security to appropriate users. Otherwise, a user can gain unauthorized access by simply changing his own security rights.
- You can assign rights to a main menu to give the user rights to all of those menus' selections. For example, if you select Reports and assign rights, those rights are applied to all available menu selections in the Reports menu.
- A user or group cannot be added using this form. Use Security>Maintain Users or Maintain Groups to add a new user or group.
- Keep in mind that menu selections for additional modules (such as, Accounts Payable and Bank Reconciliation) are integrated into the MIP Accounting menu selections.
- In order for security changes to take affect, close the active organization and then reopen it.

Copy Organization Security

Access this form with Administrative user rights using the Security>Set Up Organization Menus> Copy.

Use this form to copy the organization menu security for a user or group to a different user or group.

Fields

Copy From ID: Select an existing user or group ID that you want to copy.

Copy To ID: Select an existing user or group ID for the user or group that has the same menu security settings as the Copy From ID.

Comparing System and Organization Security Menus

The system has two types of security—System Security and Organization Security. The following sections help you determine in which database menu selections are stored.

System Security

System Security refers to security stored in the NPSSQLSYS database, which is distributed with the system. Therefore, you have one system database for all organizations you create. This also means that System Security changes, like setting up a user, only have to be done once, and then it is available in all organizations moved to the Selected Items box on the Security>Maintain Users form. System Security rights apply for all organizations in which the user is logged on.

Below are the Administration menu selections that are associated with System Security. You use the Security>Set Up System Menus form to grant security to these menu selections. Because these changes are stored in the NPSSQLSYS database, you need to do this once for every user that needs system level security:

- File>New Organization, New Consolidated Organization*, Backup, Restore, Compress, Create Client Consolidate File*, and Print Setup
- Reports>Lists>User Information
- Organization>Default Table Structure
- Security>Maintain Users, Set Up System Menus, and Manage Audit Trails>System Audit
- System>Manage Concurrent Users, Current Activity, and Activate License
- Options>System Preferences

*This menu selection displays if you have installed the appropriate module.

Organization Security

Organization Security refers to security stored in the organization database. This database is created when you create an organization (File>New Organization). Therefore, you have one organization database for each organization you create. This also means that Organization Security changes, like setting up a group or users' organization security, must be made in each organization.

Note: You must give the user access to the organization (Security>Maintain Users), so that the user is available in the organization.

Below are the Administration menu selections that are associated with Organization Security. Use the Security>Set Up System Menus form to grant security to these menu selections. You need to do this for each organization:

- Reports>Lists>Security, User Information, Group Information, Account Level Security, Advanced Organization Audit*, Requisition User Information*, User Defined Fields*, UDF Default Sources, and Currency
- Organization>Organization Information, Organization Preferences, Add a Module, Set Up Modules*, Data Integrity Checks, Consolidate Transaction History, Remove Payroll History, Set Up User Defined Fields, Set Up UDF Default Sources, Attachments, and Currency Setup
- Security>Maintain Groups, Set Up Organization Menus, Set Up Account Level Segments, Set Up Account Level Security, Manage Audit Trails>Summary Organization Audit, and Requisitions>Set Up Requisition Users* and Set Up Category Approvers*,

*This menu selection appears if you have installed the appropriate module and system.

Note: All Accounting, Payroll, and Requisitions menus are available for selection.

Audit Trails

Use these form to view and print a log of some administrative functions and completed activities for the organization. These logs provide detailed information regarding addition, modification, and deletion of user and group IDs and organization records.

System Audit

Access this form with Administrative user rights using Security>Manage Audit Trails>System Audit.

Use this form to view and print a log of some administrative functions performed in the system, such as the addition, modification, or deletion of user or group IDs.

Fields

Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria. Your choices for filtering items are: Date, User ID, Database Name, Message, and Message Type.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Available Items Table: Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading.

- **Records per Page:** Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The default setting for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.
- **Date:** This is the date and time the activity was logged.
- **User ID:** This is the user that performed the activity.
- **Database Name:** This is the organization in which the activity was performed. If you are logging on or off, this cell is blank.
- **Message:** This is the activity's description.
- **Message Type:** This is a code, indicating the type of message that is listed in the Message column.

Tips:

- When filtering data, select Operators to determine which data to display. Also, view a list of Filter Examples that are useful throughout the system and examples of How to Use Wildcards characters with Like and Not Like.
- In the Available Items table, you can sort the data based on any column. Simply double-click on a column heading to sort according to that column.
- The sorting functionality is only for table display and does not affect printing. Print uses the data from the database and is therefore not reflective of how the items were sorted.
- To view the history of an organization, use Security>Manage Audit Trails>Summary Organization Audit.
- When setting up security for users (Security>Set Up Organization Menus), we recommend you limit access to this form to include only system administrator-type users.
- For larger organizations with many records, you may want to clear the "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it eliminates the time it takes to load this form.
- To purge old history information that is no longer useful, highlight the row you want to delete, and then click Delete .

Summary Organization Audit

Access this form with Administrative user rights using Security>Manage Audit Trails>Summary Organization Audit.

Use this form to view and print a log of completed activities for the organization in which you are working. This log provides detailed information regarding addition, modification, and deletion of records, as well as, whether or not an employee's payroll calculation is edited with or without recalculating taxes on the Review/Modify Calculated Payroll form. Also, the log provides detailed information regarding what sessions have started posting, are posted, or if the posting session failed.

Fields

Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria. Your choices for filtering items are: Date, User ID, Message, and Message Type.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Available Items Table: Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading.

- **Records per Page:** Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The default setting for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.
- **Date:** This is the date and time the activity was logged.
- **User ID:** This is the user that performed the activity.
- **Message:** This is a description of the activity that was logged.
- **Message Type:** This is a code, indicating the type of message that is listed in the Message column.

Note: The grid will only display the latest 100,000 records. If a 'system out of memory' error message displays, use the date filter to narrow down your search results to less than 100,000 records.

Tips:

- When filtering data, select Operators to determine which data to display. Also, view a list of Filter Examples that are useful throughout the system and examples of How to Use Wildcards characters with Like and Not Like.
- In the Available Items table, you can sort the data based on any column. Simply double-click on a column heading to sort according to that column.
- The sorting functionality is only for table display and does not affect printing. Print uses the data from the database and is therefore not reflective of how the items were sorted.
- To view the history of the system, use Security>Manage Audit Trails>System Audit.
- You may find the information on this form useful if you are troubleshooting data problems, and your auditor may find this feature useful, since it provides a history of activity in the organization.
- When setting up security for users (Security>Set Up Organization Menus), we recommend you limit access to this form to include only system administrator-type users.
- For larger organizations with many records, you may want to clear the "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it eliminates the time it takes to load this form.

Manage Audit Trail Buttons

	Select All: Use this button to select all items in the table. This button is not available on the Organization Maintenance History form.
	Deselect All: Use this button to clear all items in the table. This button is not available on the Organization Maintenance History form.
	Delete: Use this button to delete the selected items from the data. This button is not available on the Organization Maintenance History form.
	Display/Hide Filter: Use this button to display or hide the Filters group box.
	Clear Filter: Use this button to clear all of the selected filter items. The filter is used for display purposes only; it limits what the system displays in the table. You cannot save the filter items.
	Display Records: Use this button to display only the records that match the currently selected filter items. If you are not using the filter (it is blank), the Display Records

	button displays all of the items you currently have.
	View First Page: Use this button to display the first page of data in the table.
	View Previous Page: Use this button to display the previous page of data in the table.
	View Next Page: Use this button to display the next page of data in the table.
	View Last Page: Use this button to display the last page of data in the table.
	Print Setup: Use this button to select a printer and set up default printer information for printing your list.
	Print to Screen: Use this button to view your list before it is formatted for printing. This makes your data easy to review, but does not provide an exact representation of how it looks when sent to the printer.
	Print Preview: Use this button to view your list as it actually prints.
	Print: Use this button to print the items in the list.
	Export: Use this button to export data to one of several popular file formats. This button is available only if the Data Import/Export module is installed.

Chapter 4: Advanced Security

This chapter contains information about setting up account level segments, account level security, and database encryption.

Set Up Account Level Segments

Access this form with Administrative user rights using Security>Set Up Account Level Segments. It is only available if the Advanced Security module is installed.

Use this form to activate account level security to specific segments for the active organization. Once you set up account level security, it is effective for applicable transactions and reports in which the user has been assigned rights (Security>Set Up Organization Menus).

Account level security is addressed by the system at three levels. To apply security at the:

- Organization Level - Select "Activate Account Level Security" on this form.
- Segment Level - Select segments on this form.
- User Level - Select "Enable Account Level Security" on the Security>Set Up Account Level Security form.

Therefore, even if "Activate Account Level Security" and at least one segment are selected on this form, account level security does not work unless "Enable Account Level Security" is selected on the Set Up Account Level Security form.

Fields

Activate Account Level Security: Select this check box to "turn on" account level security for the active organization. If you are using this feature and then decide to turn it off, the system may retain all security setup depending on how you respond to a system message.

If this check box is *not* selected, the account level security feature is inactive for the organization. Consequently, all users have access to all accounts.

Segments: The system displays all segments for the active organization. Once the Activate Account Level Security check box is selected, choose the segments that require account level security.

The segments selected on this form determine the accounts that display on the Security>Set Up Account Level Security form. In essence, all segments that are not selected here are filtered out of the Set Up Account Level Security form and all users will have access to these segments.

Options Allow Access, Deny Access: Select either of these options depending on if you want to grant or restrict access to accounts on the Set Up Account Level Security form.

- If the majority of users and groups will be granted access to accounts, select the Allow Access option.
- If the majority will be denied access to accounts, select the Deny Access option.

This reduces the number of accounts that need to be selected on the Set Up Account Level Security form. For example, if the active organization contains a segment named "Fund," and "Fund" and "Allow Access" are selected on this form, the Set Up Account Level Security form would only display accounts for the "Fund" segment and would be ready to grant access to the accounts. Alternatively, if "Deny Access" is selected, the form would still only display "Fund" accounts, but would be ready to deny access to the accounts.

Print Disclaimer on Report: Select this check box to print the disclaimer "This report may be affected by Account Level Security" in the header of every report that will have account level security applied to it. Also, an asterisk (*) prints after the report title.

Tips:

- To print the data entered on this form, use Reports>Lists>Account Level Security List.
- When you make changes on this form, you must close it to see the changes on any transaction entry forms or on the Security>Set Up Account Level Security form. However, changes are immediately available on any reports.
  If your System Administrator makes administrative-type changes (for example, to users or Chart of Accounts Codes), all users' Account Level Security is updated, regardless of whether or not the System Administrator's change directly affects them. Therefore, the users may experience slower performance and may need to close and reopen the form they are currently in.
- Segments were previously created using the File>New Organization wizard, and they display in the order they were created. However, the order can be changed using the Organization>Organization Information form.
- Users and groups were previously created using the Security>Maintain Users and Maintain Groups forms.

Set Up Account Level Security

Access this form with Administrative user rights using Security>Set Up Account Level Security. It is only available if the Advanced Security module is installed.

Use this form to grant or deny a user access to accounts. Once you set up Account Level Security, it is effective for applicable transactions and reports in which the user has been assigned rights (Security>Set Up Organization Menus).

Users (Security>Maintain Users or Set Up Organization Menus) must have been previously set up in order to use this form. And, this form is only available if "Activate Account Level Security" and at least one segment was selected using Security>Set Up Account Level Segments.

Account level security is addressed by the system at three levels. To apply security at the:

- Organization Level - Select "Activate Account Level Security" on the Security>Set Up Account Level Segments form.
- Segment Level - Select segments on the Security>Set Up Account Level Segments form.
- User Level - Select "Enable Account Level Security" on this form.

Therefore, even if the "Enable Account Level Security" check box is selected on this form, account level security does not work unless "Activate Account Level Security" and at least one segment is selected on the Security>Set Up Account Level Segments form.

Fields

Type: Select a type of User or Group.

ID: Select the user or group ID to which you want to assign account codes. This ID was assigned when the user or group was created (Security>Maintain Users or Maintain Groups).

Enable Account Level Security: Select this check box to activate account level security to accounts for the selected user. If you want to set up account level security, but do not want to apply it immediately, do not check this box. However, if a user does not have this selected, they have access to all accounts. (This check box is only available if User is selected in the Type box.)

Display All Accounts: Select this check box to view all account codes for the user and any groups in which they are a member. The group ID appears in the Groups column of the Selected Items box. (This check box is only available if User is selected in the Type box.)

Allow/Deny Access To Accounts: This title changes depending on what option was selected using the Security>Set Up Account Level Segments form—"Allow Access" or "Deny Access." Available account codes are being filtered according to the segments selected on that form. (This entire group box is disabled if the Display All Accounts check box is selected.)

- If the title is Allow Access to Accounts, the user or group is granted access to account codes moved to the Selected Items box.
- If the title is Deny Access to Accounts, the user or group is restricted from account codes in the Selected Items box.

This group box contains the account code <Blank>. The blank account code is provided for reporting purposes, when an organization has non-balancing and restriction segments. This allows the blank account codes to be assigned in account level security so that the user can print the blank account codes.

Tips:

- Even if Account Level Security is set up for a group and the user ID is assigned to that group, Account Level Security does not work for the user until the "Enable Account Level Security" check box is selected, with or without codes selected, as part of their setup on the Set Up Account Level Security form.
- When you make changes on this form, you must close it to see the changes on any transaction entry forms. However, changes are immediately available on any reports.
  If your System Administrator makes administrative-type changes (for example, to users or Chart of Account Codes), all users' Account Level Security is updated, regardless of whether or not the System Administrator's change directly affects them. Therefore, users may experience slower performance and may need to close and reopen the form they are currently in.
- To print the data entered on this form, use Reports>Lists>Account Level Security.
- Copy is used to copy account level security from one user or group to another.
- Segments are listed in the order they were created using the File>Open Organization wizard; however, the order can be changed using Organization>Organization Information.

Copy Account Level Security

Access this form with Administrative user rights using Security>Set Up Account Level Security> Copy.

Use this form to create an exact copy of a user or group's account level security (the accounts they have allow or deny rights to). Select an existing user or group ID to copy, and then select the name of the new user or group ID. For more information, see "Set Up Account Level Security" (page 66).

The system allows you to copy between a User ID and a Group ID and visa versa. However, even if the "Enable Account Level Security" check box is selected for the user or group ID you are copying from, it will not be copied to the new ID.

Fields

Copy FromID: Select an existing user or group ID that you want to copy.

Copy To ID: Select an existing user or group ID that you want to copy to.

Account Level Security on Transactions

Account Level Security can be applied to the transaction forms and buttons listed below. In order to activate this security, see How Do I Set Up Account Level Security?in the online help.

Module	Menu Selection
Accounts Payable	**Transactions>Accounts Payable>** Enter A/P Invoices Enter A/P Credits Enter Manual A/P Checks Edit Pay Selected A/P Invoices **Activities>Accounts Payable>** Display Vendor Balances
Accounts Receivable	**Transactions>Accounts Receivable>**

Module	Menu Selection
	Enter A/R Invoices
	Enter A/R Credits
	Enter A/R Receipts
	Edit A/R Invoices
	Activities>Accounts Receivable>
	Display Customer Balances
Allocations Management	Transactions>Edit Process Allocations
Encumbrances	**Transactions> Encumbrances>**
	Enter Encumbrances
	Enter Encumbrance Liquidations
	Activities>
	Display Encumbrance Balances
General Ledger	**Transactions>**
	Enter Cash Receipts
	Enter Cash Disbursements
	Enter Journal Vouchers
	Enter Budget
	Edit Write Checks
	Edit Receipt Writing
	Transactions>Payroll>
	Edit Payroll System Checks
	Edit Payroll Manual Checks
	Edit Payroll Void Checks

Module	Menu Selection
	Activities>
	Check Writing>Write Checks
	Receipt Writing
	Manage Recurring Entries
	Activities>Display Balances>
	Account Balances
	Available Budget Balances
G/L, A/P, A/R, A/M, Enc, and PO	**Transaction Entry buttons:**
	Copy Posted Document
	Reverse Posted Document
	Use Distribution Codes
	Use Offsets
	Memorize Document
	Memorize/Recurring Document
	Recall Memorized Document
	Choose A/P Invoices
	Choose A/R Encumbrances

Account Level Security on Reports

Account Level Security can be applied to the reports listed below. In order to activate this security, see How Do I Set Up Account Level Security? in the online help.

Reports Menu	Report Names
Reports>Lists>	Account Level Security
	Advanced Organization Audit

Reports Menu	Report Names
Reports>	Check/Voucher Register
	Journals (All Reports)
	Transactions (All Reports)
	General Ledger Analysis (All Reports)
	Quick Financial Statements (All Reports)
	Financial Statements (All Reports)
	990 Worksheets (All Reports)
Reports>Accounts Payable>	Summary A/P Ledger Detail A/P Ledger Aged Payables Invoices Selected for Payments Vendor Activity
Reports>Accounts Receivable>	Calculated Invoices/Finance Charges Summary A/R Ledger Detail A/R Ledger Aged Receivables Customer Activity
Reports>Allocation Management>	Pre-Allocation Standard General Ledger Pre-Allocation Expanded General Ledger Pre Allocation Normal Trial Balance Pre-Allocation Comparative Trail Balance Pre-Allocation Working Trial Balance Pre-Allocation Statement of Revenues and Expenditures

Reports Menu	Report Names
	Pre-Allocation Statement of Cash Flows
Reports>Bank Reconciliation>	(All Reports)
Reports>Budget>	(All Reports)
Reports>Encumbrances>	(All Reports)
Reports>Fixed Assets>	Asset Transfer Report Depreciation Calculation Asset Disposals Pre-Transfer Depreciation/Disposal Register Summary Asset Ledger
Reports>Payroll>History>	Labor Distribution
Reports>Purchase Orders>	Purchase Order Register
Reports>Requisitions>	Requisition Register Requisition History Budget and Encumbrance Balance Analysis Purchase Order Vouchers

Note: Form level security can be activated for each individual report using the Security tab.

When Security Changes Take Affect

When you make changes to Account Level Security, the changes do not always take affect immediately. Sometimes, the form must be closed and reopened.

Account Level Segments

If changes are made by the Administrator on the Security>Set Up Account Level Segments form, the changes are available immediately on reports, but not necessarily for transaction entry forms or the Security>Set Up Account Level Segments form.

The following table explains what must be done in order for the changes to take affect:

Action	TE	Set Up Account Level Security
Change Activate Account Level Security (On/Off)	Form must be closed and reopened	N/A
Change Segment Name (On/Off)	Form must be closed and reopened	Change the User/Group or close and reopen the form
Change Allow to Deny or Deny to Allow (On/Off)	Form must be closed and reopened	Immediately
Change Print Disclaimer on Report (On/Off)	N/A	N/A

Account Level Security

If changes are made by the Administrator on the Security>Set Up Account Level Security form, the changes are available immediately on reports, but not necessarily for transaction entry forms.

The following table explains what must be done in order for the changes to take affect:

Action	TE
Move Accounts from Selected to Available or Available to Selected	Form must be closed and reopened
Change Enable Account Level Security (On/Off)	Form must be closed and reopened

The system updates Account Level Security when an existing document is selected on the Transaction Entry form. It updates again, when a new or existing document is Saved or Posted.

Updating Account Level Security

Note: Account Level Security is only available if the Advanced Security module is installed.

If the System Administrator makes any of the following administrative changes, all users' Account Level Security is updated, regardless of whether or not the System Administrator's change directly affects them. Therefore, online users might need to close and reopen the form they are currently in. Users cannot be deleted if they are logged on the system. In general, we suggest that changes be

made when most users are logged off the system, if possible. For more information, see the ""When Security Changes Take Affect" (page 72)" topic.

Action	Associated Form
Modify, add, or delete user information	Security>Maintain Users
Modify, add, or delete group(s) or group information	Security>Maintain Groups
Modify, add, or delete a chart of accounts code	Maintain>Chart of Accounts Codes
Modify any segment information	Organization> - Organization Information - Organization Preferences (Account Code Combinations setup for segments) - Set Up Modules>All Modules
Modify Account Level Security setup	Security>Set Up Account Level Segments
Modify Account Level Security for users/groups	Security>Set Up Account Level Security

Note: These updates are effective in the current organization only.

Set Up Database Encryption

Access this form with Administrative user rights using Security>Set Up Database Encryption. It is only available if the Advanced Security module is installed and if your data is stored on SQL 2008 R2 or higher.

Use this form to encrypt sensitive information stored in your database, such as Social Security Numbers, Tax Identification Numbers, Driver's License Numbers, State-Issued Identification Card Numbers, and Financial Account Information. The purpose of this feature is to keep personal and financial information safe by removing it if the system database is compromised. In the event of disaster recovery, you will need the Enable and Backup Passwords to recreate the server

environment, along with the MIPServiceMasterKey.BAK file and the most up-to-date backup of the organization's system database. Without these, the encrypted data is lost and there is nothing that MIP can do to remedy the situation. It is essential to store the MIPServiceMasterKey.BAK file and passwords someplace safe as well as keep regular backups of the organization's system database.

To Access the Set Up Database Encryption form

1. Open the Set Up Organization Menus form, with Administrative user rights using Security>Set Up Organization Menus, to set up security rights for a user or group in the active organization and assign the rights to the Set Up Database Encryption form.
    a. Highlight the Set Up Database Encryption menu selection in the Set Up Menus box (located by expanding Accounting and Security), then select the Process Records check box to grant the user or group (depending on what was selected in the Type box) to perform processing rights.
    b. Click the Save button and close this form.
2. Close the active organization.
3. Open the organization and log on as the user that was given processing rights in the first step.
4. Open the Set Up Database Encryption form using Security>Set Up Database Encryption. This form is not available when the default User *Admin* is logged on to the organization's MIP Accounting system.

To Set Up Database Encryption

1. Open the organization and log on as a user with processing rights. The Set Up Database Encryption form is not available when the default User *Admin* is logged on to the organization's MIP Accounting system.
2. Open the Set Up Database Encryption form using Security>Set Up Database Encryption.
3. Verify that the top of the form displays: Database encryption is disabled.
4. Click the Enable button to encrypt sensitive information in the organization's system database using a symmetric key.
    a. Enter a strong Password.
    b. Enter the strong Password again in the Confirm Password field.

c. The Enable Encryption process form displays.

d. Click the Finish button when the Enable Encryption process has completed successfully.

5. Click the Backup button to manage the Service Master Key by creating a backup.

   a. Enter another strong.

   b. Enter the strong password again in the Confirm Password field.

   c. Locate and copy the MIPServiceMasterKey.BAK file to removable media and store it in a secure off-site location.

6. Once you have enabled encryption, you will be responsible for keeping the passwords and MIPServiceMasterKey.BAK file safe and the organization's system database regularly backed up. If the encrypted data is lost, there is nothing that MIP can do to remedy the situation.

To Regain Access to Encrypted Sensitive Information

If you migrate or move the organization's system database from the server installation to another computer, you can restore the Service Master Key to regain access to encrypted sensitive information.

1. Install the MIP Accounting software on the server.
2. Restore the latest organization system database to the new computer.
3. Be sure that the MIPServiceMasterKey.BAK is installed on the new computer.
4. Open the organization and log on as a user with processing rights. The Set Up Database Encryption form is not available when the default User *Admin* is logged on to the organization's MIP Accounting system.
5. Open the Set Up Database Encryption form using Security>Set Up Database Encryption.
6. Click the Restore button to regain access to encrypted sensitive information.

   a. Enter the Enable Password

   b. Enter the Backup Password

7. Return to work as normal.

Accounts Payable Users

If your organization's system database is compromised and you do not have pre-printed checks*, you will not be able to process checks until all of the *sensitive information* is manually re-entered.
* You should be able to print your Accounts Payable and Payroll checks if you have pre-printed check stock that contains your bank account numbers and routing numbers.

Accounts Receivable Users

If your organization's system database is compromised, you will not be able to process invoices until all of the *sensitive information* is manually re-entered.

Direct Deposit Users

If your organization's system database is compromised, you will not be able to create a direct deposit banking file when processing payroll until all of the *sensitive information* is manually re-entered.

Electronic Funds Transfer for A/P Users

If your organization's system database is compromised, you will not be able to send electronic payment information (NACHA formatted file) to the bank when processing Accounts Payable invoices until all of the *sensitive information* is manually re-entered.

Forms Designer Users

If your organization's system database is compromised, you will not be able to print forms that contains any of the *sensitive information*.

Payroll Users

If your organization's system database is compromised and you do not have pre-printed checks*, you will not be able to process payroll checks until all of the *sensitive information* is manually re-entered.
* You should be able to print your Accounts Payable and Payroll checks if you have pre-printed check stock that contains your bank account numbers and routing numbers.

Sensitive information is defined as magnetic stripe data, validation codes/values and PIN data.

Protected/Personal data is defined as first name and last name, or first initial and last name in combination with any one or more of the following:

- Social Security Number
- Tax Identification Number

- Driver's License Number
- State-issued Identification Card Number
- Financial Account Information with or without any required codes that would permit access to financial information includes;
  - Credit Card Number, PAN (primary account number), and Expiration Date
  - Debit Card Number, PAN (primary account number), and Expiration Date
  - Bank Account Numbers
  - etc.

Fields

Enable: Select this button to encrypt sensitive information stored in your database. *Sensitive information* includes Social Security Number, Tax Identification Number, Driver's License Number, State-issued Identification Card Number, Bank Account Numbers, Credit Card Number, Credit Card PAN (primary account number), and Credit Card Expiration Date, and Debit Card Number, Debit Card PAN, and Debit Card Expiration Date. In the event your database is compromised, the sensitive data in the tables will be unreadable. See above for more information about Sensitive information.

Password requirements:

- Include at least one uppercase and one lowercase letter
- Include at least one number
- Cannot contain spaces at the beginning or end
- Cannot be one of the last 6 passwords used

The system will encrypt all the modules that contain sensitive information. Click Finish to complete the Enable process. The message at the top of the form displays: Database encryption is enabled.

Important! Be sure to record this password and store it in a safe off-site location. This password will be required if you ever need to restore your data to a new instance of SQL Server.

Disable: Select this button to reverse the encryption process. Sensitive information will again be easily readable in your database tables. The message at the top of the form displays: Database encryption is disabled.

Backup: Select this button to create an encrypted copy of your Service Master Key. The Service Master Key is the root of the SQL Server encryption hierarchy. It is important to locate the MIPServiceMasterKey.BAK file, copy it to removable media, and store it in a secure off-site location, such as a safe deposit box. This information is required to restore full functionality to your encrypted database in the event of a major system change. Without it, your sensitive encrypted information will be lost. If lost, you will have to manually re-enter all of your *sensitive information* again. See above for more information about Sensitive information.

Password requirements:

- Include at least one uppercase and one lowercase letter
- Include at least one number
- Cannot contain spaces at the beginning or end
- Cannot be one of the last 6 passwords used

Important! This password will be required if you ever need to restore your data to a new instance of SQL Server.

Restore: In the event of a major system change to your database server, select this button to re-establish the keys used to encrypt your sensitive information. The Enable and Backup Passwords are necessary to restore your data to a new instance of SQL Server. You will also need the most up-to-date backup of your existing organization and system databases.

Tips:

- Modules that are affected by Encryption: General Ledger, Accounts Payable, Electronic Funds Transfer for Accounts Payable, Payroll, Direct Deposit, and Accounts Receivable.
- Passwords can be copied and pasted using Ctrl+C and Ctrl+V or by right-clicking the highlighted password and selecting Copy or Paste.
- If you find Encryption enabled but not working properly, click Restore. Enter your Enable and Backup Passwords. Your database will be returned to it's safe encrypted state and all sensitive information will remain safe in the database. However, if the Enable and Backup Passwords are lost or the MIPServiceMasterKey.BAK file cannot be restored, all of your organization's system database sensitive information will be lost and cannot be restored. The only way to restore this information is to manually re-enter it into the organization's system database. Until the information is entered, you will not be able to process A/P checks, A/R invoices, or Payroll checks, including EFT for A/P and Direct Deposits.

Advanced Audit Trails

With the Advanced Security module, advanced auditing capabilities are available. Use the Set Up Advanced Organization Audit form to select the Accounting and Payroll module Maintain menu forms. When enabled, the system records detailed information regarding new, changed, or deleted entries for these types of records. Then use the Advanced Organization Audit form to view the detailed information the system collected. This module is especially useful to find out what went wrong and who did it.

To begin Advanced Organization Auditing, you will need to set up the following:

1. Add Group and User security in order to access these forms. (As the Administrator, Security>Set Up Organization Menus)
2. Select the menus for which you want to being collecting information. (Security>Manage Audit Trails>Set Up Advanced Organization Audit)

   Note: We recommended that you clear the Enable Audit check box next to the Record Type during the initial system setup and when Importing new records. When you are auditing, every field change made or imported for these record types get recorded; taking up a lot of space on your database server that will be needed when processing transactions, checks, or any other activity.
3. Review the collected information. (Security>Manage Audit Trails>Advanced Organization Audit)
4. If applicable, print the collected information. (As the Administrator, Reports>Lists>Advanced Organization Audit)

Important! We recommend using the Advanced Organization Audit with the Full Version of Microsoft SQL Server installed on your Server machine. Otherwise, slow performance issues can occur when Microsoft SQL Server Express is installed on your Server machine.

Advanced Organization Audit

Access this form with Administrative user rights using Security>Manage Audit Trails>Advanced Organization Audit. It is only available if the Advanced Security module is installed.

Use this form to view changes that were made by the Administrator to the organization's Maintain, Organization, and Security menu forms. This form provides detailed information showing what

information was added, what was changed (displaying both before and after), who made the change, when the change was made, and so forth for each of the record types selected.

Payroll Users

The Advanced Organization Audit displays several items differently than what was originally entered, such as, the value is rounded for the Maintain>Payroll - Employee Equivalent Hourly Rate for calculations; Hourly Rate and Equivalent Hourly Rate are the same.

Direct Deposit Users

The Advanced Organization Audit displays several items differently than what was originally entered, such as, the Percent column, 100% displays as 1, and 50% displays as .5.

All Users

The Advanced Organization Audit displays several items differently than what was originally entered, such as, if a date was not entered in a field, the system displays the word *Null*.

Important! We recommend using the Advanced Organization Audit with the Full Version of Microsoft SQL Server installed on your Server machine. Otherwise, slow performance issues can occur when Microsoft SQL Server Express is installed on your Server machine.

Fields

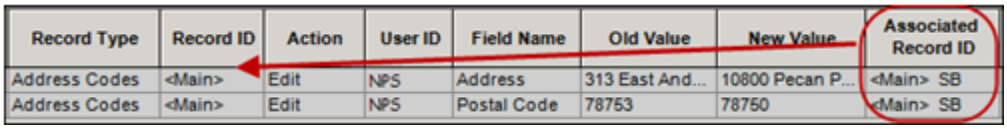
Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria. Your choices for filtering items are: Date, User ID, Message, and Message Type.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Available Items Table: Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading. To

- **Records per Page:** Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The default setting for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.
- **Date:** The system displays the date and time the activity was logged. The date is formatted as M/D/YYYY and the time is formatted as HH:MM:SS uppercase AM or PM.
- **Record Type:** The system displays the name of the form where the change occurred, (if hyphenated, the name of the Tab displays), such as Set up Advanced Organization Audit or Customer - Shipping Address.
- **Record ID:** The system displays the identity of the record that was changed, such as, Customer, ABC or AAA.
- **Action:** The system displays a code, indicating the type of action that occurred. There are three message types: ***Add*** (a new entry), ***Edit*** (change made to an existing record), and ***Delete*** (removal of an existing entry).
- **User ID:** The system displays the user who performed the activity, such as, NPSUser. Note that User ID *MIP Administrator* (on premise) or *{database}_{tenant}_Admin* (MIP Cloud), identifies when there are system processes that occurred using the system authentication. Also, on rare occasions, these identifiers will appear after performing an activity with your permission using the system authentication, such as database updates and data work.
- **Field Name:** The system displays the name of the field where the change occurred, such as, Enable Audit or Shipping Phone.
- **Old Value:** The system displays the data that was in the field before it was added or changed, such as, Disabled or (817) 555-2222 Ext. Note that a blank field displays when a new entry is added or when an existing data field was intentionally left blank.
- **New Value:** The system displays the data that was in the field after it was added or changed, such as, Enabled or (254) 555-2222. Note that a blank field displays when an existing entry is deleted or when a new data entry field was intentionally left blank.
- **Associated Record ID:** The system displays the secondary column associated to the Record ID that was changed, such as, <Billing> AAA (Shipping Address Code and Customer ID) or

- <PostOffice> S (Address Code and Address Code Type). Note that a blank field displays when there is no association for the Record ID.
  For example, if you have selected Address Codes to be audited and later your organization moves. When the NPS User updates your organization address information (Organization>Organization Information - Address Tab), the Advanced Organization Audit will display the following:



Record Type	Record ID	Action	User ID	Field Name	Old Value	New Value	Associated Record ID
Address Codes	<Main>	Edit	NPS	Address	313 East And...	10800 Pecan P...	<Main> SB
Address Codes	<Main>	Edit	NPS	Postal Code	78753	78750	<Main> SB

  The **Associated Record ID** column displays *<Main> SB* and references the *<Main>* **Record ID** column, since the changes were made to the organization's main address on the Address Tab.

- **Source:** The system displays where the activity was performed. For example,
  - If a user logged into any module in the MIP system, one of the following displays: *Administration*, *Accounting*, or *Payroll*.
  - If information was imported into the MIP system, *Import* displays.
  - If a user connected directly to the database on the SQL Server, *Other* displays.
- **Workstation:** The system displays the name of the workstation used to perform the activity, such as, NPSSERVR.

Tips:

- This form is designed to give you the most complete auditing details. To print the data entered on this form but in an organized way to fit your needs, use Reports>Lists>Advanced Organization Audit.
- When filtering data, select Operators to determine which data to display. Also, view a list of Filter Examples that are useful throughout the system and examples of How to Use Wildcards characters with Like and Not Like.
- In the Available Items table, you can sort the data based on any column. Simply double-click on a column heading to sort according to that column.
- The sorting functionality is only for table display and does not affect printing. Print uses the data from the database and is therefore not reflective of how the items were sorted.
- To save your form settings—the size and/or position of a form or the width or order of columns, select Save Form Layout using Options>Customize Workstation Settings. Then the next time you open the form, it is the same size and position when you last opened it.
- You may find the information on this form useful if you are troubleshooting data problems, and your auditor may find this feature useful, since it provides a history of activity in the organization.
- When setting up security for users (Security>Set Up Organization Menus), we recommend you limit access to this form to include only system administrator-type users.
- For larger organizations with many records, you may want to clear the "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it eliminates the time it takes to load this form.

Advanced Audit Trail Buttons

	Display/Hide Filter: Use this button to display or hide the Filters group box.
	Clear Filter: Use this button to clear all of the selected filter items. The filter is used for display purposes only; it limits what the system displays in the table. You cannot save the filter items.
	Display Records: Use this button to display only the records that match the currently selected filter items. If you are not using the filter (it is blank), the Display Records button displays all of the items you currently have.

	View First Page: Use this button to display the first page of data in the table.
	View Previous Page: Use this button to display the previous page of data in the table.
	View Next Page: Use this button to display the next page of data in the table.
	View Last Page: Use this button to display the last page of data in the table.
	Print Setup: Use this button to select a printer and set up default printer information for printing your list.
	Print to Screen: Use this button to view your list before it is formatted for printing. This makes your data easy to review, but does not provide an exact representation of how it looks when sent to the printer.
	Print Preview: Use this button to view your list as it actually prints.
	Print: Use this button to print the items in the list.
	Export: Use this button to export data to one of several popular file formats. This button is available only if the Data Import/Export module is installed.

Set Up Advanced Organization Audit

Access this form with Administrative user rights using Security>Manage Audit Trails>Set Up Advanced Organization Audit. It is only available if the Advanced Security module is installed.

Important! We recommend using the Advanced Organization Audit with the Full Version of Microsoft SQL Server installed on your Server machine. Otherwise, slow performance issues can occur when Microsoft SQL Server Express is installed on your Server machine.

Use this form to select the record types you want the system to audit. By selecting the Enable Audit check box next to the Record Type and saving the form; the system begins collecting detailed information showing what information was added, what was changed (displaying both before and after), who made the change, when the change was made, and displays this information on the Security>Manage Audit Trails>Advanced Organization Audit form.

By clearing the Enable Audit check box next to the Record Type, the system stops collecting this information.

Important! We recommended that you clear the Enable Audit check box next to the Record Type during the initial system setup and when Importing new records. Every field change associated to these record types are recorded and can take up a lot of database space.

Fields

Set Up Advanced Organization Audit

- **Enable Audit, Record Type:** Select the Enable Audit check box to begin collecting that Record Type's detailed information, such as, addition, modification, and deletion of those records. The Record Type displays the Maintain menu record type that is available for auditing.

Note: The Record Type - *Address Codes* records modifications in the Security>Manage Audit Trails>Advanced Organization Audit form, for the following forms: Organization>Organization Information>Address Tab and Maintain>Purchase Orders>Address Codes>Address Codes Tab.

Record Type	Description of what is being tracked:
Set Up Advanced Organization Audit	When any Record Type is selected and the form is saved, the system begins collecting the record types being enabled and disabled by the Administrator on the Security>Manage Audit Trails>Set Up Advanced Organization Audit form.
Address Codes	When selected, the system collects all of the active organization's <Main> address information which is added, modified, or deleted by the Administrator on the Organization>Organization Information>Address Tab, except for the following: - Voice - Fax - Email - Website
Address Codes	When selected, the system collects all of the address information which is added, modified, or deleted on the

Record Type	Description of what is being tracked:
	Maintain>Purchase Orders>Address Codes form, except for the following: - Notes tab
Benefit Codes	When selected, the system collects all of the benefit code information which is added, modified, or deleted from the Maintain>Payroll>Benefit Codes form.
Chart of Accounts {Segment Name}	The system displays a record type for each chart of account segment name entered in your system. When selected, the system collects all of the chart of account segment information which is added, modified, or deleted on the Maintain>Chart of Accounts form.
Customer	When selected, the system collects all of the customer information which is added, modified, or deleted from the Maintain>Accounts Receivable>Customers form, except for the following: - Notes tab - User Defined Fields
Deduction Codes	When selected, the system collects all of the deduction code information which is added, modified, or deleted from the Maintain>Payroll>Deduction Codes form.
Earning Codes	When selected, the system collects all of the earning codes information which is added, modified, or deleted from the Maintain>Payroll>Earning Codes form.
Employee	When selected, the system collects all of the employee information which is added, modified, or deleted from the Maintain>Payroll>Employee Information form, except for the following: - Spouse SSN on State Tax tab - Notes tab

Record Type	Description of what is being tracked:
	- User Defined Fields tab
Employee	When selected, the system collects whether an employee's payroll calculation is edited with or without recalculating taxes on the Review/Modify Calculated Payroll form.
Leave Codes	When selected, the system collects all of the leave code information which is added, modified, or deleted from the Maintain>Payroll>Leave Codes form.
User Organization Security	When selected, the system collects all of the user rights information which is added, modified, or deleted from the active organization by the Administrator using the Security>Set Up Organization Menus form.
Vendor	When selected, the system collects all of the vendor information which is added, modified, or deleted from the Maintain>Accounts Payable>Vendors form, except for the following: - Notes tab - User Defined Fields
Workers' Compensation Codes	When selected, the system collects all of the workers compensation code information which is added, modified, or deleted from the Maintain>Payroll>Workers' Compensation Codes form.

Tip: For larger organizations with many records, you may want to clear the "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it eliminates the time it takes to load this form.

Set Up Advanced Organization Audit Buttons

	Select All: Use this button to select all items in the table. This button is not available on the Organization Maintenance History form.
	Deselect All: Use this button to clear all items in the table. This button is not available

	on the Organization Maintenance History form.
	View First Page: Use this button to display the first page of data in the table.
	View Previous Page: Use this button to display the previous page of data in the table.
	View Next Page: Use this button to display the next page of data in the table.
	View Last Page: Use this button to display the last page of data in the table.
	Print Setup: Use this button to select a printer and set up default printer information for printing your list.
	Print to Screen: Use this button to view your list before it is formatted for printing. This makes your data easy to review, but does not provide an exact representation of how it looks when sent to the printer.
	Print Preview: Use this button to view your list as it actually prints.
	Print: Use this button to print the items in the list.
	Export: Use this button to export data to one of several popular file formats. This button is available only if the Data Import/Export module is installed.

Chapter 5: Adding New Modules

Activate License - Owned Tab

Access this tab with Administrative user rights using System>Activate License.

Use this form to activate an owned or evaluation system.

Use this tab to enter an Activation Code which activates or expands your system license. You can also verify the following information:

- the Concurrent Users (or Licensed Seats) you purchased;
- the Additional Requisition Users you purchased (Electronic Requisitions module only);
- the Total Requisition Users (Electronic Requisitions module only);
- the Total Executive View Users (Executive View module only);
- the system's Serial Number;
- the name of the organization that the system is Licensed To;
- Total Databases;
- New Databases Available; and
- the Owned Modules

Fields

Activation Code: Enter an activation code, and then click OK. The first dash of the activation code is required. The activation code is case sensitive, so it must be entered exactly as it appears on the notification included with the system.

Product Information

- **Concurrent Users:** This is the maximum number of users that can be logged on the system at one time.
- **Additional Requisition Users:** This is the additional requisition users that were purchased.

- **Total Requisition Users:** This is the maximum number of requisition users that can be logged on the Electronic Requisitions module at one time. It is the total of your concurrent users and your additional requisition users. For example, if you have 10 concurrent users and 10 additional requisition users, the total number of requisitions users would be 20.
- **Total Executive View Users:** This is the maximum number of Executive View users that can be logged on the system at one time.
- **Serial Number:** This is the unique number assigned to your system for identification purposes. If you need to refer to this serial number later, you can view it using Help>About.
- **Licensed To:** This is the company name that was entered when the system was installed.
- **Total Databases:** This is the total number of databases that you purchased with your system.
- **New Databases Available:** This is the number of databases that are available for use.

Owned Modules: These are the modules you purchased for your system.

Tips:

- Initially when installing the product, you entered your activation code and the system automatically copied it to this form. Therefore, you do not need to change anything on this form unless your Activation Code changes.
  Later, if you decide to add a module or increase your seats or databases, you will need to enter a new activation code. Use Organization>Add a Module to add a module to existing databases.
- Be sure to keep your activation code in a safe place for future reference.
- When setting up security for users (Security>Set Up Organization Menus), we recommend you limit access to this form to include only system administrator-type users.

Activate License - Evaluation Tab

Access this tab with Administrative user rights using System>Activate License.

Use this tab to enter an Activation Code to activate or expand your evaluation system license. You can also use this tab to verify the following information:

- the Concurrent Users (or Licensed Seats) that are available with your evaluation system;
- the Additional Requisition Users available with your evaluation system (Electronic Requisitions module only);

- the Total Requisition Users (Electronic Requisitions module only);
- the Total Executive View Users (Executive View module only);
- the system's Serial Number;
- the expiration date for your system; and
- the Evaluation Modules

Note: When your evaluation activation code expires, your data will not be lost. If you purchase the product, you can continue working with the data you used during evaluation.

Fields

Activation Code: Enter an activation code, and then click OK. The first dash of the activation code is required. The activation code is case sensitive, so it must be entered exactly as it appears on the activation card included with the system.

Product Information

- **Concurrent Users:** This is the maximum number of users that can be logged on the system at one time.
- **Additional Requisition Users:** This is the additional requisition users that are available with your evaluation system.
- **Total Requisition Users:** This is the maximum number of requisition users that can be logged on the Electronic Requisitions module at one time. It is the total of your concurrent users and your additional requisition users. For example, if you have 10 concurrent users and 10 additional requisition users, the total number of requisitions users would be 20.
- **Total Executive View Users:** This is the maximum number of Executive View users that can be logged on the system at one time.
- **Serial Number:** This is the unique number assigned to your system for identification purposes. If you need to refer to this serial number later, you can view it using Help>About.
- **Code Expires On:** This is the date that your license expires. You have access to the full functionality of the system until this date. After the expiration date, you can no longer log on to the system. At that time, you must either acquire a new evaluation system activation code, or purchase the product and enter a valid system activation code on the Owned tab.

Evaluation Modules: These are the modules included in your evaluation copy of the product.

Tips:

- Initially when installing your evaluation system, you entered your activation code and the system automatically copied that code to this form. Therefore, you do not need to change anything on this form unless your Activation Code changes. Your code will change if you purchase the product or get an extension on your evaluation system.
- Be sure to keep your activation code in a safe place for future reference.
- When setting up security for users (Security>Set Up Organization Menus), we recommend you limit access to this form to include only system administrator-type users.

Add a Module

Access this wizard with Administrative user rights using Organization>Add a Module.

Use the Add a Module wizard to add a module to an existing organization.

Add a Module Wizard - Module Panel

Access this panel with Administrative user rights using Organization>Add a Module.

Use this panel to select the module you want to add to the active organization. The Available to Add box contains the modules that are installed, but not yet a part of the active organization. In the Currently Installed box, the system lists the modules that have already been added to this organization.

If you are adding one of the following modules to your organization, be sure to set it up after you complete this wizard using Organization>Set Up Modules>:

- Accounts Payable
- Accounts Receivable (Sales Order Entry)
- Budget
- Electronic Funds Transfer (Direct Deposit and EFT for A/P)
- Requisitions
- Fixed Assets
- Grant Administration

- Multicurrency
- Payroll
- Purchase Orders

To set up options for General Ledger use Organization>Organization Preferences.

Fields

Which licensed modules do you want to add to this organization?: Select at least one module to add to the active organization. The system only displays licensed, installed modules on the right side of the screen.

Tips:

- If you have already added all licensed modules for the active organization, you cannot access this menu selection.
- General Ledger is not available for selection, since it is required and is already installed.
- Remember, a new user does not have any security rights. Therefore, you need to set up its security in each organization using Security>Set Up System Menus and Set Up Organization Menus, respectively. Use the Set Up System Menus form to assign rights to Backup, Restore, and so on. Use the Security>Set Up Organization Menus form to assign access to the MIP Fund Accounting menu selections in which you want new users to have access.

Add a Module Wizard - Field Lengths Panel

Access this panel with Administrative user rights using Organization>Add a Module.

Use this panel to view and/or alter the default field lengths for the modules you are adding. The lengths entered here indicate the maximum number of characters allowed for various elements within your organization. Once you have completed this wizard, field lengths for these modules cannot be changed.

Fields

Module: The system displays the modules already added to this organization, as well as those you selected on the previous panel.

Category: The system displays the category the field name belongs to, such as Code/ID and Title/Description.

Field Name: The system displays the name of the field, as it appears in the system.

Field Length: Either change the length, or accept the default for each of the fields listed in the table. Field lengths for previously added modules cannot be changed.

Tips:

- We recommend that you evaluate your needs, and shorten and lengthen fields as appropriate.
- The list displays all customizable field lengths for this organization. Fields not listed are not customizable.

Add a Module Wizard - Security Panel

Access this panel with Administrative user rights using Organization>Add a Module.

Use this panel to confirm that all security rights have been granted to the current user for the active organization. The current user is the user name you entered when logging on to the system.

Tip: Before other users can access these modules, you (the current user) need to grant them rights (Security>Set Up Organization Menus).

Add a Module Wizard - Finish Panel

Access this panel with Administrative user rights using Organization>Add a Module.

Use this final panel to review all selections you made while adding modules to the active organization. When you click the Finish button, the system adds the designated modules to the active organization.

Tips:

- When you have completed this wizard, you need to set up module preferences using the Organization>Set Up Modules forms. To set up General Ledger, use Organization>Organization Preferences.
- If you need to make changes before you click Finish, use the Back button to move back to the appropriate panel and make the necessary changes before you click the Finish button.

Chapter 6: Attachments

Set Up Locations

Access this form with Administrative user rights using Organization>Attachments>Set Up Locations.

Use this form to activate the Attachments feature and set up the location in which encrypted documents are stored for the current database. Encrypted documents are scrambled by the system to prevent unauthorized access, and copied to a default or user defined attachment location for later retrieval and viewing.

Note: TO SYSTEM ADMINISTRATORS The system uses Universal Naming Convention (UNC) to store the path to the attachments. The encrypted attachment is written to the location that is specified on this form. To ensure that the encrypted file can be written to the selected location, verify that all users have proper share rights to that location. Also, ensure that the MIP Share Directory is not read-only.

Fields

Enable Attachments: Select this check box to enable the Attachments feature.

Module: The system displays all available modules that support attachments.

Path: The system displays the module's default path for storing attachments. To change a path, select a module and click on the default path. Click Browse to select the attachments new location. Be sure you have created the appropriate attachment folders before changing the location path.

Tips:

- All available modules appear on this form, regardless if the module is installed or owned.
- When installing a new module, if "Enable Attachments" is selected, the new module becomes available, and you can change the default path, if needed.
- Select "Documents Attached" in the Available column for any Posted/Unposted Transaction report to display the number of attachments associated with the accounting entries.
- Remember to periodically back up the attachment folder structure and its documents.

Set Up Categories

Access this form with Administrative user rights using Organization>Attachments>Set Up Categories.

Use this form to create a folder structure to organize your attachments, which provides easy classification and retrieval. You can create sub-categories for the system-generated Category folders.

- Encrypted attachments are "physically" stored in the location created using Organization>Attachments>Set Up Locations.
- Linked attachments are simply "linked" to *any* destination in which you choose.

The initial setup automatically created system-defined Category folders (such as Cash Receipts, Vendors) for all installed modules and sub-category folders (such as 2014, Correspondence) for some Category folders. You cannot add or delete these system-defined Category folders; however, you can add up to four levels of sub-categories to each Category folder.

Fields

Category Title: Enter or change the title for an existing sub-category folder. The folders display the structure of the Attachment categories as you are designing it. All of the system-defined Category folders are shown, and you can create up to four levels of sub-category folders under each of these.

Tips:

- You can delete any sub-category folder and its contents.
- Select "Documents Attached" in the Available column for any Posted/Unposted Transaction report to display the number of attachments associated with the accounting entries.
- We recommend limiting your entry to strictly alphabetic characters (A through Z) or numeric characters (0 through 9), and avoiding the use of symbols.

Set Up Categories Example

If you want to create two sub-categories under the Vendor category, follow these steps.

1. Select "Vendors."
2. Click .

3. Enter title "2014."
4. Select "2014."
5. Click .
6. Enter title "2015." Now you have two sub-categories under the Vendor category folder.

Set Up Categories Buttons

	Add Same Level: Use this button to add a sub-category folder to the same level. When you click this button for sub-categories, the Category Title box becomes available and the words "New Category" display. You can then enter the name for the sub-category you wish to create. (The system generates the Category folders and does not allow additions or edits.)
	Add Lower Level: Use this button to add a sub-category folder to a lower level. You can only have up to four sub-category levels.
	Delete Level: Use this button to remove a selected sub-category and all of its contents. (System-generated Category folders cannot be deleted.)
	Move Up: Use this button to move a selected sub-category folder up in the same level. A sub-category cannot be moved to another level; it must be deleted and recreated on the desired sub-category level. (System-generated Category folders cannot be moved.)
	Move Down: Use this button to move a selected sub-category folder down in the same level. A sub-category cannot be moved to another level; it must be deleted and recreated on the desired sub-category level. (System-generated Category folders cannot be moved.)

Chapter 7: User Defined Fields

Set Up User Defined Fields

Use this form to create user defined fields (UDFs). This requires exclusive access to the organization and system databases. (All users must be logged out of the database before you can create user defined fields.)

Set Up User Defined Fields - Setup Tab

Access this tab with Administrative user rights using Organization>Set Up User Defined Fields. This requires exclusive access to the organization and system databases.

Use this tab to set up fields based on A/R invoices, A/R invoices detail, charge codes, customers, employees, {segment codes}, purchase orders, and vendors. To set up transaction document and transaction line records, use this tab along with the Transaction Sources tab.

Note: User defined fields can have an effect on performance, especially while posting, loading documents, running reports, and filtering. Carefully consider creating user defined fields, because the more you create, the longer the processing times throughout the system.

User defined fields can be grouped into three general categories: Master, Transaction Document, and Transaction Line/Detail records.

- *Master* records include user defined fields for maintenance or setup-type data, which is generally entered within the Maintain or Activities menus. If a master level field is created, a User Defined Fields tab will be added to the form in the system. You can connect the user defined field type of *Charge Codes, Customers,* and *Vendors* to certain Transaction Document and Transaction Line level records.
- *Transaction Document* records include user defined fields for transaction entry documents. If a document level field is created, a User Defined Fields tab is added to the Transaction Entry form. You can connect the user defined field type of *Transaction Document* to certain Transaction Line level records.
- *Transaction Line/Detail* records include user defined fields for transaction line items. If a transaction line level field is created, new columns are added to the existing transaction entry table. You cannot connect this type with any other field.

Note: You can create up to 100 user defined fields with the Vendors, Customers, Segment Codes, Charge Codes, Employees, and Purchase Orders (Master) record types. Additionally, you can create up to 20 fields with the Transaction Document record type, and another 20 fields with the Transaction Line/Detail record type.

Multicurrency Users

Each Type is currency specific, except for segments codes. Note that since the Payroll module can only use US Dollar as its functional currency, if an organization uses a functional currency other than USD, the Employee Type is not available.

Purchase Orders and Encumbrances Users

If you are creating user defined fields for purchase orders only, the new fields display on the Activities>Purchase Orders>Create/Modify Purchase Orders>User Defined Fields tab. If you are creating user defined fields for encumbrances only, the new fields display on the Transactions>Encumbrances>Enter Encumbrances and/or Enter Encumbrance Liquidations forms (depending on what you select on the Transaction Source tab.)

Important! If you own the MIP Advance system and get the message that you do not have exclusive access, be sure to review the System>Manage Concurrent Users and System>Manage Services forms; sending emails to the users accessing the system and explaining the need for exclusive access, remind them to save their changes and log out of the system quickly. Afterwards, if you still need to establish exclusive system access, open System>Manage Services. Click the Set Maintenance Mode button and set the organization and system databases offline. This will set the system into maintenance mode and prevent others from logging on to the system but it will also kick the logged on user's out of their databases; thus losing any unsaved work. Once the User Defined Field is created, you will need to clear these check boxes on the Set Maintenance Mode form and place the organization and system databases back online.

Fields

Type: Select one of the following record types in which to apply user defined fields:

- **A/R Invoices**: Adds user defined fields to the Activities>Accounts Receivable>Review/Modify Invoices>User Defined Fields tab. The Accounts Receivable module must be installed.
- **A/R Invoices Detail:**Adds user defined fields to the Activities>Accounts Receivable>Review/Modify Invoices table. The Accounts Receivable module must be installed.

- **Assets**: Adds user defined fields to the Maintain>Fixed Assets>Assets>User Defined Fields tab. The Fixed Assets module must be installed.
- **Charge Codes**: Adds user defined fields to the Maintain>Accounts Receivable>Charge Codes>User Defined Fields tab. The Accounts Receivable module must be installed.
- **Customers**: Adds user defined fields to the Maintain>Accounts Receivable>Customers>User Defined Fields tab. The Accounts Receivable module must be installed.
- **Employees**: Adds user defined fields to the Maintain>Payroll>Employee Information>User Defined Fields tab. The Payroll module must be installed.
- **{Segment Codes}:** Adds user defined fields to the Maintain>Chart of Accounts Codes>User Defined Fields tab. These fields can be assigned for all segments and segment types.
- **Purchase Orders**: Adds user defined fields to the Activities>Purchase Orders>Create/Modify Purchase Orders>User Defined Fields tab. The Purchase Orders module must be installed.
- **Transaction Documents:** Adds the User Defined Fields tab to any of the forms listed on the Transaction Sources tab. Select the appropriate form using the Transaction Sources tab.
- **Transaction Lines**: Adds user defined fields as columns to any of the forms listed on the Transaction Sources tab. Select the appropriate forms using the Transaction Sources tab.
- **Vendors**: Adds user defined fields to the Maintain>Accounts Payable>Vendors>User Defined Fields tab. The Accounts Payable module must be installed.

Field Name: Enter a name for the user defined field. This name is associated with the actual data, not the Display Name in the system. Note that we recommend limiting your field name to strictly alphabetic (A through Z) or numeric characters (0 through 9). You cannot add spaces, but you can change the Display Name for the field.

Description: Enter a description for the field. The description is not available as a column on reports.

Field Characteristics: The following is a list of characteristics that can be assigned to the user defined field:

- **Display Name:** Enter or edit the name of the field. It appears on the designated form in the system and on reports.
- **Required:** Select this check box to require the user to enter a value for the user defined field.

- **Field Type:** Select a type to use for the user defined field, and then the system display its description. We recommend using a *string* instead of a *number* when setting up numeric codes. When the system compresses data, numeric fields are totaled.

Consider the following when selecting a Field Type for a user defined field: The *String, Editable Drop-Down List*, and *Non-Editable Drop-Down List* field types are only available (in the Items by Page group box and the Filter tab) on selected reports. The *Date* and *Yes/No* field types are only available in the Content and Filter tabs of selected reports. The *Number* and *Currency* field types are only available (in the Report Body group box and the Filter tab) on selected reports.

Field Type	Description
Currency	Enter a currency amount in the organization's functional currency, e.g., $0,000.00. User defined fields with a Field Type of Currency will be formatted in the organization's functional currency.
Date	Enter a short date (mm/dd/yy)
Editable Drop-Down List	Enter new data.
Non-Editable Drop-Down List	Select from a drop-down list, which must be set up in the User Defined Fields Setup Table (below).
Number	Enter a number with or without decimals.
String	Enter text.
Yes/No	Select or clear a check box.

- **Shared List Type:** Select an existing non-editable drop-down list to share with the user defined field. For example, if you have a Customer Type UDF, Customers appear in this list, and so on for every possible Type—A/R Invoices, A/R Invoices Detail, Charge Codes, Customers, Employees, {Segment Codes}, Purchase Orders, Transaction Documents, Transaction Lines, and Vendors. This eliminates the need to create new non-editable drop-down lists for every UDF you add, and share what was originally created for another UDF.
- **Shared List Field Name:** If an existing type was selected for re-use in the Shared List Type box, the system displays all existing Field Names for that Shared List Type. This allows you to specify an existing shared list. For example, if you selected Purchase Orders as the Shared List Type, and you had existing purchase order fields of "Authorized By" and "Date," those two fields would be available in this drop-down list.

- **Length:** Enter a number between 1 and 255 which represents the maximum number of characters allowed in the field. This box is only available if Editable Drop-Down List, Non-Editable Drop-Down List, or String was selected as the field type.
- **Decimal Places:** Enter the number of decimal places (up to five) for the field. This box is only available if Number was selected as the field type.
- **Default:** Enter a value to be used as the default when the user defined field is displayed in the system (such as 03/17/15 for date, 1,234.56 for currency, or 1,234.5 for number). When you add a default value to a user defined field, this value displays on new entries, not existing ones. This box is not available for the Non-Editable Drop-Down List Field Type.

User Defined Fields Setup Table: Enter codes and their values for user defined fields that have a Field Type of Non-Editable Drop-Down List.

- **Code:** The code you want to create for the user defined field. It displays in the drop-down list of the field. Once a code has been used in the system, you cannot remove it. However, you can mark it as Discontinued.
- **Description:** A description of the code.
- **Default:** This check box indicates which code to use as the default code.
- **Status:** The status of the code: Active (A), Inactive (I), or Discontinued (D).

Tips:

- To print data entered on this form, use Reports>Lists>User Defined Fields List.
- If you create two user defined fields with a type of Number and a transaction source of BD, and assign one or both of them a default value, when the budget worksheet (containing one of the UDFs) is transferred (Activities>Budget Worksheet), the system also includes the default value of the second UDF.
- If you have a Transaction Document or Transaction Line type user defined field, and the document is reversed or voided, the Number field type receives the opposite sign of the original amount. Consider this when assigning the Number field type to user defined fields.
- If you want data from a user defined field name to flow to another user defined field (a master level record, transaction document level record, and/or transaction line/detail level record), ensure that a UDF with the same name is created at each level. This UDF must also have the same number of decimal places and the same field type, such as string to string, date to date, and number to number. Then, you can use Organization>Set Up UDF Default Sources to "connect" the UDF, so that the UDF flows through each level.
- User defined fields are automatically applied to accounts payable (APV) and general ledger (VCK) void checks (Activities>Check Writing>Void Checks/Vouchers/Invoices).
- We recommend that you use Number field types for tracking items such as Units; and String, Editable Drop-Down List, or Non-Editable Drop-Down List field types for tracking items such as Contract Numbers.
- The functional currency was determined by the Administrator when the organization was created (File>New Organization>Functional Currency panel).

Set Up User Defined Fields - Transaction Sources Tab

Access this tab with Administrative user rights using Organization>Set Up User Defined Fields. This requires exclusive access to the organization and system databases.

Use this tab to determine where to assign Transaction Document and Transaction Line type user defined fields that were created on the Setup tab.

- If the field was set up as a Document type, the fields display on a new tab named "User Defined Fields." For example, if you create a user defined field for a CR transaction source code, the existing Cash Disbursements entry form changes to a tab entitled "Transaction Entry," and the

- system adds a new tab named "User Defined Fields."
- If the field was set up as a Transaction Lines type, the fields display as columns added to the existing transaction entry/detail table on the form designated here. For example, if you create a user defined field for a CR transaction source code, new columns are added to the transaction entry table (Transactions>Enter Cash Receipts).

Important! If you own the MIP Advance system and get the message that you do not have exclusive access, be sure to review the System>Manage Concurrent Users and System>Manage Services forms; sending emails to the users accessing the system and explaining the need for exclusive access, remind them to save their changes and log out of the system quickly. Afterwards, if you still need to establish exclusive system access, open System>Manage Services. Click the Set Maintenance Mode button and set the organization and system databases offline. This will set the system into maintenance mode and prevent others from logging on to the system but it will also kick the logged on user's out of their databases; thus losing any unsaved work. Once the User Defined Field is created, you will need to clear these check boxes on the Set Maintenance Mode form and place the organization and system databases back online.

Fields

Transaction Sources Available Items, Selected Items: The system displays all available transaction source codes and their descriptions. Use the Mover (>) to move a code from the Available Items box to the Selected Items box.

The BD Transaction Source can only be used for Transaction Line type user defined fields that are assigned a number. Furthermore, it must be selected with at least one other Transaction Source. This allows you to capture "actual" amounts that can then be tracked using the Activities>Budget Worksheet.

Depending on the Transaction Source code selected here, the user defined field appears on the following forms. (You may not see all transaction sources, depending on the modules you have installed.)

Transaction Source	Transaction Document and Transaction Line Forms
APC	Transactions>Accounts Payable>Enter Manual A/P Checks
API	Transactions>Accounts Payable>Enter A/P Invoices

Transaction Source	Transaction Document and Transaction Line Forms
APM	Transactions>Accounts Payable>Enter A/P Credits
APS	Transactions>Accounts Payable>Edit Pay Selected A/P Invoices
ARB	Transactions>Accounts Receivable>Enter A/R Invoices
ARC	Transactions>Accounts Receivable>Enter A/R Receipts
ARP	Transactions>Accounts Receivable>Enter A/R Receipts - Prepayments
ARM	Transactions>Accounts Receivable>Enter A/R Credits
ARS	Transactions>Accounts Receivable>Edit A/R Invoices
BD	Transactions>Enter Budget
CD	Transactions>Enter Cash Disbursements
CDS	Activities>Check Writing>Write Checks
CR	Transactions>Enter Cash Receipts
CRS	Activities>Receipt Writing
ENC	Transactions>Encumbrances>Enter Encumbrances
ENL	Transactions>Encumbrances>Enter Encumbrance Liquidations
JV	Transactions>Enter Journal Vouchers

Set Up UDF Default Sources

Access this form with Administrative user rights using Organization>Set Up UDF Default Sources.

Use this form to "connect" user defined field (UDF) values from master level records to transaction document and transaction line/detail level records. This process is known as flow-thru. (The system facilities several "Flow-Thru Scenarios" (page 109).) If you want a user defined field name to flow to another user defined field, you must have previously created UDFs (Organization>Set Up User Defined Fields) with the same name at each level (master, transaction document, and transaction line/detail). These UDFs must also have the same number of decimal places and the same field type, such as, string to string, date to date, and number to number.

Note: Master UDFs cannot flow to other Master UDFs, and Transaction Document and Transaction Line UDFs cannot flow to Master UDFs.

Fields

Type: Enter a record type that can have UDF Default Source (flow-thru) values.

- A/R Invoices - Uses data from the Activities>Accounts Receivable>Review/Modify Invoices>User Defined Fields tab.
- A/R Invoices Detail - Uses data from the Review/Modify Invoices table (Activities>Accounts Receivable>Review/Modify Invoices).
- Transaction Documents - Uses data from User Defined Fields tabs. This does not include every transaction source available on the Set Up User Defined Fields>Transaction Sources tab.
- Transaction Lines - Uses data from user defined field columns from Transaction Entry forms. This does not include every transaction source available on the Set Up User Defined Fields>Transaction Sources tab.

Field Name: Select a specific Receiving UDF to be assigned a Default Source (or flow-thru). The list only displays field names associated with the type selected above. This is the field name created on the Set Up User Defined Fields form.

Each receiving UDF can have multiple Transaction Sources, which can have a different source or share the same source UDF.

Default Source Assignment: This identifies another UDF in which you want to connect the Field Name UDF. You will identify the type and field name of the Default Source UDF in this table.

Since A/R Invoices and A/R Invoices Detail are Master Records, the Available Transaction Source, Description, Transaction Source, and Additional Transaction Source columns are not available, if you choose one of these as your type.

- **Available Transaction Source:** The system displays all Transaction Source codes assigned to this UDF using the Set Up User Defined Fields>Transaction Sources tab.
- **Description:** The system displays the description associated with the Transaction Source.
- **Type:** Enter a UDF type (such as, Vendors, Charge Codes, Customers, or Transaction Documents). The system only displays the types that can be used with the Additional Transaction Source on that row. Types were assigned to UDFs on the Set Up User Defined Fields form.

- **Field Name:** Enter a Source UDF Field Name. The system only displays those UDFs that can be used as a Default Source for the Additional Transaction Source on that row. You must have previously created a field name that is the same field type (such as, string, number, or date) as the UDF Field Name above.
- **Transaction Source:** Enter a UDF Transaction Source for the Default Source Field Name—APC, API, APM, APS, ARB, ARC, ARM, ARP, ARS, CD, CDS, CR, or CRS. This column is not available if the Type selected is a Master UDF, such as, Vendors, Customers, and Purchase Orders.
- **Additional Transaction Source:** Enter a UDF Transaction Source for the selected Available Transaction Source that can be assigned as a Default Source. The column is only available if both ARB and ARS are included as an Available Transaction Source. ARC can be assigned a default source of ARB, ARS, or both.

Tips:

- To print data entered on this form, use Reports>Lists>UDF Default Sources List.
- The transaction source BD (Transactions>Enter Budget) is not available in the Default Source Assignment table, even if it has been selected in the Set Up User Defined Fields form.
- Field Types for Source and Receiving UDFs: The data type of the source and receiving UDFs must be the same (such as, string to string, date to date, and number to number). However, there are some exceptions with regards to Non-editable Drop-Down Lists. You can assign Non-editable to Editable or Non-editable to String; but not String to Non-editable or Editable to Non-editable. The number of decimal places in the Source UDF must be the same as the number of decimal places in the Receiving UDF selected.

Flow-Thru Scenarios

Consider the following flow-thru scenarios, with Administrator user rights when setting up the Organization>Set Up UDF Default Sources form:

- Vendor to API Transaction Documents to APS Transaction Lines, APC Transaction Lines, or APM Transaction Lines.
- Customers to A/R Invoices Detail to ARS Transaction Documents
- Customers to ARB Transaction Documents to ARC Transaction Lines
- Customers to ARS Transaction Documents to ARC Transaction Lines
- Charge Codes to A/R Invoices Detail to ARS Transaction Documents or ARS Transaction Lines

Example

The following example describes the first option above. Suppose you want to track a "Contract Number" from the vendor record (Maintain>Accounts Payable>Vendors), to an A/P invoice (Transactions>Accounts Payable>Enter A/P Invoices), all the way through to an A/P check (Activities>Accounts Payable>Pay Selected A/P Invoices). You must first create three UDFs called Contract Number. As the Administrator, use the Organization>Set Up User Defined Fields form as follows:

1. Select a type of Vendor, a field name of ContractNumber, and a field type of string.
2. Select Transaction Document, ContractNumber, and string. Then, select API on the Transaction Sources tab.
3. Select Transaction Lines, ContractNumber, and string. Then, select APS on the Transaction Sources tab.

   Now, you are ready to connect these fields using the Set Up UDF Default Sources form.
4. Select a type of Transaction Documents, a field name of ContractNumber, a default source type of Vendors, and a default field name of ContractNumber. This connects the Vendor record to the A/P invoice.
5. Select Transaction Lines, ContractNumber, Transaction Documents, and ContractNumber. Then, select API on the Transaction Sources tab. This connects the A/P invoice to the A/P check.
6. Select Transaction Lines, ContractNumber, Transaction Documents, and ContractNumber, Then, select APS on the Transaction Sources tab. This connects all three pieces together.

Now, if you enter a contract number on the Maintain>Accounts Payable>Vendors>User Defined Fields tab, the system displays that value on the Transactions>Accounts Payable>Enter A/P Invoices>Transaction Entry tab, and on the Edit Pay Selected A/P Invoices>Transaction Entry tab.

Source/Receiver Relationships Outline

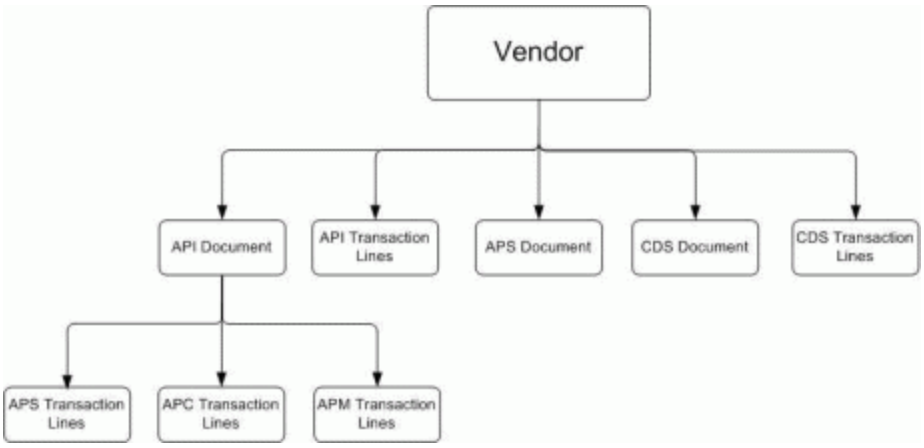
The following table outlines all Source/Receiver relationships that can be created using the system. To view flowcharts of the A/P and A/R process, see A/P Flow-Thru and A/R Flow-Thru.

Source	Receiver
Vendor (Maintain>Accounts Payable>Vendors)	API Transaction Documents (Transactions>Accounts Payable>Enter A/P Invoices)
	API Transaction Lines (Transactions>Accounts Payable>Enter A/P Invoices - Transaction Entry Table)
	APS Transaction Documents; A/P System Generated Checks/Vouchers (Transactions>Accounts Payable>Edit Pay Selected A/P Invoices)
	CDS Transaction Documents (Activities>Check Writing>Write Checks)
	CSD Transaction Lines (Activities>Check Writing>Write Checks - Transaction Entry Table)
API Transaction Documents (Transactions>Accounts Payable>Enter A/P Invoices)	APS Transaction LInes; A/P System Generated Checks/Vouchers (Transactions>Accounts Payable>Edit Pay Selected A/P Invoices - Transaction Entry Table)
	APC Transaction Lines (Transactions>Accounts Payable>Enter Manual A/P Checks - Transaction Entry Table)
	APM Transaction Lines (Transactions>Accounts Payable>Enter A/P Credits - Transaction Entry Table)
Charge Code (Maintain>Accounts	A/R Invoice Detail (Activities>Accounts Receivable>Review/Modify Invoices -

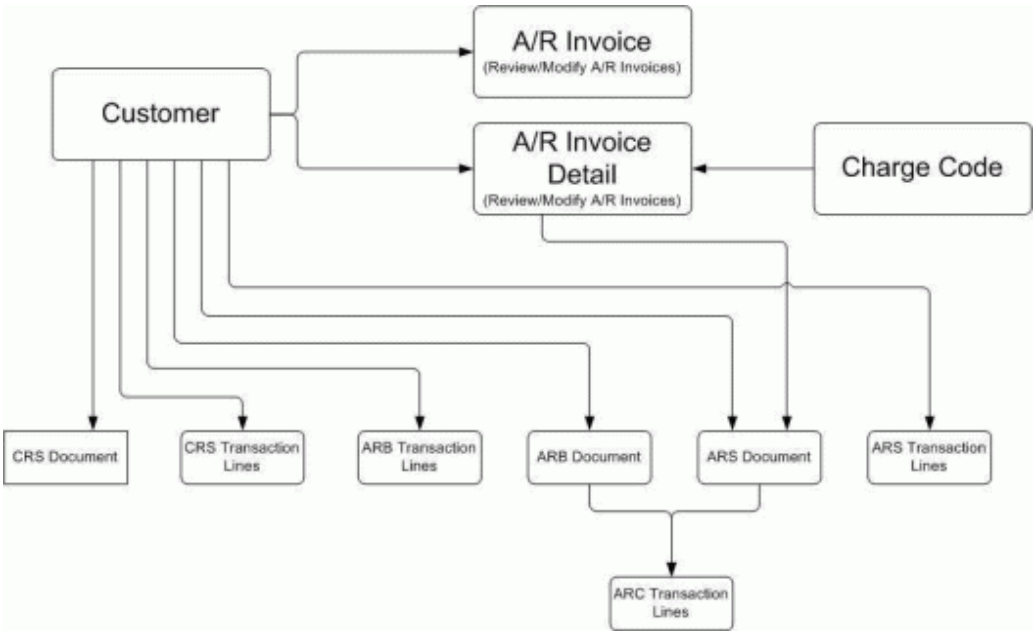
Source	Receiver
Receivable>Charge Codes)	Transaction Entry Table)
Customer (Maintain>Accounts Receivable>Customers)	A/R Invoice (Activities>Accounts Receivable>Review Modify Invoices)
	A/R Invoice Detail (Activities>Accounts Receivable>Review/Modify Invoices - Transaction Entry Table)
	ARB Transaction Documents (Transactions>Accounts Receivable>Enter A/R Invoices)
	ARB Transaction Lines (Transactions>Accounts Receivable>Enter A/R Invoices Transaction Entry Table)
	ARS Transaction Documents; A/R System Generated Invoices (Transactions>Accounts Receivable>Edit A/R Invoices)
	ARS Transaction Lines; A/R System Generated Invoices (Transactions>Accounts Receivable>Edit A/R Invoices - Transaction Entry Table)
	CRS Transaction Documents (Activities>Receipt Writing)
	CRS Transaction Lines (Activities>Receipt Writing - Transaction Entry Table)
A/R Invoice Detail (Activities>Accounts Receivable>Review/Modify Invoices - Transaction Entry Table	ARS Transaction Documents; A/R System Generated Invoices (Transactions>Accounts Receivable>Edit A/R Invoices)

Source	Receiver
ARB Transaction Documents (Transactions>Accounts Receivable>Enter A/R Invoices)	ARC Transaction Lines (Transactions>Accounts Receivable>Enter A/R Receipts - Transaction Entry Table)
ARS Transaction Documents; A/R System Generated Invoices (Transactions>Accounts Receivable>Edit A/R Invoices - Transaction Entry)	

A/P Flow-Thru



A/R Flow-Thru


A/R Invoice
(Review/Modify A/R Invoices)
Customer
A/R Invoice Detail
(Review/Modify A/R Invoices)
Charge Code
CRS Document
CRS Transaction Lines
ARB Transaction Lines
ARB Document
ARS Document
ARS Transaction Lines
ARC Transaction Lines

Chapter 8: Alerts

Alerts give you the ability to detect potential fraudulent activity that may otherwise go unnoticed. You can set alerts to notify specific users inside and outside of MIP when: there are changes in cash balance or document amounts, failed log on, checks that have been printed and then deleted from the system, checks that have been reprinted, change in Pay Rate for employee, a change in vendor names, and a system user has written a check to their self.

These notifications can be sent using real-time email or in-product messaging, or at your demand by viewing the Alerts Message Center.

Note: Real-time notifications require a separate IIS installation and SMTP email connectivity.

Set Up Alerts

Use this form to create and configure, preview, and assign alerts in the system.

Set Up Alerts - Setup Tab

Access this form with Administrative user rights using Organization>Set Up Alerts.

Use this form to create and configure, preview, and assign alerts in the system. Create a unique name for each alert, chose who will receive it, and how they should be notified - either as a menu display while logged in the system or email. Once the alert has been setup, use the Preview Tab to edit and preview the message, and the Assign Tab select the users who will receive the alert notification.

Use this tab to create and configure alerts.

Creating an alert:

- To notify the CFO when your budget goes over a certain percentage of the budgeted amount spent, see How Do I Create an Alert - Budget Tolerance?
- To notify an AP Clerk when the cash balance falls to or below $10,000, see How Do I Create an Alert - Cash Balance Threshold?
- To notify the AP Supervisor when someone in your organization cuts a check to a linked system user, see How Do I Create an Alert - Check Issued to Linked Users?

- To notify the AP Supervisor when a check is printed without a valid Vendor ID on the Write Checks activity form, see How Do I Create an Alert - Check Issued without Vendor ID?
- To notify the Payroll Supervisor when someone in your organization changes the pay rate for any employee, see How Do I Create an Alert - Employee Pay Rate Change?
- To notify the CFO when someone in your organization prints a system generated check or voucher but does not record it, see How Do I Create an Alert - Printed Check/Voucher Not Recorded?
- To notify the CFO when someone in your organization deletes a system generated check, voucher, or a session, see How Do I Create an Alert - System Check/Voucher Deleted?
- To notify the System Administrator when someone is attempting to incorrectly log on to your organization, see How Do I Create an Alert - Three Failed Log On Attempts?
- To notify an AP Clerk when someone in your organization initiates or changes a Hold Payment on a vendor, see How Do I Create an Alert - Vendor Hold Payment Changed?
- To notify the AP Supervisor when someone in your organization changes the name on a vendor ID, see How Do I Create an Alert - Vendor Name Change?
- To notify the AP Supervisor when someone in your organization initiates a payment to a vendor with an amount over $500, see How Do I Create an Alert - Vendor Payment Threshold?

Fields

Name: Enter a unique name to represent the alert you are setting up, or use the drop-down list to select an existing alert to change. This field is required.

Importance: Select the level of importance for this alert. When creating a new alert, if you do not know the level of importance, accept the default of *Medium*, or select **High**, **Low** from the drop-down list. The importance can be changed at any time.

Status: Specify the status of the alert. When creating a new alert, accept the default status, A (Active), or select I (Inactive) from the drop-down list. The status of Inactive disables the alert, so that it cannot be used in the system. A status of discontinued is not available on this form. The status can be changed at any time.

Real-time Notices: Select an option for how the system will notify the recipient about this alert. Choose to send an email, display on the menu bar, select both, or neither to only enter the alert in the Message Center. (Real-time Notifications require some additional setup, see How Do I Set Up Alerts?)

- **Email:** Select this box to have the system send an email, as the way to be notified about this alert.
- **In-product:** Select this box to have a menu display, while the recipient is logged on to the system, as the way to be notified about this alert.

Configure: Select the module and the specific event in which you want to be alerted.

- **Module:** Select from the drop-down list, the module in which the alert is related.
- **Event:** Select the type of event in which you want to be alerted.

Filter: This group box contains your alert options based on the focus and event selected. You are required to filter on at least one item.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the Alert is limited to the data that falls within the designated filter criteria.
- **Compares To:** Select an operator from the drop-down list.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the ***IN*** operator.

Note: Note that User IDs and Vendor IDs that contain symbols or special characters, such as commas, cannot be included with the ***IN*** operator range; each User ID or Vendor ID filtered will need to be in a separate Alert.

Tips:

- Use the Alert Limit filter to limit the number of notifications you receive for a specific alert, such as cash balance. For example, select the Alert Limit equals one hour, to be notified the first time the alert occurs and then to be notified at hour long intervals until there are no other occurrences. At the next occurrence of the alert notification, the hour long intervals will be reset.
- System Users have the ability to turn off the Real-time In-product notifications, by clearing the Connect to the Alert Server check box on the Options>User Preferences form. If not selected, the alerts will continue to collect in the Message Center and Real-time Email Alert Notices will be sent, but the number count on the Message Center will not reflect accurately.

Set Up Alerts - Preview Tab

Access this form with Administrative user rights using Organization>Set Up Alerts.

Once the alert has been setup, use this tab to view the subject line and edit and preview the message for the alert.

Editing and previewing an alert message:

- For the CFO when your budget goes over a certain percentage of the budgeted amount spent, see How Do I Create an Alert - Budget Tolerance?
- For an AP Clerk when the cash balance falls to or below $10,000, see How Do I Create an Alert - Cash Balance Threshold?
- For the AP Supervisor when someone in your organization cuts a check to a linked system user, see How Do I Create an Alert - Check Issued to Linked User?
- For the AP Supervisor when a check is printed without a valid Vendor ID using the Write Checks activity form, see How Do I Create an Alert - Check Issued without Vendor ID?
- For the Payroll Supervisor, when someone in your organization changes the pay rate for any employee, see How Do I Create an Alert - Employee Pay Rate Change?
- For the CFO when someone in your organization prints a system generated check or voucher but does not record it, see How Do I Create an Alert - Printed Check/Voucher Not Recorded?
- For the CFO when someone in your organization deletes a system generated check, voucher, or a session, see How Do I Create an Alert - System Check/Voucher Deleted?
- For the System Administrator when someone is attempting to incorrectly log on to your organization, see How Do I Create an Alert - Three Failed Log On Attempts?
- For an AP Clerk when someone in your organization initiates or changes a Hold Payment on a vendor, see How Do I Create an Alert - Vendor Hold Payment Changed?
- For the AP Supervisor when someone in your organization changes the name on a vendor ID, see How Do I Create an Alert - Vendor Name Change?
- For the AP Supervisor when someone in your organization initiates a payment to a vendor with an amount over $500, see How Do I Create an Alert - Vendor Payment Threshold?

Fields

Email: Enter the From address and Subject line for the Alert message that you created on the Setup Tab.

- **From:** Accept the default email address or enter an email address that can be used specifically for this alert message. It is recommended that the Administrator creates a default "From" email address using the Options>System Preferences form. By keeping a consistent From address your email recipients will recognize and identify where the email is coming from and will more likely NOT mark the email as spam; which is important to ensure the delivery and receipt of the notification. It is recommended that you create a generic email address, related to the purpose of your alert email, but use something the receiver will recognize and know it is a trusted source. Some examples include: "alert@yourorganization.org", "MIPalert@yourdomain.gov", and "yourorganizationALERT@yourdomain.com"
- **Subject:** Accept the default Subject line which references the organization generating the alert or enter a meaningful Subject line. This is important to ensure the delivery and receipt of the notification.

Message: Compose the message in the edit field and preview it.

- **Edit:** Accept the default message, or customize the notification using the Key Term variables < >. Note that the information in the variable <Key Terms> contains coded information, sometimes it can be edited but most of the time it is meaningful in the final message. Or if your alert is specific, you can remove the variables and enter your own information. NOTE that when a message variable is removed, that information will be excluded from the message of the issued alert. For more information about these variables are and how to use, see "Alert Message Terms" (page 119).
- **Preview:** The system displays the editable message above. Once you have entered your message information, click the **Update** button to display your message. Click the **Reset** button to remove all previous edits to the message and to recover any message variables that may have been deleted.

Alert Message Terms

Below are all of the key term variables and their descriptions, available in the Alerts Set Up Alerts form.

Key Term	Definition
<Amount>	The amount of the check that was sent to the printer.
<Balance>	The balance amount specified in the Cash Balance area for the Balance Threshold event. For example, $10,000.
<Document Number>	The document number, such as check number.
<Employee ID>	The identity of the employee.
<Employee Name>	The name of the employee associated to the Employee ID.
<GL Code>	The General Ledger Account Code ID. For example, 11001.
<GL Title>	The General Ledger Account Code's title. For example, Cash in Checking.
<Linked User ID>	The system User ID that is associated to an Employee or Vendor.
<Linked User Name>	The System User Name that is associated to an Employee or Vendor.
<Message>	The content of the message specific to the alert being composed. Replace this key term with customized content of the message body but leave the other Key Terms when composing the message. For example, The cash balance has only <Balance> remaining for G/L Account Code <GL Code>, <GL Title>.
<Payment>	The amount of the payment specified in the Check Writing area for the Pay Selected A/P Invoices event. For example, $500.00
<To Name>	The name entered for whom a check was sent to the printer, such as Employee ID, Payee, or Vendor ID.
<User ID>	The identity of the user logged on to the system.
<User Name>	The name of the user associated to the User ID.
<Vendor ID>	The identity of the vendor.
<Vendor Name>	The name of the vendor associated to the Vendor ID.
<Workstation Name>	The computer name for the workstation being accessed.

Tips:

- It is a good idea to keep the key term variables in the message, so that the notification can contain specific information regarding the alert.
- For example, if you created an alert to watch for Payroll pay code changes - you would want to know who changed the pay code and for which employee it was changed. So, the <User Name> and <Employee Name> key terms would not be edited.
- However, if you create an alert to watch a specific vendor and the name of that vendor has not been updated in the system, it might be a good idea to use the name you recognize for the specific vendor when alerted.

Set Up Alerts - Assign Tab

Access this form with Administrative user rights using Organization>Set Up Alerts.

Use this tab to assign the users who will receive the alert notification.

Assigning users to be alerted:

- Consider the CFO when your budget goes over a certain percentage of the budgeted amount spent, see How Do I Create an Alert - Budget Tolerance?
- Consider an AP Clerk, when the cash balance falls to or below $10,000, see How Do I Create an Alert - Cash Balance Threshold?
- Consider the AP Supervisor, when someone in your organization cuts a check to a linked system user, see How Do I Create an Alert - Check Issued to Linked Users?
- Consider the AP Supervisor, when a check is printed without a valid Vendor ID on the Write Checks activity form, see How Do I Create an Alert - Check Issued without Vendor ID?
- Consider the Payroll Supervisor, when someone in your organization changes the pay rate for any employee, see How Do I Create an Alert - Employee Pay Rate Change?
- Consider the CFO when someone in your organization prints a system generated check or voucher but does not record it, see How Do I Create an Alert - Printed Check/Voucher Not Recorded?
- Consider the CFO when someone in your organization deletes a system generated check, voucher, or a session, see How Do I Create an Alert - System Check/Voucher Deleted?

- Consider the System Administrator, when someone is attempting to incorrectly log on to your organization, see How Do I Create an Alert - Three Failed Log On Attempts?
- Consider an AP Clerk, when someone in your organization initiates or changes a Hold Payment on a vendor, see How Do I Create an Alert - Vendor Hold Payment Changed?
- Consider the AP Supervisor, when someone in your organization changes the name on a vendor ID, see How Do I Create an Alert - Vendor Name Change?
- Consider the AP Supervisor, when someone in your organization initiates a payment to a vendor with an amount over $500, see How Do I Create an Alert - Vendor Payment Threshold?

Fields

ID: In the Available Items column, select the name of the user who the alert will be assigned, and then click the Mover (>) to move the item to the Selected Items column.

- **Available Items:** The Available Items list displays your available IDs. Assign a name to your alert by clicking the name in the Available Items box twice to move it to the Selected Items box. You may also use the Mover buttons (>, >>) to move one or more highlighted names to the Selected Items box. You may also re-size the columns by clicking the line between the headings and moving it until the columns are the size you would like.
- **Selected Items:** Remove an ID from the Selected Items box by clicking the name twice to move it to the Available Items box. You may also use the Mover buttons (<<, <) to move one or more highlighted names to the Available Items box.

Copy Alerts Setup

Access this form with Administrative user rights using Organization>Set Up Alerts> Copy.

Use this form to copy the alert settings for the selected alert to a different alert. Click OK to complete the copy process.

Fields

Copy From Name: Select an existing alert name that contains the alert settings that you want to copy.

Copy To Name: Enter a unique Alert name for the new alert. The Drop-Down Lookup opens a list of existing Alerts. None of the names in the list can be used for the new alert.

Alerts Activity Log

Access this form with Administrative user rights using Organization>Alerts Activity Log.

Use this form to view and/or print all of the alerts that have been detected and recorded in the system.

Fields

Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Alerts Table: The system displays the applicable columns for the preceding form. Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The default value for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.

Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading. The column on which items are sorted has (ascending order) or (descending order) in the column heading.

Tips:

- Click to print a list of alerts in the activity log.
- Use the Display Records button to refresh the table.
- When filtering data, select Operators to determine which data to display. Also, view a list of Filter Examples that are useful throughout the system and examples of How to Use Wildcards characters with Like and Not Like.
- In the Available Items table, you can sort the data based on any column. Simply double-click on a column heading to sort according to that column.
- The sorting functionality is only for table display and does not affect printing. Print uses the data from the database and is therefore not reflective of how the items were sorted.
- For larger organizations with many records, you may want to clear the "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it will eliminate the time it takes to load the Find form.

Chapter 9: Grant Administration

Set Up Grant Administration Module

Access this tab with Administrative user rights using Organization>Set Up Modules>Grant Administration. It is only available if the Grant Administration module is installed.

Use this form to determine which segment to use as the Grant Administration segment. Segments must have been previously set up using the File>New Organization wizard.

Fields

Designate Grant Segment: Enter or select the segment name to use as the grant segment. The General Ledger segment is not available.

Activate Grant Management Integration: Select this check box if you own the Grant Management system and prefer to maintain your grant information there. Note that by selecting this check box, the MIP Accounting system will make some of the existing information read-only on the two Grant Administration tabs (Chart of Accounts>Grant Administration Tab and Grantor Information Tab) in order for your grant data to be maintained in the Grant Management system. Also, be sure the Grant Management system is installed and set up a connection to the MIP Accounting organization database.

Tips:

- Use Reports>Lists>Chart of Accounts to print the data entered on this form.
- If this menu selection is not available, determine if the module needs to be added to the current organization using the Organization>Add a Module wizard.

Chapter 10: Utilities

Backup

Access this form using File>Backup.

Use this form to back up existing organization and system databases. The path to the database backup file is from the server's perspective. So, if you are running a local install of the server, by default, the backup will reside on the local hard drive.

We recommend that you use this form to back up your database, rather than other backup software. Often times when backing up with other software, the database is shown to be "in use." However, if you want to use your other backup software, you should use this form to back up first, and then run your other backup software. You can then make a back up of your database using your other software.

Note: Ensure all users are logged out of the system and/or organization prior to backing up your database.

MSDE and SQL Express Users

The system (NpsSqlSys) backup is always stored in the Backup directory of the Microsoft SQL Server folder. By default, organization backups are stored here also.
If data was backed using other software, the file cannot be restored using the File>Restore form. In such a case, the database should be backed up using this form, and then your backup software. That way your backup can be restored, if necessary.

Nonprofit Online Users

MIP manages organization and system database backups automatically for you; therefore, the Backup menu selection is not available. Full backups are performed weekly and differential backups are performed daily. See Nonprofit Online.

SQL Server Users

The system (NpsSqlSys) backup is always stored in \MSSQL\Backup. By default, organization backups are stored here as well.

Fields

Database to Backup: Select an existing database to back up using the drop-down list. The list contains the system database (NpsSqlSys), the NTO database (if it was installed), and any organization databases that have been created.

Backup to File: The system displays the file name for the database being backed up. However, you can change the path and file name.

Tips:

- The system backs up any database selected from the Database to Backup drop-down list—not the database for the active organization.
- The backup process can take several minutes or longer to complete, depending on the size of the databases. Very large databases may take some time. When you make a backup, the system makes a copy of your database. The backup files are not compressed; therefore, they will be about the same size as your database.
- If you use Browse to change the location of the backup on your server, you will only see hard drives that are available on the computer on which the server component of the system is installed.
- If Warning on Exit is selected (Options>Customize Workstation Settings>Alerts tab) and you have rights to this form, a message displays asking if you want to back up the database upon existing the system. If you click Yes, the system automatically displays this form. After closing this form, the system is exited regardless if the database was backed up.
- If you perform a nightly backup to another source, ensure that you backup your Backup directory instead of your Data directory. You cannot copy files from the Data directory while the system is running.
- You should maintain the files in your Backup directory. The size of this directory could increase over time. You should clean it out periodically to avoid using up free disk space.

Backing Up Databases

To Back Up a System Database

1. Ensure all users are logged out of the system.
2. Open the File>Backup form.

3. Select the system database, and then the file name displays in the Backup to File box. You cannot change the file name or where the database is stored. The database is named according to the following format:

Name	Year				Month		Day		Time			
15.x.0.0-NpsSqlSys-	2	0	1	2	0	3	0	9	1	3	2	5

   For example, if NpsSqlSys is backed up on March 9, 2012 at 1:25 p.m., the name of the backup file will be 15.x.0.0-NpsSqlSys-201203091325. The version number will appear in front of the NpsSqlSys backup name. You will not be able to restore a system database unless it has the appropriate version number in the backup name.
4. Click Start to begin the database backup process.

To Back Up an Organization Database

1. Ensure all users are logged out of the organization.
2. Open the File>Backup form.
3. Select the organization database, and then the file name displays in the Backup to File box.
4. You can change the file name and path using Browse , if needed. By default, the database is named according to the following format:

Name	Year				Month		Day		Time			
NTO-	2	0	1	2	0	3	0	9	1	3	2	5

   For example, if NTO is backed up on March 9, 2012 at 1:25 p.m., the name of the backup file will be NTO-201203091325.
5. Click Start to begin the database backup process.

How do I give a user permission to backup?

If the Administrator creates a new user and want them to be able to perform backups, complete the following steps:

1. Select the user's ID (Security>Set Up System Menus)
2. Expand Administration and File in order to select Backup. Then select the "Process Records" check box in the Rights section.
3. Click Save.

The user now has the ability to perform backups though out the system. Without completing these steps above there is no menu selection for backup and in Payroll the backup request that should occur when printing checks does not display.

Restore

Access this form with Administrative user rights using File>Restore.

Use this form to restore both system and organization databases. The databases must have been previously backed up using File>Backup; if data was backed up using other software, the file cannot be restored using this form.

Note: Ensure that all users are logged out of the organization prior to starting this process.

When a database is backed up, the system automatically associates the backup path and filename with the organization database you are backing up. For example, suppose the NTO organization was backed up to \Backup\NTO-201303091325.NPS. In this case, NTO is associated with that path and filename. If you decide to restore the backup file, you must select NTO from the Restore to Database box. At this point, any NTO backup database can be restored including \Backup\NTO-201303091325.NPS. The version number appears in front of the NpsSqlSys backup name. You cannot restore a system database unless it has the appropriate version number in the backup name.

Nonprofit Online Users

The Restore menu selection is not available. If you need to restore a database, please contact Customer Support via web ticket, chat, or phone. See contact information and support hours on the Support Resources page. For more information, see Nonprofit Online.

Fields

Restore to Database: Select an existing database to restore using the drop-down list. The list contains the system database (NpsSqlSys), the NTO database (if it was installed), and any organization databases that have been created. Only backup files that are associated with the selected database can be restored.

Restore from File: Enter the path and filename for the database being restored. If necessary, use Browse to locate the file.

If you use Browse , you will only see hard drives that are available on the computer on which the server component of the system is installed.

Compress

Access this form with Administrative user rights using File>Compress.

Use this form to compress both system and organization databases. Compression reduces the size of your database; with a large database, this can take time. Select the database and then, click Start to begin the compression process.

Nonprofit Online Users

MIP manages database compression procedures on a regular basis automatically for you; therefore, the Compress menu selection is not available. See Nonprofit Online.

Fields

Select a Database to Compress: Select an existing database to compress. The drop-down list contains the system database (NpsSqlSys), the NTO database (if it was installed), and any organization databases that have been created.

Data Integrity Checks

Access this form with Administrative user rights using Organization>Data Integrity Checks. This requires exclusive access to the system database and IIS Server.

Use this form to check the integrity of your data files. It allows you to conduct a complete check of data, which identifies errors in the tables.

Data Integrity checks take time to process. It is recommended that the first time you run integrity checks you do so at a time you can afford to be out of the software for some time. You need to benchmark how long the integrity checks take to process for your organization. The amount of time needed for the checks to complete varies based on the hardware configuration and the size of the database being checked.

Important! For **SYSTEM ADMINISTRATORS with Employee Web Services**, the data integrity check requires exclusive access to the system database, including the IIS server. Before running a data integrity check, you will need to sever the connections to the IIS server running EWS or shut down IIS while running the data integrity checks. Otherwise, the operation fails with an error message.

Multicurrency Users

If you experience failing data integrity checks associated with Cash, Accounts Payable, and Accounts Receivable balances, use Activities>Revalue Multicurrency to adjust functional currency balances for foreign cash accounts to accurately reflect current exchange rates and record appropriate realized gains and losses.

Important! If you own the MIP Advance system and get the message that you do not have exclusive access, be sure to review the System>Manage Concurrent Users and System>Manage Services forms; sending emails to the users accessing the system which explain the need for exclusive access, remind them to save their changes and log out of the system quickly. Afterwards, if you still need to establish exclusive system access, open System>Manage Services. Click the Set Maintenance Mode button and set the organization and system databases offline. This will set the system into maintenance mode and prevent others from logging on to the system but it will also kick the logged on user's out of their databases; thus losing any unsaved work. Once the Data Integrity Checks are complete, you will need to clear these check boxes on the Set Maintenance Mode form and place the organization and system databases back online.

Fields

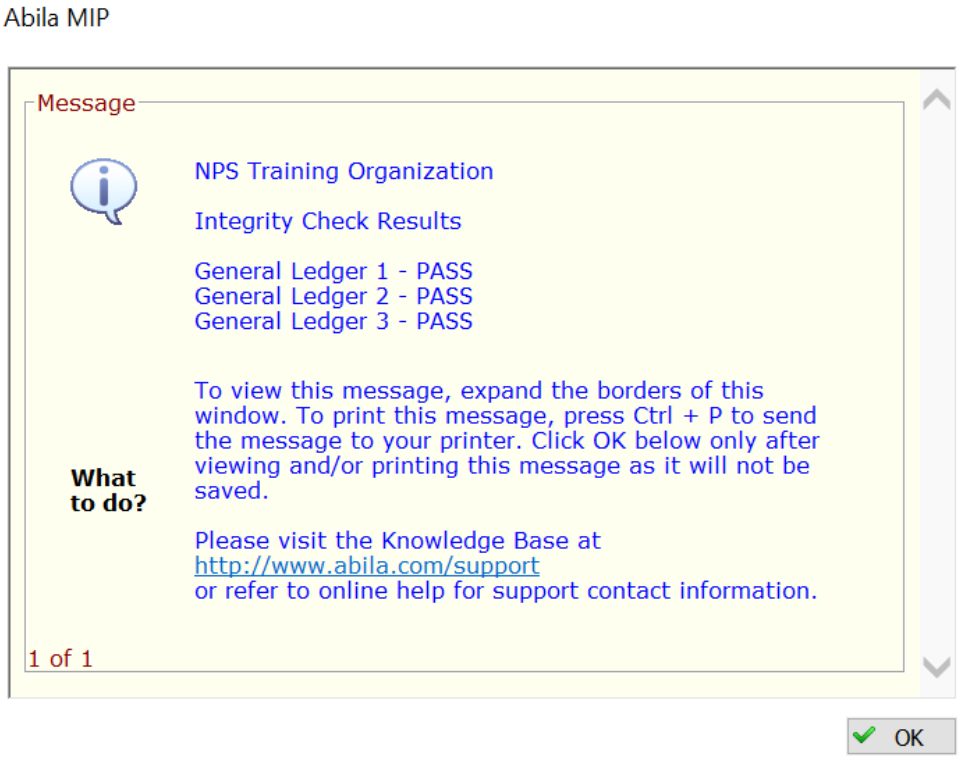
Select: Click the check box to select the test you want the system to perform. A check mark appears next to selected items.

Module: The system displays the module for which the corresponding test applies. Only installed modules appear in this column.

Description: The system displays the description (or name) of each test. For more information, see "Description of Individual Integrity Checks" (page 132).

Tips:

- Click Start to run integrity checks anytime you suspect that problems with your computer system may have damaged your data.
- Make sure that a network backup procedure does not interfere with running a data integrity check overnight. To ensure there is no interference with the process, run the checks on a workstation.
- Review the information displayed on the Data Integrity Checks Message screen.



Description of Individual Integrity Checks

The following lists the integrity checks by module, and offers you a detailed description about each test the system performs using Organization>Data Integrity Checks. You will only see checks for the modules you have installed and added to the current organization.

General Ledger

General Ledger Balance Records are in Balance: Each General Ledger balance record is first grouped according to its effective date and entry type. Then, the sum of credits and debits are compared. When credits equal debits, the test will PASS; otherwise, it will FAIL.

General Ledger Detail Records are in Balance: Each General Ledger detail record is first grouped according to its Effective Date and Entry Type. Then, the current amount field will be totaled. If the total is equal to zero the test will PASS. Otherwise, it will FAIL.

General Ledger Balance Records have Corresponding Detail Records: Each General Ledger balance record is first grouped according to its Effective Date, Entry Type (limited to Normal "N" and Adjust Opening Balance "AO" types), and Account Code. Then, the current amount field will be totaled. All matching detail records will be grouped and compared to each balance record. If the total of the current amount fields net to zero, and the Account Codes are identical, the test will PASS; otherwise, it will FAIL.

General Ledger Detail Records have Corresponding Balance Records: Each General Ledger detail record is first grouped according to its Effective Date, Entry Type (excluding any System Opening "SO" types), and Account Code. All matching balance records will be grouped in the same way and compared to each detail record. The Account Codes must be identical for the test to PASS; otherwise, it will FAIL.

General Ledger Detail and Balance Record Amounts Agree: Each General Ledger balance record is first grouped according to its Effective Date, Entry Type (excluding any System Opening "SO" types), and Account Code. Then, credit and debit amounts are totaled. All matching detail records will be grouped and the current amount is totaled. The total of the detail record's current amount must equal the balance record's net of credits and debits for the test to PASS; otherwise, it will FAIL.

Fund and Balancing Segment Balance Records are in Balance: Each Fund and Balancing Segment Balance record is first grouped according to its Effective Date, Entry Type, and Account Code. Then, the sum of credits and debits are compared. If credits equal debits, the test will PASS; otherwise, it will FAIL.

Fund and Balancing Segment Detail Records are in Balance: Each Fund and Balancing Segment detail record is first grouped according to its Effective Date, Entry Type and Account Code. Then, the current amount field will be totaled. If the current amount field equals zero, the test will PASS; otherwise, it will FAIL.

Check All Segment Detail Records for Blank Account Codes: Each General Ledger, Fund, and Balancing Segment detail record must have a valid Account Code. If the Account Code exists for all detail records, the test will PASS; otherwise; it will FAIL.

Check All Segment Balance Records for Blank Account Codes: Each General Ledger, Fund, and Balancing Segment balance record must have a valid Account Code. If an Account Code exists for all balance records, the test will PASS; otherwise, it will FAIL.

Check Non-Balancing Segment Revenue and Expense Detail Records for Blank Account Codes: Each Non-Balancing Segment revenue and expense detail record must have a valid Account Code. If an Account Code exists for all Non-Balancing detail records, the test will PASS; otherwise, it will FAIL.

Check Non-Balancing Segment Revenue and Expense Balance Records for Blank Account Codes: Each Non-Balancing Segment revenue and expense balance record must have a valid Account Code. If an Account Code exists for all Non-Balancing balance records, the test will PASS; otherwise, it will FAIL.

Check Restrictions Segment Revenue, Expense, and Equity Detail Records for Blank Account Codes: Each Restricted Segment revenue, expense, and net equity/asset detail record must have a valid Account Code. If an Account Code exists for all restricted detail records, the test will PASS; otherwise, it will FAIL.

Check Restrictions Segment Revenue, Expense, and Equity Balance Records for Blank Account Codes: Each Restricted Segment revenue, expense, and net equity/asset balance record must have a valid Account Code. If an Account Code exists for all restricted balance records, the test will PASS; otherwise; it will FAIL.

All Document ID Records must have Supporting Detail Records: Each Document ID record must have a supporting record of detail. If a detail record exists for each document ID found, the test will PASS; otherwise, it will FAIL.

All Detail Records must have Supporting Document ID Numbers: Each detail record must have a supporting Document ID number. If a document ID exists for each detail record found, the test will PASS; otherwise, it will FAIL.

Detail Transaction Totals are in Balance by Document and Session Records: The amount of each credit detail record must equal the amount of the debit detail record for the same Document and Session. If the total amounts are in balance, the test will PASS; otherwise, it will FAIL.

Accounts Payable

Accounts Payable Records Reconcile to General Ledger Balance Records: Each Accounts Payable record in the General Ledger balance table should have a reconciling record in the Accounts Payable transactions table (excluding all System Opening "SO" records). If the total of

Accounts Payable records in the General Ledger equal the sum of those in the Accounts Payable, the test will PASS; otherwise, it will FAIL.

Accounts Payable Transaction Records have a Supporting Document Record: Each Accounts Payable transaction record should have a matching record in the Accounts Payable open document. If matching Accounts Payable document IDs are found in the Accounts Payable open document table, the test will PASS; otherwise, it will FAIL.

Accounts Payable Transaction Record Amounts Reconcile to Document Record Amounts: The amount of the Accounts Payable transaction records (grouped by document ID, document number, and vendor) should be equal to the current amount of the Accounts Payable open document record. If the total of the transactions records are equal to the current amount of the open document record (excluding zero balances), the test will PASS; otherwise, it will FAIL.

Detail Records Reconcile to Accounts Payable Transaction Record Amounts: The sum of the Accounts Payable detail records (grouped by detail document number and vendor) should be equal to the sum of the Accounts Payable open document records. If the total of the detail records are equal to the current amount of the open document record, the test will PASS; otherwise, it will FAIL.

Open Accounts Payable Beginning and Ending Dates Match Dates in Detail Records: The beginning and ending dates of the Accounts Payable open document records (grouped by document ID, document number, and vendor) should match the beginning and ending dates of the similarly grouped detail records. If beginning and ending dates match, the test will PASS; otherwise, it will FAIL.

Open Accounts Payable Records Match Document Detail Records: The document ID of the Accounts Payable open document records (grouped by document ID, document number, document date, and vendor) should match the detail document ID in the detail records. If they match, the test will PASS; otherwise it will FAIL.

Check All Segment Open Accounts Payable Transactions Records for Blank Account Codes: Each General Ledger, Fund, and Balancing Segment in the Accounts Payable open transaction table must have a valid Account Code. If an Account Code exists for all open transactions records, the test will PASS; otherwise, it will FAIL.

Check Non-Balancing Segment Revenue and Expense Open A/P Transactions Records for Blank Account Codes: Each Non-Balancing Segment Revenue and Expense record in the Accounts Payable open transaction table must have a valid Account Code. If an Account Code exists for all open transactions records, the test will PASS; otherwise, it will FAIL.

Check Restrictions Segment Revenue, Expense, and Equity Open A/P Transactions Records for Blank Account Codes: Each Restrictions Segment Revenue, Expense, and Net Equity/Asset record in the Accounts Payable open transaction table must have a valid Account Code. If an Account Code exists for all open transactions records, the test will PASS; otherwise, it will FAIL.

Accounts Receivable

Accounts Receivable Records Reconcile to General Ledger Balance Records: Each Accounts Receivable record in the General Ledger balance table should have a reconciling record in the Accounts Receivable transactions table (excluding all System Opening "SO" records). If the total of Accounts Receivable records in the General Ledger equal the sum of those in the Accounts Receivable, the test will PASS; otherwise, it will FAIL.

Accounts Receivable Transaction Records have a Supporting Document Record: Each Accounts Receivable transaction record should have a matching record in the Accounts Receivable open document. If matching Accounts Receivable document IDs are found in the Accounts Receivable open document table, the test will PASS; otherwise, it will FAIL.

Accounts Receivable Transaction Record Amounts Reconcile to Document Record Amounts: The amount of the Accounts Receivable transaction records (grouped by document ID, document number, and vendor) should be equal to the current amount of the Accounts Receivable open document record. If the total of the transactions records are equal to the current amount of the open document records (excluding zero balances), the test will PASS; otherwise, it will FAIL.

Detail Records Reconcile to Accounts Receivable Transaction Record Amounts: The sum of the Accounts Receivable detail records (grouped by detail document number and vendor) should be equal to the sum of the Accounts Receivable open document records. If the total of the detail records are equal to the current amount of the open document record, the test will PASS; otherwise, it will FAIL.

Open Accounts Receivable Beginning and Ending Dates Match Dates in Detail Records: The beginning and ending dates of the Accounts Receivable open document records (grouped by document ID, document number, and vendor) should match the beginning and ending dates of similarly grouped detail records. If beginning and ending dates match, the test will PASS; otherwise, it will FAIL.

Open Accounts Receivable Records Match Document Detail Records: The document ID of the Accounts Receivable open document records (grouped by document ID, document number, document date, and vendor) should match the detail document ID in the detail records. If the

document ID of the open Accounts Receivable record matches the detail record document ID, the test will PASS; otherwise, it will FAIL.

Check All Segment Open Accounts Receivable Transactions Records for Blank Account Codes: Each General Ledger, Fund, and Balancing Segment in the Accounts Receivable open transaction table must have a valid Account Code. If an Account Code exists for all open transactions records, the test will PASS; otherwise, it will FAIL.

Check Non-Balancing Segment Revenue and Expense Open A/R Transactions Records for Blank Account Codes: Each Non-Balancing Segment Revenue and Expense record in the Accounts Receivable open transaction table must have a valid Account Code. If the Account Code exists for all open transactions records, the test will PASS; otherwise, it will FAIL.

Check Restrictions Segment Revenue, Expense, and Equity Open A/R Transactions Records for Blank Account Codes: Each Restrictions Segment Revenue, Expense, and Net Equity/Asset record in the Accounts Receivable open transaction table must have a valid Account Code. If the Account Code exists for all open transactions records, the test will PASS; it will FAIL.

Budget

Budget Records Reconcile to General Ledger Balance Records: Each Budget record in the General Ledger balance table should have a reconciling record in the Budget transactions table (excluding all System Opening "SO" records). If the total of Budget records in the General Ledger equal the sum of those in the Budget, the test will PASS; otherwise, it will FAIL.

Budget Records Match Document Detail Records: The document ID of the Budget document records (grouped by control ID, document number, and document date) should match the detail document ID in the transaction records. If the control ID of the Budget document record matches the transaction record document ID, the test will PASS; otherwise, it will FAIL.

Encumbrance

Encumbrance Records Reconcile to General Ledger Balance Records: Each Encumbrance record in the General Ledger balance table should have a reconciling record in the Encumbrance transactions table (excluding all System Opening "SO" records). If the total Encumbrance record amounts in the General Ledger equal the sum of those in the Encumbrance transactions table, the test will PASS; otherwise, it will FAIL.

Encumbrance Transaction Records have a Supporting Document Record: Each Encumbrance transaction record should have a matching record in the Encumbrance open document. If

matching Encumbrance document ID records are found in the Encumbrance open document table, the test will PASS; otherwise, it will FAIL.

Encumbrance Transaction Record Amounts Reconcile to Document Record Amounts: The amount of the Encumbrance transaction records (grouped by document ID, document number, and vendor) should be equal to the current amount of the Encumbrance open document record. If the total of the transactions records are equal to the current amount of the open document record (excluding zero balances), the test will PASS; otherwise, it will FAIL.

Open Encumbrance Beginning and Ending Dates Match Dates in Detail Records: The beginning and ending dates of the Encumbrance open document records (grouped by document ID, document number, and vendor) should match the beginning and ending dates of the similarly grouped detail records. If beginning and ending dates match, the test will PASS; otherwise, it will FAIL.

Detail and Encumbrance Transaction Records Reconcile to Open Encumbrance Record Amounts: The sum of the Encumbrance transaction records (grouped by detail document number and vendor) and the Encumbrance detail records should be equal to the sum of the Encumbrance open document records (to include liquidations processed through Accounts Payable). If the total of the transaction records plus the detail records are equal to the amount of the open document record, the test will PASS; otherwise, it will FAIL.

Open Encumbrance Records Match Document Detail Records: The document ID of the Encumbrance open document records (grouped by document ID, document number, document date, and vendor) should match the detail document ID in the detail records. If the document ID of the open Encumbrance record matches the detail record document ID, the test will PASS; otherwise, it will FAIL.

System

Check TblOrgDataDictionary for Multiple OR Records: The system verifies that only one OR record is located in the tblOrgDataDictionary. If multiple records are found, a message will display directing you to seek assistance in removing the superfluous record. If only one OR record is located in the tblOrgDataDictionary, the test will PASS; otherwise, it will FAIL.

Chapter 11: System Activity

Manage Concurrent Users

Access this form with Administrative user rights using System>Manage Concurrent Users.

Use this form to view and print a list of users currently logged on to the system.

Your system is licensed for a specific number of concurrent users per system also called "seats." Each time a user logs on to the system, a record is entered into the Manage Concurrent Users list. Occupied seats are counted by User ID and Workstation. Each unique combination of User ID and Workstation counts as one seat. When the number of occupied seats equals the total for which you are licensed, access to the system is denied until a seat becomes available. When a user logs off the system, the record is deleted from the search list and that seat is once again available.

Fields

Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Available Items Table: Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading.

- **Records per Page:** Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The

- default setting for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.
- **Submit Time:** This column displays the date and time that the user logged on to the system.
- **User ID:** This column displays the user currently logged on to the system (Security>Maintain Users).
- **User Type:** This column displays the type of user currently logged on to the system—Regular or EV User. EV User is only an option if the Executive View User module is installed.
- **Workstation:** This column displays the computer name for the workstation on which the user is working.
- **Activity:** This column displays "MIP Fund Accounting" if the user is currently logged on to the MIP Accounting system.

Tips:

- When filtering data, select Operators to determine which data to display. Also, view a list of Filter Examples that are useful throughout the system and examples of How to Use Wildcards characters with Like and Not Like.
- In the Available Items table, you can sort the data based on any column. Simply double-click on a column heading to sort according to that column.
- The sorting functionality is only for table display and does not affect printing. Print uses the data from the database and is therefore not reflective of how the items were sorted.
- When users exit the system incorrectly, sometimes they create an "unoccupied licensed seat"; that is, they are logged as active even though they are no longer using the system. For example, if a user reboots their machine (due to power failure or system lockup) while the system is running, you can have an unoccupied licensed seat on your system. When you delete the user from this form, it frees up their licensed seat for another user.
- To find out how many concurrent users are allowed, open the System>Activate License form. The number listed for "Concurrent Users" is the number of users allowed in the system at one time.
- When setting up security for users (Security>Set Up Organization Menus), we recommend you limit access to this form to include only system administrator-type users.
- For larger organizations with many records, you may want to clear the "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it eliminates the time it takes to load this form.
- To remove users who are logged as active (even though they are no longer using the system); simply highlight the line, and click Delete . This frees up those licensed seats for other users.

Manage Services

Access this form with Administrative user rights using System>Manage Services.

Use this form to manage the REST API services to see what services are active for MIP Advance and other third party services. If a task requires exclusive access, click the Set Maintenance Mode button, to turn the organization and/or system database offline.

You typically need exclusive system access when running data integrity checks, creating user defined fields, consolidating transaction history, and closing the fiscal year.

Fields

Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Service Table: Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading.

- **Records per Page:** Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The default setting for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.
- **Workstation:** This column displays the computer name for the workstation on which the user is working.
- **State:** This column displays "MIP Fund Accounting" if the user is currently logged on to the MIP Accounting system.
- **Issued By:** This column displays the user currently logged on to the system (Security>Maintain Users).
- **Issued Date:** This column displays the date and time that the user logged on to the system.

Set Maintenance Mode

Access this form with Administrative user rights using System>Manage Services> Set Maintenance Mode Button.

Use this form to manage the REST API services to grant exclusive access for maintenance or when running data integrity checks, creating user defined fields, consolidating transaction history, and closing the fiscal year; click the Set Maintenance Mode button, to turn the organization and/or system database offline.These processes require exclusive access and once complete, simply clear the check box to place the databases back online; allowing access to users, REST API services, and Third-Party services.

Fields

Set Organization Database Offline: Check the box to take the organization database offline, in order to run data integrity checks, add user defined fields, consolidate transaction history, or perform some task that requires exclusive access. When complete, you will need to clear this check box in order to place the database back online.

Set System Database Offline: Check the box to take the system database offline, in order to run data integrity checks, add user defined fields, consolidate transaction history, or perform some task that requires exclusive access. When complete, you will need to clear this check box in order to place the database back online.

Current Activity

Access this form with Administrative user rights using System>Current Activity.

Use this form to view and/or print a log of current system activity.

Whenever users are in the system, records are written to the current activity log indicating the program or table is in use so that write conflicts do not occur. When the user changes activities, the activity log changes accordingly. You can look at the current activity and see which users are currently in the system and what jobs they are doing.

Fields

Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria. Your choices for filtering items are: Submit Time, User ID, Workstation, Activity, and Database Name.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Available Items Table: Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading.

- **Records per Page:** Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The default setting for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.
- **Submit Time:** The date and time the current activity started.
- **User ID:** The user currently in the system.
- **Workstation:** The computer name for the workstation on which the user is working. If your computer is not on a network, the system displays "Default."
- **Activity:** The description of the activity currently occurring.
- **Database Name:** The name of the database in which the activity is being performed, such as System or NTO.

Tips:

- When filtering data, select Operators to determine which data to display. Also, view a list of Filter Examples that are useful throughout the system and examples of How to Use Wildcards characters with Like and Not Like.
- In the Available Items table, you can sort the data based on any column. Simply double-click on a column heading to sort according to that column.
- The sorting functionality is only for table display and does not affect printing. Print uses the data from the database and is therefore not reflective of how the items were sorted.
- Before backing up your database, use this form to determine whether someone is using the system.
- When setting up security for users (Security>Set Up Organization Menus), we recommend limiting access to this form to include only system administrator-type users.
- For larger organizations with many records, you may want to clear "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it eliminates the time it takes to load this form.

System Menu Buttons

	Select All: Use this button to select all items in the table.
	Deselect All: Use this button to clear all items in the table.
	Delete: Use this button to delete the selected items from the data.
	Display/Hide Filter: Use this button to display or hide the Filters group box.
	Clear Filter: Use this button to clear all of the selected filter items. The filter is used for display purposes only; it limits what the system displays in the table. You cannot save the filter items.
	Display Records: Use this button to display only the records that match the currently selected filter items. If you are not using the filter (it is blank), the Display Records button displays all of the items you currently have.

	View First Page: Use this button to display the first page of data in the table.
	View Previous Page: Use this button to display the previous page of data in the table.
	View Next Page: Use this button to display the next page of data in the table.
	View Last Page: Use this button to display the last page of data in the table.
	Print Setup: Use this button to select a printer and set up default printer information for printing your list.
	Print to Screen: Use this button to view your list before it is formatted for printing. This makes your data easy to review, but does not provide an exact representation of how it looks when sent to the printer.
	Print Preview: Use this button to view your list as it actually prints.
	Print: Use this button to print the items in the list.
	Export: Use this button to export data to one of several popular file formats. This button is available only if the Data Import/Export module is installed.

System Preferences

Access this form with Administrative user rights using Options>System Preferences.

Use this form to set up system-wide preferences for Administration, General Ledger, and all modules that are installed. You can choose to:

- Allow a user to log on to more than one Workstation at a time
- Use "Windows Authentication" (page 148) to maintain security when accessing MIP Accounting by using a Windows network user name and password
- Set a Minimum Password Character Length (Security>Maintain Users)
- Select how often a password should be reset
- Enter a default From email address for Alerts

Nonprofit Online Users

You cannot make any changes to your system preferences; it is for viewing purposes only. Also note that Windows Authentication is automatically enabled and required with the Private Cloud environment; therefore, the Use Windows Authentication check box is not available. See Nonprofit Online.

Fields

Allow User to Log On to more than One Workstation at a Time: Clear this check box if you do *not* want a user to log on to more than one workstation at a time. (By default this option is selected.) This is a convenient feature when you have personnel who need to log on to a different workstation without logging off their own workstation.

Use Windows Authentication: Select this check box to maintain security but eliminate the hassle of administering multiple passwords by granting access to MIP Accounting through each user's network user name and password. Windows Authentication is only available when connected to a network with Windows Active Directory. Existing users in the system are no longer valid when this check box is selected, with the exception of User "Admin."

If the Use Windows Authentication check box is cleared, the Windows network user names remain valid; however, all user passwords are set to A6i1a_MIP (capital A, number six, lower-case i, number one, lower-case a, underscore, all caps MIP).

Password

- **Minimum Password Character Length:** Set a minimum length for the password. Passwords must be a minimum of 8 characters.
- **Days Before Passwords Expire:** Set the number of days before the user's password expires. Minimum value is 1 and maximum value is 365. If a user does not change their password before it expires, they will be required to reset their password at next login.

Note: If the ***Use Windows Authentication*** check box is selected, the password features will not be available.

Password requirements:

- Include at least one uppercase and one lowercase letter
- Include at least one number

- Cannot contain spaces at the beginning or end
- Cannot be one of the last 6 passwords used

Alert Defaults

- **Email From Address:** Enter an email address that can be used system-wide for all alert messages. By keeping a consistent From address your email recipients will recognize and identify where the email is coming from and will more likely NOT mark the email as spam; which is important to ensure the delivery and receipt of the notification. It is recommended that you create a generic email address, related to the purpose of your alert email, but use something the receiver will recognize and know it is a trusted source. Note that the system is limited to one From email address. Some examples include: "alert@yourorganization.org", "MIPalert@yourdomain.gov", and "yourorganizationALERT@yourdomain.com"

Important! If the Use Custom Credentials check box was selected and a User name was entered on the Organization>Organization Information>Email Setup tab, the “From” email address here must match the User name, in order to use the selected Process Type’s format.
You cannot use a User name with someone else's email address when the Use Custom Credentials check box is selected.

Tips:

- The preferences specified here apply to *all* organizations and users in this system.
- Access to this form should be limited to only those system administrator-type users (Security>Set Up Organization Menus).

Windows Authentication

Windows Authentication allows a user to log on to MIP Accounting using their existing Windows network user account.

Nonprofit Online Users

Windows Authentication is automatically enabled and required with the Private Cloud environment; therefore, the Use Windows Authentication check box is not available. See Nonprofit Online.

Once you elect to use Windows Authentication, you can:

- Have single log on capabilities which allow you to log on to the workstation using a Windows network user name and password, then have access to the MIP Accounting system without having to log on again
- Open MIP Accounting using the default Organization database or the last database logged on
- Use File>Open Organization to access other Organization databases or log on using a different Windows user name and password
- Import and use Windows network user names and passwords for MIP Accounting users
- Import Windows users individually or by group into the MIP Accounting system. It is important to set up your Executive View users in Windows and import them into the system.

Note: If the Use Windows Authentication check box is cleared (on the System Preferences form), the Windows network user names remain valid; however, all user passwords are set to A6i1a_MIP (capital A, number six, lower-case i, number one, lower-case a, underscore, all caps MIP), with the exception of User "Admin."

Chapter 12: Table Structure

Default Table Structure

Access this form with Administrative user rights using Organization>Default Table Structure.

Use this form to view all fields in the system. You may want to look in the system to determine all acceptable values for each field.

Fields

Filters: The filter is for display purposes only; it simply allows you to limit which items are displayed in the Available Items table.

- **Available Filter, Selected Filter:** Select an item in the Available Filter column, and click the Mover (>) to move it to the Selected Filter column. Once an item is in the Selected Filter column, set up its filtering criteria. Then, the table is limited to the data that falls within the designated filter criteria. Your choices for filtering items are: Table Name, Field Name, and Module.
- **Compares To:** Select an operator from the drop-down list. The operator compares the value in the Selected Filter column with the values in Criteria 1 and Criteria 2 to determine which items are displayed in the Available Items table.
- **Criteria 1:** Enter a value to compare with the item in the Selected Filter column. When using Like or Not Like, you can use "%" to represent any number of characters.
- **Criteria 2:** Enter a value for the end of a range if the Compares To column contains the Between or Not Between operators.

Available Items Table: Records are initially sorted on the first data column in ascending order. However, records can be sorted based on any column by clicking on the column heading.

- **Records per Page:** Select how many items per page to display using the Records per Page drop-down list. You can view items in the table in increments of 10, 25, 50, 100, 250, 500, or 1000. The default setting for the Records per Page drop-down list was selected using the Options>Customize Workstation Settings>Preferences tab.
- **Table Name:** The table where the field information is stored.

- **Field Name:** The field name identified by the system. Most of these field names correspond to a field name on a form. All field names begin with common letters that identify a field's function.

Field Identified	Field Type	Example
dtm	date	dtmDocDate
s	string	Description
d	double	dDocID
cur	currency	curAmount
guid	number	guidUserIDf
n	integer	nOrderID
ysn	yes/no	ysnSuta

- **Field Description:** A description of the designated field. Often the description also contains acceptable values for the field.
- **Field Size:** This is the default size assigned by the system. Some fields are user defined; therefore, this field size may have changed.
- **Module:** The system displays the module associated with the designated field. The available modules are as follows (depending on which ones are installed):

AB	Accounts Receivable Billing
AM	Allocations Management
AP	Accounts Payable
AR	Accounts Receivable Reporting
AS	Advanced Security
BG	Budget
BK	Bank Reconciliation
DD	Direct Deposit

EN	Encumbrances
EP	Electronic Funds Transfer for A/P
FA	Fixed Assets
FD	Forms Designer
GA	Grant Administration
GL	General Ledger
MC	Multicurrency
OE	Order Entry
PO	Purchase Orders
PR	Payroll
RQ	Electronic Requisitions
SY	Administration

Tips:

- When filtering data, select Operators to determine which data to display. Also, view a list of Filter Examples that are useful throughout the system and examples of How to Use Wildcards characters with Like and Not Like.
- In the Available Items table, you can sort the data based on any column. Simply double-click on a column heading to sort according to that column.
- The sorting functionality is only for table display and does not affect printing. Print uses the data from the database and is therefore not reflective of how the items were sorted.
- This is a very lengthy table; therefore, you might want to filter by module, then print the data.
- To see a table which defines user defined field lengths and identifies default values (if any) for fields that are importable (such as chart of accounts, offset account assignments, vendors, and charge codes.), you can review the documentation for the File>Import form.
- The field size displayed in this table is the default size assigned by the system. Some fields are user defined; therefore, adjustments may have been made to the field lengths when the current organization was created (File>New Organization).
- For larger organizations with many records, you may want to clear the "Use Drop-Down List on Find Forms" using the Options>Customize Workstation Settings>Preferences tab. By doing so, it eliminates the time it takes to load this form.

Default Table Structure Buttons

	Display/Hide Filter: Use this button to display or hide the Filters group box.
	Clear Filter: Use this button to clear all of the selected filter items. The filter is used for display purposes only; it limits what the system displays in the table. You cannot save the filter items.
	Display Records: Use this button to display only the records that match the currently selected filter items. If you are not using the filter (it is blank), the Display Records button displays all of the items you currently have.
	View First Page: Use this button to display the first page of data in the table.

	View Previous Page: Use this button to display the previous page of data in the table.
	View Next Page: Use this button to display the next page of data in the table.
	View Last Page: Use this button to display the last page of data in the table.
	Print Setup: Use this button to select a printer and set up default printer information for printing your list.
	Print to Screen: Use this button to view your list before it is formatted for printing. This makes your data easy to review, but does not provide an exact representation of how it looks when sent to the printer.
	Print Preview: Use this button to view your list as it actually prints.
	Print: Use this button to print the items in the list.
	Export: Use this button to export data to one of several popular file formats. This button is available only if the Data Import/Export module is installed.

Chapter 13: History

Consolidate Transaction History

Access this form with Administrative user rights using Organization>Consolidate Transaction History. This requires exclusive access to the organization and system databases.

Use this form to consolidate the balance and detail data in your database. The consolidation process creates summary records from the detail records, and then the detail records are deleted from your database (thereby reducing the size of the database).

- The balance records are consolidated by fiscal year date, one year at a time. The summation periods available are fiscal month-end, fiscal quarter-end, or fiscal year-end.
- Typically, you can only run the consolidation process on a closed fiscal year. However, if you have imported or converted data that is dated prior to a closed fiscal year, the system consolidates those earlier years first, one year at a time, beginning with the oldest year. Then, it consolidates the closed fiscal years.

Note: In order to consolidate, there must be at least three times the current database of free space on the drive. We also STRONGLY URGE making a backup of the database prior to consolidation, using File>Backup. So if an error occurs during the consolidation process, you have a backup database.

After the consolidate transaction history process is complete, you may see some entries that were not consolidated. This happens when transactions with the same Matching Document IDs have dates that occur within two different fiscal years. This can occur in subledgers as well as other transactions. For example, this will happen if you have a prior year adjustment with another adjustment made to the opening balances in the current fiscal year, and both are processed with the same Document ID within the same session.

Fields

Fiscal Year: The system displays the oldest fiscal year (opened or closed) that has not been previously consolidated. This date range cannot be edited. (A fiscal year was assigned when this organization was created using File>New Organization.)

Method of Summation: Select the method to consolidate your data–Monthly, Quarterly, or Annually. Then, click Start to begin consolidating data.

Tips:

- The current fiscal year cannot be consolidated.
- Budget version is one of the criteria used when consolidating budget balances.
- The Document Number, Document Description, Transaction Description, or Session Description will be renamed if they exceed the user defined length for these fields. These lengths were defined when the organization was created (File>New Organization>Field Lengths panel).

Remove Payroll History

Access this form with Administrative user rights using Organization>Remove Payroll History.

Use this form to delete historical payroll data by calendar year. Through this process, leave balances are summarized and rolled into the next calendar year as an Adjustment.

After clicking Start, the system displays a message asking if you have backed up the database.

- Click *Yes* to continue through the Remove Payroll process.
- Click *No* if you want to return to the desktop, so that you can back up the database (File>Backup).

Note: As a best practice, you should periodically archive a full backup for historical purposes before deleting Payroll History.

Fields

Calendar Year: This is the calendar year that you would like to remove from the database. The system displays the first year available for deletion. It cannot be the current system date year or one year prior to that date.

Chapter 14: Administration Reporting

The system provides numerous report selections so you can create custom reports that satisfy the reporting needs in your organization. This reporting gives you the flexibility you need, from specifying which columns appear, to sorting and totaling the information presented. You control the output so you get just the reports you want.

Below is a list of all the reports available to you with Administrative user rights:

Report Menu Selections	Reports
Lists>	"Security List" (page 157)
	"User Information List" (page 161)
	"Group Information List" (page 162)
	"Account Level Security List" (page 163)
	"Advanced Organization Audit List" (page 165)
	"User Defined Fields List" (page 167)
	"UDF Default Sources List" (page 170)
	"Currency List" (page 171)

For an overview of the report tabs and buttons, refer to the "Report Setup" chapter of the *General Ledger Reports* guide.

Security List

Access this report with Administrative user rights using Reports>Lists>Security.

Use this report to obtain a list of users and their security rights. It lists all menu selections in which the user has rights.

- Users were created using Security>Maintain Users and they were granted security using the Security>Set Up Organization Menus and Set Up System Menus forms. Only the menu selections in which you gave them rights display in this report.

- In order to see a user's System Security rights on this report, the User ID must be associated with an organization on the Security>Maintain Users form.
- An organization has to be open to run this report.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.
- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
Type	"User" or "Group" displays here to identify whether it is a single user or a group of users.
Group ID	All groups created for the organization using the Security>Maintain Groups form, such as Management.
Group Name	The name assigned to the groups, such as Program Services Department.
User ID	All users created for the organization using the Security>Maintain Users form, such as JoeG.
User Name	The name assigned to the user, such as Joe Green.
Application	The systems in which the user has rights—Accounting (ACCT), Administration (ADMIN), Payroll, and/or Electronic Requisitions (REQ).
Module	The modules in which the user has rights. They could include any or all of the following modules. AB (Accounts Receivable Billing) AM (Allocations Management)

Column	Description
	AP (Accounts Payable) AR (Accounts Receivable Reporting) AS (Advanced Security) BG (Budget) BK (Bank Reconciliation) CC (Data Consolidation Client) DD (Direct Deposit) EN (Encumbrances) EP (Electronic Funds Transfer for A/P) EV (Executive View) FA (Fixed Assets) FD (Forms Designer) GA (Grant Administration) GL (General Ledger) GR (GASB Reporting) IE (Import/Export) MC (Multicurrency) NS (Scheduler) OE (Order Entry) PO (Purchase Orders) PR (Payroll) RQ (Electronic Requisitions) SY (Administration)

Column	Description
Menu	The menus and form names in which the user has rights, such as File – Print Setup and Maintain – Chart of Accounts.
View	If the user has rights to open and view records on the associated form, the system displays "Yes." Alternatively, if the user does not have rights, or if that particular right is not available for that form, the system displays "No."
Edit	If the user has rights to make changes to records on the associated form, the system displays "Yes." Alternatively, if the user does not have rights, the system displays "No."
Delete	If the user has rights to remove records on the associated form, the system displays "Yes." Alternatively, if the user does not have rights, the system displays "No."
Add	If the user has rights to enter new data on the associated form, the system displays "Yes." Alternatively, if the user does not have rights, the system displays "No."
Process	If the user has rights to perform a process on the associated form, the system displays "Yes." Alternatively, if the user does not have rights, the system displays "No."
Sensitive	If the user has rights to view fields that contain sensitive information on the associated form, the system displays "Yes." Alternatively, if the user does not have rights, the system displays "No."
Requisition User	A designation of Y (Yes) or N (No) depending on if the "Requisition User" option was selected for the user (Security>Maintain Users). This column is only available if the Electronic Requisitions module is installed.

Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Use this tab to change the font and page setup for a report.

Security Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

User Information List

Access this report with Administrative user rights using Reports>Lists>User Information.

Use this report to obtain a list of users and other data which was set up on the Security>Maintain Users form. An organization does *not* have to be open to run this report.

Scheduler Users

Please note that Scheduler is not available for any of the tabs in this report.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.
- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
User ID	All users IDs created in the system, such as JoeG.
User Name	The first, middle, and last name assigned to the user.
Email	The user's email address, such as joeg@ssa.com.
Status	The status of the user ID–Active or Inactive, depending on what you selected on the Security>Maintain Users form.
Organization	All organizations that are currently assigned to the user.
Modified By	The user ID that modified the current users' data last.
Date Modified	The date and time the users' data was last modified.

Column	Description
Executive View User	A designation of Yes or No depending on if the "Executive View User" option was selected for the user. This column is only available if the Executive View module is installed.
Requisition User	A designation of Yes or No depending on if the "Requisition User" option was selected for the user. This column is only available if the Electronic Requisitions module is installed.
HR Management User	A designation of Yes or No depending on if the "HR Management User" option was selected for the user. This column is only available if the Payroll and HR Management modules are installed.
User Identification Number	The user's unique identification number assigned in the system.

Filter Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Layout Use this tab to change the font and page setup for a report.

Security Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

Group Information List

Access this report with Administrative user rights using Reports>Lists>Group Information.

Use this report to obtain a list of groups and other data which was set up using the Security>Set Up Organization Menus form. An organization has to be open to run this report.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.

- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
Group ID	All groups created for the active organization (Security>Maintain Groups).
Group Name	The name assigned to the group.
Date Modified	The date and time the group was last modified.
Modified By	The user ID that last modified the group.
User ID	All user IDs that are part of the group.
User Identification Number	The user's unique identification number assigned in the system.

Filter Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Layout Use this tab to change the font and page setup for a report.

Security Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

Account Level Security List

Access this report with Administrative user rights using Reports>Lists>Account Level Security. It is only available if the Account Level Security module is installed.

As the Administrator, use this report to print a list of users and groups and their account level security settings. Account level security was set up and activated using the Security>Set Up Account Level Segments and Set Up Account Level Security forms.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.
- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
Type	"User" or "Group" displays here to identify the type. The type was decided when the user or group was assigned account level security.
Group ID	All groups that have account level security assigned.
Group Name	The name assigned to the group IDs (Security>Maintain Groups), such as Program Services Department.
User ID	All users that have account level security assigned.
User Name	The name assigned to the user ID (Security>Maintain Users), such as Joe Green.
Enable Account Level Security	"Yes" or blank depending on if the user's security settings include the Enable Account Level Security check box. The check box is not available for Groups; therefore, it is always blank.
Segment Sequence	The number that designates the order of your segments. The segment sequence can be changed by the Administrator using the Organization> Organization Information>Segments tab. The report shows each segment's sequence number.
Segment Name	The segments that have account level security assigned, such as Fund or GL.
Account Code	The account code, such as 201, 05, 45001, or blank.
Account Title	The account title, such as Housing or Service Fees.
Account Short Title	The Account Short Title, usually the first 15 characters of the Account Title, such as Housing or Svc Fees.

Column	Description
Account Status	The status of the segment–Active, Inactive, or Discontinued. The report prints A, I, or D.
Account Type	The account type (if using a GL segment) that was assigned account level security. Valid account types include the following: Cash, Accounts Receivable-Customers, Accounts Receivable, Pledges Receivable, Interfund Receivable, Fixed Assets, Other Assets, Accounts Payable-Vendor, Accounts Payable, Interfund Payable, Other Liabilities, Net Assets/Equity, Revenues, Expenses/Expenditure, Interfund Transfers, and 3rd Party Inventory. The report prints CSH, AR, ARO, PLO, IFR, FAO, OA, AP, APO, IFP, OL, NAE, REV, EXP, IFT, or INV.

Filter Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Layout Use this tab to change the font and page setup for a report.

Security Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

Advanced Organization Audit List

Access this report with Administrative user rights using Reports>Lists>Advanced Organization Audit. It is only available if the Account Level Security module is installed.

Use this report to print a list of changes that were made by the Administrator to the Organization's Security>Set Up Organization Menus, as well as, Maintain menu forms for the organization. This form provides detailed information regarding addition, modification, and deletion of records. You can see what information was added, what information was changed (both before and after), who made the change, when the change was made, and so forth.

Advanced Organization Audit Trail was set up and activated using the Security>Manage Audit Trails>Set Up Advanced Organization Audit form.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.
- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
Date	The date and time the activity was logged. The date is formatted as M/D/YYYY and the time is formatted as HH:MM:SS uppercase AM or PM.
Record ID	The identity of the record that was changed, such as, Customer, ABC or AAA.
Action	A code displays, indicating the type of action that occurred. There are three message types: *Add* (a new entry), *Edit* (change made to an existing record), and *Delete* (removal of an existing entry).
User ID	The user who performed the activity, such as, NPSUser.
Field Name	The name of the field where the change occurred, such as, Enable Audit or Shipping Phone.
Old Value	The data that was in the field before it was added or changed, such as, Disabled or (817) 555-2222 Ext. Note that a blank displays when a new entry is added or when an existing data field was intentionally left blank.
New Value	The data that was in the field after it was added or changed, such as, Enabled or (254) 555-2222. Note that a blank displays when an existing entry is deleted or when a new data field was intentionally left blank.
Associated Record ID	The secondary column associated to the Record ID that was changed, such as, <Billing> AAA (Shipping Address Code and

Column	Description
	Customer ID) or <PostOffice> S (Address Code and Address Code Type). Note that a blank field displays when there is no association for the Record ID.
Source	Where the activity was performed. For example, if the user logged into the system, one of the following displays: *Administration*, *Accounting*, or *Payroll*. If the information was imported into the system, *Import* displays. Also, if a user connected directly to the database on the SQL Server, *Other* displays.
Workstation ID	The name of the workstation used to perform the activity, such as, NPSSERVR.

Filter Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Layout Use this tab to change the font and page setup for a report.

Security Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

User Defined Fields List

Access this report with Administrative user rights using Reports>Lists>User Defined Fields.

Use this report to obtain a list of user defined fields that have been created. User defined fields were created by the Administrator using the Organization>Set Up User Defined Fields form. You can add data to these fields using the appropriate form in the MIP Accounting system.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.
- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
Type	A record type of A/R Invoices, A/R Invoices Detail, Charge Codes, Customers, Employees, {Segment Codes}, Purchase Orders, Transaction Documents, Transaction Lines, or Vendors.
Field Name	The internal field name that is used in the system, such as grantmanager.
Display Name	The name for the user defined field as it appears on the form in the system, such as Grant Manager.
Required	A designation of (Y) Yes or N (No) depending on whether the field is required.
Field Type	A field type of Currency, Date, Editable Drop-Down List, Non-Editable Drop-Down List, Number, String, or Yes/No.
Length	A field length between 1 and 255 if the field type is String, Non-Editable Drop-down List, or Editable Drop-down List.
Number of Decimal Places	The number of decimal places for a Number field type.
Default Text	The default text for String or Editable Drop-Down List field types.
Default Yes/No	The default value for Yes/No field types.
Default Date	The default value for Date field types.
Default Currency	The default value for Currency field types. This value is formatted in the organization's functional currency. The functional currency was determined by the Administrator when the organization was created (File>New Organization>Functional Currency panel).
Default Number	The default value for Number field types.
Shared List Type	The shared list type—A/R Invoices, A/R Invoices Detail, Assets, Charge Codes, Customers, Employees, {Segment Codes},

Column	Description
	Purchase Orders, Transaction Documents, Transaction Lines, and Vendors—if the UDF uses one.
Shared List Field Name	All non-editable drop down list field names for the Shared List Type. This field is used in conjunction with the Set Up UDF Default Sources form.
Non-editable Code	The codes available for Non-Editable Drop-Down List field types.
Non-editable Description	The description for the associated code.
Non-editable Default	The default value for the associated code: Yes or No.
Non-editable Status	The status for the associated code: A-Active, I-Inactive, or D-Discontinued.
Transaction Source	The transaction sources associated with a Transaction Document or Transaction Line type user defined field, such as APC, API, APM, APS, ARB, ARC, ARM, ARP, ARS, BD, CD, CDS, CR, CRS, ENC, ENL, or JV.
Field ID	The BO Item ID that is used for Import. It is determined by a combination of the following fields: {type}:{an internal distinction}:{fieldname}
Date Last Modified	The date and time the field was last changed.
Modified By	The user who modified the field last.

Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Use this tab to change the font and page setup for a report.

Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

UDF Default Sources List

Access this report with Administrative user rights using Reports>Lists>UDF Default Sources.

Use this report to obtain a list of user defined fields with their default sources. User defined fields were created using Organization>Set Up User Defined Fields, while default sources were applied using Organization>Set Up UDF Default Sources.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.
- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
Type	A record type of A/R Invoices, A/R Invoice Detail, Transaction Documents, or Transaction Lines.
Field Name	The internal field name that is used in the system, such as grantmanager.
Display Name	The name for the user defined field as it appears on the form in the system, such as Grant Manager.
Field Type	A field type of Currency, Date, Editable Drop-Down List, Non-Editable Drop-Down List, Number, String, or Yes/No.
Assigned Transaction Sources	The transaction sources associated with this user defined field, such as APC, API, APM, APS, ARB, ARC, ARM, ARP, ARS, CD, CDS, CR, CRS, ENC, ENL, and/or JV.
Default Source Type	A record type of Vendors, Charge Codes, Customers, and Transaction Documents.
Default Source Field Name	The Default Source field name.

Column	Description
Default Source Transaction Source	Other transaction sources associated with the default source, such as APC, API, APM, APS, ARB, ARC, ARM, ARP, ARS, CD, CDS, CR, CRS, ENC, ENL, or JV.
Default Source Additional Transaction Source	The transaction sources associated with Default Source UDFs, such as ARB and ARS.

Filter Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Layout Use this tab to change the font and page setup for a report.

Security Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

Currency List

Access this report with Administrative user rights using Reports>Lists>Currency.

Use this report to print a list of currencies, which were set up using the Organization>Currency Setup form.

Report Criteria

Setup Use this tab to assign a report name and determine whether or not to include it on the actual report. The report name can be printed in the header or the footer of the report.

Content Use this tab to determine what data to include in the report and to define the report layout.

- By selecting Available Items, the data is divided onto separate pages. The report starts a new page for each item, and the item is printed in the page header of the report.
- By selecting Available Columns, the data that appears in the body of the report is determined.

Column	Description
Currency Code	The currency code, such as USD, CAD, EUR, GBP, or MXN or any custom currency code created.
Status	The status of the currency code–Active, Inactive, or Discontinued. The report prints A, I, or D.
Currency Description	The description associated with the currency code, such as US Dollar, Canadian Dollar, Euro, Pound Sterling, or Mexican Peso.
Symbol	The symbol associated with currency, such as $ or Mex$.
Positive Format	The positive format for the currency, such as $1 or Mex$1.
Decimal Symbol	The decimal symbol assigned to the currency, such as a period or comma.
Digits after the decimal	The number of digits designated after the decimal place.
Grouping Symbol	The grouping symbol assigned to the currency, such as a period or comma.
Negative Format	The negative format for the currency, such as ($1) or (Mex$1).
{Account Code}	The gain/loss accounts assigned to all currencies other than the functional currency. The report shows a segment code–01, 201, 11001, for example. The report prints one column for each segment, such as Fund Code or GL Code.

Use this tab to narrow down and more explicitly define the data to include in the report by selecting from the Available Filters.

Use this tab to change the font and page setup for a report.

Use this tab to secure the active report so that other users cannot save their changes to it. The user that selects the check box, and then saves the report, is the only user that can change or save it later. This check box cannot be cleared by any user other than the user that locked the report.

Index

A

account code combinations
  options 33
account level security
  audit 165
  organizations 64
  printing 163
  reporting on 163
  users 66
account segments
  defining properties 6
  renaming 17
  setting up security 64, 66
  unified chart of accounts 6
  viewing properties 17
activating account level security 64, 66
activating licenses 90
activation codes 90
Active Directory 148
activity
  current 143
  organization history 60
  organization maintenance history 80
  system audit 58
  system history 58
addresses
  organizations 15
administration
  account level security 64, 66
  activating licenses 90
  adding modules 93
  backing up databases 126
  changing passwords 47
  compressing databases 130
  consolidating transaction history 155
  creating new organizations 3
  current activity 143
  data integrity checks 130
  encryption 74
  managing concurrent users 139
  managing services 141
  opening organizations 2
  organization history 60
  organization information 13
  organization maintenance history 80
  organization preferences 33
  removing payroll history 156
  renaming users 46
  restoring databases 129

setting up alerts 115
setting up attachment categories 98
setting up attachment locations 97
setting up security 50, 53
setting up SMTP email 21
setting up user defined fields 100
setting up user groups 47
setting up users 42
summary organization audit 60
system audit 58
system history 58
system preferences 146
administration reports 157
Account Level Security List 163
Advanced Organization Audit List 165
Group Information List 162
Security List 157
User Defined Fields List 167
User Information List 161
advanced organization audit 80
reporting on 165
alerts
assigning groups 121
assigning users 121
configuring alerts 115
default email address 146
previewing messages 118
setting up alerts 115
system preferences 146
attachments
setting up categories 98
setting up locations 97
audit trail 58, 60, 80
advanced 80
advanced organization 80
printing 165
reporting on 165
setting up advanced 85
summary organization 60
system 58
auto-incrementing 36, 40-41

B

backing up databases 126

C

checking data 130
compress databases 130
concurrent users
licensed seats 90
managing 139
configure SMTP 31
consolidating data
transaction history 155
copying
account level security 68
organization security 56
system security 52

user groups 49
creating new organizations 3
creating user defined fields 100
currency
printing 171
reporting 171
current activity 143

D

data consolidation
transaction history 155
data history log 58, 60, 80
data integrity checks 130
databases
backing up 126
compression 130
consolidating transaction history 155
creating 3
encryption 74
integrity checks 130
licensed 90
opening 2
restoring 129
rights 50, 53
security 50, 53
setup options 13
default table structure 150

E

eFiling 20
electronic filing 20
electronic requisitions
setting up users 42
email 31
setting up users 42
emailing 21
enabling encryption 74
enabling FAS Asset Quick Entry 33
encryption 74
evaluation systems 91
executive view 42, 53

F

FAS Asset Accounting
setting up defaults 33
federal tax IDs 13
field lengths
adding modules 95
setting up organizations 11
viewing organizations 18
fiscal year ends 13
flow-thru 107, 109, 113-114
functional currency 4

G

grant management
assigning grants 125
granting security rights 50, 53
groups
account level security 66
copying account level security 68
copying users 49
printing 162
reporting on 162
setting up users 47

H

history
consolidating data 155
maintain forms 80
organization 60
system 58

I

integrity checks 130

L

licensed seats 90
logging on 2
logs
advanced organization audit 80
concurrent users 139
current activity 143
organization history 60
organization maintenance history 80
summary organization 60
system audit 58
system history 58

M

magnetic media 20
maintain
history log 80
modules
adding 93
assigned to organizations 18
licensed 90
owned 90
multicurrency reports
Currency List 171

N

new organizations 3

O

occupied seats 143
opening organizations 2
options
organization 33

system 146
organizations
account level security 64
account segments 17
adding modules 93
address 15
backing up 126
compression 130
consolidating transaction history 155
creating new 3
database integrity checks 130
database security 53
electronic filing 20
encryption 74
field lengths 18
history log 60
opening 2
preferences 33
restoring 129
setup advanced audit 85
setup options 13
summary audit 60
owned systems 90

P

passwords
changing 47
requiring 146
setting up users 42
preferences
organization 33
system 146
printed address 15-16
printing
account level security 163
audit 165
currency 171
group information 162
security information 157
user defined fields 167
user information 161
processing modes 33

R

registered organization 90
Remove Payroll History 156
removing unoccupied seats 139
reports 157
Account Level Security List 163
administration 157, 161-163, 165, 167
Advanced Organization Audit List 165
Currency List 171
Group Information List 162
Security List 157
User Defined Fields List 167
User Information List 161
requisitions
setting up users 42

Rest API 141
restoring databases 129
rights
  account level 66
  account level segments 64
  copying users 52, 56
  organization menus 53
  system menus 50
  users 50, 53

S

Scheduler
  setting up users 42
seats
  licensed 90
  occupied 143
  unoccupied 139
security
  account level segments 64
  adding modules 95
  advanced organization audit 80
  copying users 52, 56
  encryption 74
  organization databases 53, 57
  printing 157, 163
  reporting on 157, 163
  summary organization audit 60
  system databases 50, 57
  users 50, 53
segments
  account level security 64
  defining properties 6
  renaming 17
  unified chart of accounts 6
  viewing properties 17
serial numbers 90
services
  managing 141
setting up encryption 74
setting up SMTP 21
settings
  system preferences 146
SMTP
  configure Gmail 31
  configure Yahoo 31
system audit log 58
system databases
  backing up 126
  compressing 130
  restoring 129
  security 50
system history log 58
system preferences 146
system tables 150

T

table structure 150
tax identification numbers 13

testing data 130
third party 141
tracking
  audit trail 58, 60, 80
  concurrent users 139
  current activity 143
  organization history 60
  system history 58
transaction entry
  auto-incrementing IDs 40-41
  options 33
  warning dates 38
transferring
  assets to FAS Gov 33
troubleshooting data problems
  organization history 60
  system history 58

U

UCOA 6
UDF Default Sources 170
unified chart of accounts 6
unoccupied seats 139
user defined fields
  default sources 107, 170
  flow-thru 109, 113-114
  master records 100
  printing 167, 170
  reporting on 167
  setting up 100
  transaction sources 105
users
  adding 42
  concurrent 139
  copying account level security 68
  current activity 143
  grouping 47
  licensed seats 90
  maintaining 42
  organization history 60
  passwords 42, 47
  printing 161
  renaming 46
  reporting on 161
  rights 50, 53
  security 50, 53
  setting up 42
  system history 58

V

verifying data 130

W

Windows Authentication 148
Windows integration 148
windows security 148
workstations
  concurrent users 139

current activity 143
organization history 60
system history 58
system preferences 146

Y

year end fiscal 13