Infor Distribution FACTS
System Management User Guide

Release level 9.3.2

Important Notices

Trademark Acknowledgements

Publication Information

Release: Infor Distribution FACTS Release level 9.3.2

Publication date: December 1, 2020

Contents

About this guide

This guide describes workflow, concepts and procedures for using the Infor Distribution FACTS System Management module.

Intended audience

This guide is for FACTS end users, managers, in-house analysts, and trainers who require an understanding of the product and how to use it.

Organization

This table shows the chapters of the guide:

Section	Description
About this guide	Lists the intended audience as all users. Describe the purpose and the related documentation.
Overview	The overview section described the purpose of the application in terms of the business solutions that it provides, program listings, and menu trees, as applicable to the application.
Work Flows & Program Concepts	This section includes process flows for each module, program descriptions and concepts that are key to using this FACTS module.
Transaction Procedures	This section contains daily, weekly and end of year procedures as well as step-by-step processing information for entry, inquiry and transaction programs.

Related documents

You can find the documents in the product documentation section of the Infor Support Portal, as described in "Contacting Infor" on page 8.

Refer to the contents of the FACTS Version 9.3 & Incrementals folder located at https://support.infor.com/. Click Search>Browse Documentation>FACTS> Version 9.3 & Incrementals to view a document tree like this.

- *FACTS Version 9.3 & Incrementals*
  - *Installation and Administration Guides*
    - *Configuration Guides*
    - *Demo Application Installation Guide*
    - *Hardware Guide*
    - *Installation Guide*
    - *Online Help Installation Instructions*
    - *Product Compatibility Matrix*
    - *Technical Information*
  - *Integrations*
    - *Credit Card*
    - *Document Management*
    - *Infor Solutions*
      - *eCommerce*
      - *Storefront Integration Layer*
    - *WMS*
  - *Release Information*
    - *Feature Demonstration Videos*
    - *Program Menu Changes*
    - *Release notes*
      - *Incremental Release Notes*
  - *User Guides*
    - *Feature Implementation Guides*
    - *Standard Module User Guides*

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1 Overview

The System Management module is the backbone of all modules in the Infor Distribution FACTS system. It will accommodate hundreds of companies maintaining accurate file information and providing complete audit trails. This allows users the secure feeling that all information is traceable throughout the system. Instructional prompts, default values and the capability to back up to previous inputs promote both user efficiency and comfort in using the system.

Many of the programs in the main System Management module are advanced level programs and should not be accessed or changed by unauthorized users. This is especially true of System Management file maintenance programs.

These submenus are located on the System Management menu.

Banking System

Menu Setup

Security System

System Dashboards Menu

Infor OS Menu

Messages

Inquiries

Reports & Prints

End-of-Period Checklist

File Maintenances

The system supports up to 980 terminals. For each terminal on the system, the user may set a default branch, warehouse, department, salesperson and printer. This relieves the user of having to enter the correct information at these important inputs. The system will automatically insert the correct information where necessary as set by the user. All reports throughout FACTS may be printed to a terminal. You can set a hex code per terminal to print 132 columns of information (if applicable and within the range of the terminal) when printing to the terminal. Hot keys can also be defined to each terminal.

The system supports up to 99 printers. For each printer the user may set the compressed and standard print hex codes (as applicable based on the printer). At any time during processing, the print size may be set by the user through the Set Standard/Compressed

Print program. Each program in the system may also be set to a default printer by terminal. For example, when printing work orders from certain terminals, the system may automatically print the work orders on the warehouse printer.

System Security: Tracking Who Logs In

The FACTS Security System is built into the menu driver where it monitors the number of users logging into FACTS versus the number of licenses purchased.

It relies on an environment variable, called SSI_BASE, and an SMFIDS file to cross reference FID(0), which is the value that appears as Terminal ID in System Management's Terminal F/M.

SSI_BASE is the heart of the security system, enabling it to determine who is logging into FACTS and how many times. The variable also compares this information to the number of licenses purchased.

Each licensed user can log into FACTS up to nine times, as long as they do so with the same FACTS user code and on the same workstation.

In any SSI_BASE discussion the word unique appears often, and with good cause. How FACTS uses SSI_BASE is the reason why administrators shouldn't rely on pseudo ttys as SSI_BASE values, and why SSI_BASE needs to be recognized as early as possible in the start up procedure.

When users log into FACTS, the security system captures the SSI_BASE value and SME100 checks the SMFIDS file for the SSI_BASE to determine and set the Terminal ID. These Terminal IDs remain in SMFIDS as long as the User ID is maintained. Every time a user starts a session, the first session will be Terminal ID TA, for example; the second session will be terminal ID TB and so on.

The following table shows a NT/PC user, JohnD, who successfully signed into FACTS three times. He can log into the system six more times with the user code "SSI" without experiencing any problems.

	SSI_BASE	If UID OK, check NID	If NID OK, check TCP/IP	If TCP/IP OK, check C0$(1,3)	If C0$(1,3) OK, check …
Session 1	john	UID=JohnD	NID=Iron	TCP/IP=123.1.1.1	User code=SSI
Session 2	john	UID=JohnD	NID=Iron	TCP/IP=123.1.1.1	User code=SSI
Session 3	john	UID=JohnD	NID=Iron	TCP/IP=123.1.1.1	User code=SSI

When the user launched the first session, the FACTS security system noted network sign on (UID), the PC's network ID (NID), the PC's TCP/IP address and the FACTS user code.

As new sessions are launched, the security system checks each of these identifiers in succession. As soon as one fails to match, it drops all sessions for that SSI_BASE.

In the following table, for instance, one user launched two FACTS sessions successfully. However, the third attempt failed because the security system detected a network sign on for SSI_BASE=john that differs from the first two sessions. This indicates that same SSI_BASE value may have been set in two different autoexec.bat files.

	SSI_BASE	If UID OK, check NID	If NID OK, check TCP/IP	If TCP/IP OK, check C0$(1,3)	If C0$(1,3) OK, …
Session 1	john	JohnD	Iron	123.1.1.1	SSI
Session 2	john	JohnD	Iron	123.1.1.1	SSI
Session 3	john	MaryF	Quartz	127.3.3.3	SSI

The next example shows a user trying to launch a third FACTS session with a different FACTS user code. His third attempt will be successful, but when he returns to the other two sessions and tries to open a program, "User Not Signed On, CR-Continue" will display at the bottom of the screen.

	SSI_BASE	If UID OK, check NID	If NID OK, check TCP/IP	If TCP/IP OK, check C0$(1,3)	If C0$(1,3) OK, …
Session 1	john	JohnD	Iron	123.1.1.1	SSI
Session 2	john	JohnD	Iron	123.1.1.1	SSI
Session 3	john	JohnD	Iron	123.1.1.1	MAR

Chapter 2 Work flow and program concepts

Banking

All bank accounts are set up as separate banks (may have same descriptions) through the Bank F/M program. Each bank that you set up is used system wide.

The Banking subsystem maintains bank account balances through postings from

- Accounts Payable when checks are written
- Accounts Receivable when cash is posted (deposits are made) and when invoices are entered as cash invoices
- Payroll when checks are written
- Sales Orders when invoices are entered as cash invoices.

You can use Bank Transaction Entry to create and edit open bank transactions, such as deposits, bank transfers, miscellaneous bank transactions and non-bank transactions.

Use the Bank Transaction Register to select open bank transactions to print and optionally update. The registers creates a detail listing and a GL distribution.

Use the Bank Reconciliation program to reconcile your bank transactions in FACTS with your bank statement.

Use the Bank Inquiry program to view general information, stored ledgercards and written checks.

The Bank Transaction Listing program allows you to print transactions for a selected bank.

Use the Bank Transaction Removal program to print and remove cleared bank transactions only.

Use Bank F/M (SMF510) to create and maintain alphanumeric bank codes, which are used throughout the system to represent banks used by the company and Bank Control F/M to set up the bank transfer clearing account.

Work flow

The Banking system contains bank transaction header and line files that contain the actual bank transactions. You can edit and delete bank transaction header and lines and use this

information to reconcile to the bank statement. The indirect or detail transaction header and line files hold the cash and check transactions that represent cash coming into the bank from other modules in FACTS. These transactions are used to make up the deposit and non-bank transactions in the bank transaction file.

There are 8 types of transactions in the bank transaction file: checks from the AP and PR modules, returned checks from the AR module, deposits, miscellaneous bank transactions, non-bank transactions, transfer in, transfer out and adjustments.

When you create a bank transfer, the system creates the two transfer type records.

The AP check register, PR check register and returned check register all create transactions directly into the bank transaction files. The bank's balance and the bank GL# is updated. The Cash Receipts Register, AR Sales Register and SO Daily Sales Register write records into the indirect transaction header file for the total of each cash type terms code that is set to use the bank's GL. Check type terms codes write to the indirect transaction line file. If the bank for these transactions does not use the deposit system, the registers will automatically create a deposit record in the bank transaction files that is made up of all of the indirect transactions that were created by the register. The bank transaction is set to a status of complete. The system updates the bank's balance and the bank GL#. If the bank does use the deposit system, the system does not update the registers and updates the bank clearing GL# instead of the bank GL#. You can then use the Bank Transaction Entry program to create a bank deposit composed of the open indirect transactions. Optionally, you can set a bank that uses the deposit system to have the registers automatically create the deposit record. This creates one deposit for all of the indirect transactions but is not updated. You can edit or delete this deposit.

Bank Transaction Entry (SME510) allows entry of bank transfers, miscellaneous bank transactions and if the bank uses the deposit system, deposits and non-bank transactions (both of which require selecting indirect transactions). The system maintains an audit file each time you add, edit or delete transactions in Bank Transaction Entry and Bank Reconciliation Entry program.

Bank transactions are updated by running the Bank Transaction Register (SMR510). The Bank Transaction Register prints a register listing of all transactions to be posted and a GL distribution. Then, it updates the bank's balance and the bank GL# and change the status of each bank transaction to complete. Transactions can also be updated immediately from within the Bank Reconciliation program. This updates the bank balance and the GL but not mark the transaction complete. The register prints those transactions also so you have a hardcopy of what was updated.

Before a transaction is updated, it can be edited or deleted. Once a transaction is updated either from the Update option in Bank Reconciliation or through the Transaction register, changes or deletions may only be done by making adjustments. Each adjustment has its own data, status, GL distribution, etc. You can change the amount of the transaction and the bank reconciliation processing creates an adjustment record tied to the original for the difference in the amount. This adjustment record updates through the next transaction register. When adjustments exist, the original transaction is presented as the net amount after the adjustments have been applied.

Transactions and adjustments can have a status of: Open, Updated but not run through the register, or Complete (i.e. run through the register).

Use the Bank Inquiry program to view general information, stored ledger cards and written checks. Available information includes: General Information--address, contact, phone number, bank account number, current balance, general ledger number and use of ledger cards flag, ledger cards information--date, debit amount, credit amount, balance, memo and register number, and Check information, including check number, check date, check period, payee number/name, check amount and clear date. You can access the deposit ticket using the Menu option "View" - "Archived Deposit Ticket", or using the button "Archived Dep", or right-click on the line that has a Deposit Ticket number and select "Archived Deposit Ticket". Individual ACH payments and wire transfers post to the Bank Reconciliation system as individual checks using the ACH or wire payment number. Combined ACH payments post the combined totals as individual checks using the combined ACH payment number. For combined ACH payments, the View Detail window of Bank Inquiry you can select Ind ACH to view the individual ACH checks that made up this combined check. FACTS displays all of the individual ACH payments that make up this combined payment in the line browser. The browser information includes Check number, Payee number, Payee Name, Check Amount, Discount, and Voided.

The Bank Transaction Listing program allows you to print transactions for a selected bank.

Use Bank Reconciliation Entry to reconcile the bank transactions to the bank statement. You can quickly set the status of any updated transaction to "cleared". Once the transactions balance, you can select the Reconcile function to change the reconciled flag of all transactions to "Y" and set the reconciled date. The last reconciled balance and date of last reconciliation in the bank file are updated.

Each bank transaction has a cleared status and reconciled status relative to the bank reconciliation function. All sequence numbers for a transaction (i.e. the transaction and all adjustments to it) also have the same cleared and reconciled status.

During Bank Reconciliation, you can enter new transactions, edit open transactions or make adjustments to transactions that are already updated or complete. Use the Update function to update an open transaction or adjustment immediately. This causes the bank balance and GL updates to take place and the transaction status to be changed to "updated". The system also maintains a GL detail file to hold the GL information of each transaction and adjustment that is updated in the bank reconciliation. This record is used by the register to document what GL postings actually occurred and to fill in the remaining detail of register number, etc., in the GL transactions. The Transaction Register has two sections, one for open transactions and one for updated transactions. When the register is updated, the status changes to Complete for all transactions appearing on the register.

Banking processing includes bank reconciliation history processing.

The Bank Reconciliation Report (SMR590) shows cleared checks and deposits and outstanding checks and deposits. Most companies are using this from current period balancing, prior period analysis, and research perspectives. A Reconciliation Summary is also printed. The Reconciliation Summary can be run for an ‘in-process’ reconciliation and

one that has been updated in the past. When running the report for a past statement, the bank statement ending date is validated against the reconciliation history file.

The Bank Reconciliation History Entry (SME598) program is available to view, create and maintain historical reconciliations. You can maintain a historical account of each bank's reconciliations using the beginning and ending balances for the statement, as well as the reconciliation date. This information is used to print the Bank Reconciliation Report (SMR590).

Historical bank reconciliations are typically required by auditors during the course of a Financial Statement Audit or Review.

Use the Bank Transaction Removal program to print and remove cleared bank transactions only.

Use Bank F/M (SMF510) to create and maintain alphanumeric bank codes, which are used throughout the system to represent banks used by the company and Bank Control F/M to set up the bank transfer clearing account. Use this program to create and maintain alphanumeric bank codes, which are used throughout the system to represent banks used by the company. Before you create bank codes, make sure General Ledger account numbers exist for the bank or banks the codes will represent. Account numbers are created and maintained in the Account F/M program (General Ledger>File Maintenances>Account F/M). Bank codes can be up to two characters long and they are used in the following programs (among others): Cash Receipts & Adjustments Register (deposits), Daily Sales Register (cash sales), AR and PR Check Registers (checks)

In the Security Code section, enter security codes side by side for this access to this bank.

Note: With unrestricted access, the user will be able to do all of the functions available in the banking system for this bank.

By giving a user the limited access security code instead of the unrestricted code, the user will only be able to view, edit or delete open deposit and transfer out transactions for this bank in Bank Transaction Entry. In all other banking programs, the user will get the message "User does not have security to access this bank".

With neither code, the user will not be able to do anything with this bank.

Use Bank Control F/M to set up the bank transfer clearing account. The system uses the bank transfer clearing account when posting bank transfers so that each bank can update its side of the transfer independently. Bank Control F/M is also where the system keeps track of the last register number used for the Transaction Register.

Program concepts

Non-bank and miscellaneous bank transactions

Non-bank transactions are a way to take money that was originally intended to go into the bank and direct it to some other GL account. An example of a non-bank transaction is credit card processing fees coming out of the credit card deposit for the day. These transactions create records in the transaction header file, SMTRNH, with a new transaction number and a zero sequence number. You can also "change" an updated or completed transaction. Note that the original transaction does not change but FACTS creates an adjustment record to reflect the changes made. The adjustment record has the same transaction number but will have a non-zero sequence number. This ties all transactions and their adjustments together. The adjustment records are not available in the entry program but the net effect of the adjustment is visible on the original transaction line.

Miscellaneous bank transactions allow you to enter transactions that affect the bank balance and bank GL# and then indicate via the GL# what other account to post it to. Miscellaneous bank transactions are not created from another function in FACTS. An example of a Miscellaneous bank transaction would be bank service charges.

Bank transfers

A bank transfer is actually made up of two separate transactions that are tied together. When you select to create a transfer, it means you are transferring money out of the bank of this entry and into another bank that you indicate. FACTS creates two records in the bank transaction file for this. One will be a "transfer out" for the bank that created the transfer. The other will be a "transfer in" for the bank the money is being transferred to. Each bank can only view its own half of this transaction. FACTS keeps these two transactions in sync but only the "transfer out" transaction can be changed. Each bank posts its part of the transfer independently so if either half of the transfer is already updated, the open side can no longer be changed or deleted. Additionally, you cannot adjust the open transaction in Bank Reconciliation Entry until it is updated. If the other half of the transaction cannot be found in the file (if it has been removed), the transaction cannot be changed or deleted and it displays asterisks on the Bank Transaction Register (SMR510) and in the Bank Inquiry (SMI510). Once updated, adjustments can be done from either side and they will no longer effect the other transaction.

You can create new deposits regardless of the "Use Deposit System" setting in Bank F/M (SMF510) as long as there are indirect transactions to be selected. This way, if the Use Deposit System setting is inadvertently turned off, any unconsumed indirect transactions can still be used. The cash transactions are in the indirect transaction files and are selected to make up the deposit. If the bank did not use the deposit system, then the individual registers in FACTS create the deposit record in the bank transaction files and marks it as complete.

A non-bank transaction can be created regardless of the "Use Deposit System" setting in Bank F/M (SMF510)as long as there are indirect transactions to be selected. This way, if the Use Deposit System setting is inadvertently turned off, any unconsumed indirect transactions can still be used. The cash transactions are in the indirect transaction files and are selected to make up the transaction. FACTS Bank Reconciliation is designed so you can select to take some cash that was received and put it to something other than the bank, like into petty cash. Enter the GL# to post to. Once updated, non-bank transactions cannot be adjusted. You can simply enter any corrections directly into General Ledger.

An adjustment transaction allows you to change a transaction amount after it has already updated the bank balance and General Ledger. You must indicate the GL# to post to for the adjusted amount.

If you do not have either the unrestricted access security code or the restricted access security code in the bank you try to enter, FACTS does not allow you to proceed into the program.

If you have a restricted access security code for the bank entered, you are able to view, edit or delete open deposit and transfer out transactions only.

Bank reconciliation

In Bank Reconciliation Entry as you choose transactions to clear in the line browser, the system adjusts the Difference amount. As you select un-cleared checks/transactions, the system updates the status from "uncleared" to "cleared." Once the Difference amount is zero, select the Reconcile button to finalize the check clearing process. At reconcile, the system updates the checks/transactions status to "reconciled." You can exit the Bank Reconciliation program without having to finish the entire task of reconciling.

You also have the ability to "clear" un-updated transactions, but you cannot reconcile them until the Bank Adjustment Register has been run. When you clear un-updated transactions, the system displays a message: "Please run the Bank Adjustment Register before reconciling" if there are un-posted adjustments on file.

Transaction adjustments

You can adjust an existing bank transaction within the Bank Reconciliation program. Use this function to correct the occasional clerical error and to allow for credit card companies that take their fee directly from daily deposits into the customer’s accounts. You can add bank adjustments during the bank reconciliation process. The adjustments to the line may be a file keyed off of the transaction record. This adjustment record must be maintained for audit purposes.

When you enter the adjustment, FACTS also adds it to the bank adjustments file (used in Bank Adjustment Entry), which changes the Unposted Adjustments balance in the header. You can choose the GL account to which the difference is posted.

Archived deposit tickets

You can access the deposit ticket using the Menu option "View" - "Archived Deposit Ticket", or using the button "Archived Dep", or right-click on the line that has a Deposit Ticket number and select "Archived Deposit Ticket".

Menu Setup

FACTS ships with a complete set of menus and program descriptions. However, if new programs are added to the system, this sub module enables administrators to add them to the menu system. Administrators can also delete menus for modules that were not purchased.

All programs and menus must be set up in the Program F/M before they can be set up on menus in the Menu F/M.

Use Program F/M to add programs to or delete programs from the menu system. You can also customize the way program descriptions appear in menus, restrict certain terminals from accessing these programs and control how users print from these programs.

FACTS ships with a standard menu system; however, you can use the Menu Entry (SME320) program to arrange and edit menus to suit the needs of your business. The menu name, return menu and all called programs must be defined through the Program F/M program. The third character of the menu and return menu names must be S. The FACTS Master Menu is always MMS000.

Adding and customizing programs in Program FM

In addition to adding programs to the system, Program F/M can be used to customize the program descriptions that appear in the menu system, create selection numbers for the character menu system and set up new access codes or change existing ones.

Naming standards: When creating or renaming programs, make sure you follow the naming standards set by Infor™. We provide a quick overview here. For more information, refer to the FACTS Technical Manual for this release.

Every FACTS program goes by two names. One is an alphanumeric programming name, for example SMF310. The other is a descriptive title, such as Program F/M.

All alphanumeric names are six characters long and follow these rules:

The first two characters represent the module. For example, in the name SMF310, the first two characters tell you that the program is part of the System Management module.

The third character conveys which type of program it is. The F in SMF310 indicates that this program is a file maintenance. Use E for entries, I for inquiries, P for special form prints, R

for reports, S for menus (selectors) and U for updates. The last three characters must be numeric and designate the subsystem to which the program belongs.

Restricting access

You can set up the code to access the program and if the program is a file maintenance, you can also determine if the information in the file should be audited. You can also establish, by program, availability of a printer and the default printer for the program by terminal.

Once program names are defined, menus may be constructed using the Menu F/M program.

Password protecting the System Install menu (SMS999)

Customers can create a password that will be required for access to the System Install Menu (SMS999). To create a password for the System Install menu, first create an entry in Program F/M (SMF310) for SMS999. All fields in this program will be ignored for SMS999, but a record must exist for it. Then use Program Security Maintenance (SMF420) to create the password for SMS999 in Company 01. When running the install menu, the user is not signed into any company, but passwords are specific to company. As a result, you must choose a company to use for the password to System Install Menu (SMS999). The security code for SMS999 is ignored because when accessing the System Install menu as the user is not signed into FACTS.

Having done these two steps, users attempting to access the System Install menu from the FACTS Sign-on Screen will be required to enter the correct password assigned to company 01 and the System Install Menu (SMS999).

Note that the user will be prompted for the Install Menu password every time they return to it (e.g. after entering System Control F/M, etc.). The other options on the Install Menu will not require passwords. If users are able to access the install menu, they will be allowed to run any of the programs on it.

Security System

The programs available on this menu enable the System Administrator to create and maintain FACTS users and to set program security.

The first line of security is the FACTS Sign On Screen. Each user must have a user code, password and company number to gain access to FACTS. This keeps unauthorized individuals from entering your system, but many companies find that they need to restrict authorized FACTS users from gaining access to programs and menus inside the system.

Passwords and the security system

Administrators can set up three additional types of security for FACTS users.

User security codes: This security method is effective for restricting certain users to certain programs in a more automated and transparent manner.

Administrators can assign up to 10 security codes to each user record in User Code F/M. Use this program to create and maintain user codes for each user of the system. Each user code is assigned a password, security levels, valid companies they may work in, fax phone number, suffix and cover page, whether user tracking is used and the initial menu to display. These entries, in conjunction with the program security levels and passwords, provide maximum security and privacy of information.

When signed on, the user's code is displayed in the upper right corner of the menu screen. As users attempt to access a program, their security code is checked against the program's security code. The codes must match for users to use the program.

These same security codes can be assigned to programs or menus in the Program Security Maintenance. Use this program to create and maintain passwords and security codes for all programs and menus. By doing so, you can establish which users and terminals have access to a program or menu. It is suggested that this program also be assigned a password to maintain security. All programs initially are assigned a security code of zero. You can assign a security code and password to any program or menu. During normal processing, the security code is checked and validated.

If a user lacks the security code assigned to a program, the system prevents access. Each program is assigned to one security code. Initially, all programs are set to 0. The user may then modify security codes and allow specific users into specific programs. For instance, most companies may want to keep their salespeople from the Salesperson/Territory F/M, where they could potentially change minimum required calls, commissions, monthly sales, etc. An administrator could assign a security code of 1 to each salesperson's user code record and then assign that same security code to Salesperson/Territory F/M and any other programs salespeople should not access. This method enables the system to track security clearance so that administrators don't need to keep track of passwords, and users don't have to remember them. Users simply can't gain access to areas they are not "coded" to use.

Similar to the idea of assigning security codes to users, terminal IDs can be assigned numbers in Terminal F/M. By assigning these numbers, administrators can create groups of Terminal IDs and then designate which numbers (representing groups of terminal IDs) have access to which programs in Program F/M (System Management--> Menu Setup-->Program F/M). By default, all terminals are flagged as valid for all programs. This method enables administrators to assign security rights based on terminal ID and assign security rights across a range of terminal IDs, which can save time.

Individual programs and menus can be password protected in the Program Security Maintenance program. This method can be used in conjunction with user security codes so even users with the proper code must enter a password to access a program.

User tracking

The FACTS User Tracking feature enables the System Administrator to track program usage on the system. User Tracking monitors and records program entry, exit and usage time by user.

User Tracking Inquiry (SMI640) displays program usage information by user code. Display is limited to user codes designated for tracking in the User Code F/M. Inquiry information includes for each user: date, company, program designation, program name, time of entry into program, terminal ID, and error code.

Use Security Code Maintenance (SME016) to assign descriptions to each security code and to quickly identify all users who have the code and all programs where the security code is used. These same security codes can be assigned to programs or menus in the Password Security F/M. If a user lacks the security code assigned to a program, the system prevents access.

User Tracking Removal enables the System Administrator to remove the tracking information.

Use Security Code Update (SMU410) to change security codes by any range of programs and any selected program types.

Use Notes Entry (SME710) to enter and maintain notes for AR documents, Sales Order documents, Purchase Order documents, customers, items, and vendors. The system displays notes information from several points within FACTS: Item F/M (ICF910) and Customer F/M (ARF910), Item Inquiry (ICI610) and AR Customer Inquiry (ARI610), Item Search and Customer Search, Purchase Order and Sales Order entry programs.

The User Management (SME900) program monitors user activity and remove users from the system or by company. User Management (SME900) is also available from the System Install menu. User Management Access privileges are specified in User Code F/M (SMF410). When all users are locked out of FACTS, an authorized user can get to User Management from the System Install menu to let the users get back in. User Management (SME900) allows you to give "Free Passes" to signed-on FACTS users, which allows those users to remain signed on when everyone else is forced out of a company or entirely out of FACTS. The purpose is to allow the system administrator to selectively allow some individuals to continue working while they keep others out, allowing them to complete tasks like month-end processing. To maintain Free Passes, right-click on any user from within User Management. You can click **Update This User's Free Passes** to select to give the user a free pass for the company you currently are logged into or all companies, or **Clear All Users' Free Passes** to remove free passes from all users in the FACTS system. A Free Pass is only valid while the user is signed in, and it applies to all of that user's sessions which are signed in. To view free pass information for all users, select Options>Show All Free Passes. The All Out function, which logs all users in all companies, except for users who have Free Passes for specific companies, off of the FACTS system is not available if there is no user who has User Management Access privileges in User Code F/M (SMF410). A warning message is displayed, and you cannot click All Out.

The API Key Code Entry (SME007) program allows you to enter the API Publish key code, once the API Toolkit is installed and running. This program also helps prevent unauthorized access to the API by providing a password that is required for access to the Subscribe APIs.

In User Code F/M (SMF410) settings are available for users' password, security levels, valid companies to work in, fax phone number, suffix and cover page, whether user tracking is used and the initial menu to display and administrator privileges. These entries, in conjunction with the program security levels and passwords, provide maximum security and privacy of information. User code settings of note are defined in this table.

Setting	Definition
Allow Command Mode	Indicates whether to allow this user to use the 'break' key to access command mode to clear FACTS program or system errors. Note: Infor recommends this check box is unchecked (not selected) for all users as the default. It is provided in case a user encounters an error and must use this method to clear it. After an error is encounter the user can access this program and select the check box. After completing the command mode action, the user record should be re-accessed in User Code F/M and this check box should then be unchecked.
Require Escape Code	Indicates whether this user must enter an escape code before they can abort out of an error. If you check this check box, the user must contact the system administrator for the escape code when the window describing the error condition is displayed. By doing this, you prevent users from aborting out of programs that can be updating files without first checking with the system administrator. If you enter N, this user will be able to abort from any error in any type of program. From an error handling window, a user set up with No (unchecked) will also be able to enter SS to escape into the workspace of the current program. However, regardless of the entry in this field, all users are able to abort from an error resulting from a locked record. Note: Certain programs can always require an escape code (for example, the DSR update). If Z8$ is set to "**" prior to calling the standard escape routine, all users will be required to enter an escape code regardless of this flag or which error was encountered.
FACTS Date Change	Indicates whether to allow this user to change the FACTS system date using the Set FACTS Date program under the user name drop-down on the FACTS Main screen. The Set FACTS Date program is only available if you select this check box.
CCToken Management	Indicates whether to allow this user to add, delete and

Setting	Definition
Access	modify credit card tokens. Refer to *Infor Distribution FACTS Electronic Payments Guide for CenPOS* for credit card handling information.
User Management Access	Indicates whether this user has access to the User Management program as the restoring user when the All Out or Comp Out functions have locked all users out of FACTS. When checked, this user code and password will access User Management to restore access for all other users. When all users have been kicked out of FACTS via User Management, the message: Proceed to User Management? is displayed at log in. Click OK and specify the user code and password that has User Management Access privileges. In User Management, click All In. Note: Infor recommends that at least one user have this check box checked and this user code and password documented for access.

Messages

Work flow

The Messages menu enables you to set up messages to send to a specific user or all users. You can enter messages so they display on a specific menu on a specific date. When users sign in and access a menu, the entire message appears in a pop-up window.

Individual messages can be created and deleted individually through the Message Entry program. Use this program to enter system messages that display on any menu on the current or any future date. Messages can be used as reminders, such as meetings or as PR, such as birthdays. The program enables you to establish the message content, the date it appears and the menu on which it is displayed. Messages can be displayed for a specific user or for all users. Up to six lines may be defined for each message.

Messages may be removed individually through this entry program or by date through the Remove Messages program. Messages should be removed periodically to prevent the file from becoming full. You can remove messages for a specific menu, a range of menus or for all menus. Messages to be removed are determined by the message date. All messages dated on or before the user-entered date are removed.

To create message that can be output to printers, fax machines or sent as an OA message in the Office Automation system, use the Quick Note Entry program. The note or message

can be up to 999 lines. Once the program is exited, the note/message entered is not saved. The same note/message that is entered may be printed, faxed and sent as an OA message to as many destinations as needed up until you exit the program.

Use Note Entry to enter and maintain notes for AR documents, customers, items, IC transfer tickets (header and lines), and vendors.

System Dashboards menu

Work flow

The system alert and background processing routines facilitate any actions needed to feed into FACTS programs. System alerts processing has a defined set of routines and the update interval required to perform calculations and alerts. The background processing agent is responsible for handling these updates and providing the data to the system.

Program concepts

The Background Scheduler Dashboard allows FACTS administrators to schedule background activities. The browser displays each of the background processes currently scheduled, including the process code and description, run frequency, next scheduled run date and time, last run date and time and result. You can modify the schedule for a background process using this screen.

Background processes

These background processes are available:

API Polling Directory Handler (A), which is used to process API Polling directories/locations through to completion.

System Alert Miner (A1), which is used to process alert to facilitate any actions needed to feed into the Buyers Control Center and Exception Control Center.

Publish XML to destinations (I1-BKC201), which is used to publish XML content, both internally and for Infor OS.

Infor OS Database Output Writer (I2-BKC202), which is used to deliver the XML in the SMXOUT file to Infor OS.

Infor OS Database Inbox Handler (I3-BKC203), which is used to retrieve XML from the Infor OS inbox and deliver them to the polling directory.

Infor OS Database Inbox Cleaner (I4-BKC204), which is used to remove processed XML records from the Infor OS inbox and outbox.

Replenishment Calculations (R1-BKC600), which is used to process replenishment routines for usage rollup, warehouse rank, and warehouse item controls.

Replenishment Calculations (R2-BKC601), which is used to process replenishment routines for warehouse rank and warehouse item controls.

Replenishment Calculations (R3-BKC603), which is used to process replenishment routines for warehouse item controls only and auto-calculations in the Buyers Control Center (POE400).

Replenishment Calculations (R4-BKC604), which is used to process replenishment routines for seasonality analysis.

Usage Review and Update (R5-BKC606), which is used to process replenishment routines for usage.

Replenishment Calculations (R6-BKC607), which is used to process replenishment routines for auto-calculations in the Buyers Control Center (POE400).

System Clean Up (S1-BKC605), which is used to remove closed alerts and background processing history in the FACTS system.

Rebuild Sort Files (S2 – BKC608), which is used to rebuild the sort files in place, eliminating the need to lock the source files during a rebuild. S2 handles AP, AR, MC, PO, IC, SO and RM sort files. The default is to run this monthly on the 15th of the month, at 1AM.

System Data Updater (S3 – BKC609), which is used to make various direct updates to the FACTS data. The program updates the status of expired quotes once they are expired. By default, S3 is run at daily 12:30 AM.

Background Process (S4 – BKC610), which is used to notify the user when a service hold alert action or service hold release alert action is issued. The alert is raised, and users are directed to Order Review (SOE230) based on the type of alert being responded to. These alert types are available: Hold Status = N – Documents Not on Hold if alert is a release alert, Hold Status = H – All Documents On Hold if alert is a hold alert.

Jobstreams (BKC611) background process which is used to spawn unique and individual background processes for each job stream that is scheduled to run. The program raises the JOBSTREAM alert when it is run.

The System Alerts Dashboard is used to review the alerts that a user is subscribed to and manage alert subscriptions. In the browser in the lower portion of the screen, the system displays the alert code and description and number of subscriptions and alert status. You can highlight an alert line in the browser and click Manage Subscriptions to access the Manage Alert Subscriptions (ALE101) screen where you can add a subscription for an alert type. Click Alert Details to view the Details for System Alert screen, which displays the Alert code and name, an explanation of the alert and the condition that generated it, where the

alert is delivered: to the user, the Alert Control Center program or both, and the available subscription values. Below the alert description, the Raise Alert status is displayed to indicate if any alert, company-level, or system-level check box is inactive. Once you review the alert detail information, click OK to exit the screen and return to the System Alerts Dashboard.

Use the Background Process Log Viewer (SMI915) to view records from the Background Process Log file, SMXBLF. You can specify a particular Transaction GUID, allowing for quick research on a particular transaction or view the contents of the log file using various filters. Use the Search option for a specific transaction GUID and sort by the results “CID In” and “CID Out” order, allowing a return of a transaction GUID based on incoming or outgoing CIDs. In the Filters section additional check boxes and prompts are available for specifying the browser results. In the line browser, the following information is displayed for each record: Date/Time, Transaction GUID, Sequence number, Disposition (I-In, O-Out), Error Indicator(‘*’ or blank), Event Code, Event Code Description, API Name, Entity, CID In, CID Out, LID, Generation, Destination path, and Message Memo. When you double click on a GUID line in the browser, all sequence numbers for the selected Transaction GUID are displayed.

Use the Background Processor Results (SME911) screen to review results file details for the alert highlighted in the browser. For alerts, the display includes the background alert process code and description, start and completion dates/times for the alert, the alert result status, error code, run time and user code that generated the alert. For replenishment calculations and system clean up, the display includes the process code and description, program number, last scheduled and non-scheduled run date and time and the run frequency. For Job Streams, all background job stream process results in order, job stream name, then within the name by date recent-to-oldest. Click **Jobstreams** to display all background process job stream results in the JobStreams window.

Infor OS menu

The Infor OS menu contains programs used to configure FACTS to use Infor Operating Service to exchange data with another Infor product or third-party product. These programs are available.

- System Control F/M - Infor OS tab settings
- Company Control F/M - Infor OS setting to enable Inbox/Outbox functionality.
- Database Definition - to configure the connection string and other information used by the stored procedures, including Infor OS-specific information based on the Usage Type.
- Background Scheduler Dashboard - to schedule background activities, including these Infor OS processes:
    - API Polling Directory Handler (A), which is used to process API Polling directories/locations through to completion.

  - Infor OS Database Output Writer (I2-BKC202), which is used to deliver the XML in the SMXOUT file to Infor OS.
  - Infor OS Database Inbox Handler (I3-BKC203), which is used to retrieve XML records from the Infor OS inbox and deliver them to the polling directory.
  - Infor OS Database Inbox Cleaner (I4-BKC204), which is used to remove processed XML records from the Infor OS inbox and outbox.
  - System Clean Up (S1-BKC605), which is used to remove closed alerts and background processing history in the FACTS system.
- Background Process Log File Viewer - to view records from the Background Process Log file (SMXBLF).
- Infor OS On-Boarding - to push all relevant FACTS data to Infor OS in a hierarchical manner, provide flexibility as to information that is sent, feedback of current status, and access to historical push request data.
- Infor OS Management FM (SMF951) - to manage all Infor OS-related settings and values. The SMOSFM file is used to store these values.

Managing stored procedures for Infor OS

FACTS can use the inbox/outbox connection point methodology to connect to the Infor OS interface. Stored procedures are used to maintain the inbox/outbox tables of a database created on SQL or PostgreSQL servers. This topic is a guide for maintaining the stored procedures within FACTS and addresses behind the scenes operations that take place to keep the systems inline.

To establish a connection to a SQL server or PostgreSQL database, create a corresponding database definition in Database Definition (DOE400). Complete the connection string with valid parameters. Click Test to update the stored procedures on the SQL or PostgreSQL server for the indicated connection string. If the stored procedures do not exist within the SQL or PostgreSQL database, they are created when you click Test. If the stored procedure version number within the SQL or PostgreSQL database does not match the version number on the stored procedure in FACTS, clicking Test updates the stored procedures in the SQL or PostgreSQL database with the ones maintained in FACTS.

All sequel statements from FACTS to SQL or to PostgreSQL are performed using the CSSQL.pvc object to execute the stored procedures or manipulate variable values. To make the CSSQL.pvc object available to any running procedure, this object is added as a property to the %CSYS object. The property name is %CSYS'sql_object. By default, the property is instantiated to the class to access the routines and variables is via syntax.

Refer to these examples:

- To set the desired database: %csys'sql_object'database_id$=<the desired database ID>

- To use the stored procedure to clean the database inbox for PostgreSQL: ret_val=%csys'sql_object'execute_sp("pgs_facts_clean_inbox").

All sequel statements to manage and maintain the SQL or PostgreSQL databases first implement this Connect routine: ret_val=%csys'sql_object'connect()>.

The Connect request uses the selected Database Definition's connection string to obtain a valid connection to the SQL or PostgreSQL database. Then, the version number within FACTS for the stored procedures is validated for the given database. If the version number is out of sync, the stored procedures in the database are deleted and the ones from FACTS are uploaded and saved for use.

Program concepts

Use Database Definition (DOE400) to configure the connection string and other information used by the stored procedures. It includes Infor OS-specific information based on the Usage Type.

Use Stored Procedure Maintenance (DOF400) to manage stored procedures in FACTS. These stored procedures are used to maintain the stored procedures in SQL or PostgreSQL databases. Stored procedures are delivered with FACTS and cannot be renamed. The syntax of the stored procedures is specific to the type of database installed and used for Infor OS inbox/outbox connection point methodology. When revisions are made to the stored procedures within FACTS, the associated version number is incremented. Then, the version number within FACTS for the stored procedures is validated for the given database. If the version number is out of sync, the stored procedures in the database are deleted and the ones from FACTS are uploaded and saved for use. If the version number is not changed the database will not be updated for the revisions. Revisions should not be made to the store procedures within the database. Using CSSQL.pvc and the Connect() routine overwrites the database stored procedures when they become out of sync. Proper management of stored procedures is done using Stored Procedure Maintenance and associated version number updates.

This table describes the available stored procedures.

PostgreSQL syntax	SQL syntax	FACTS background process	Description
pgs_facts_create_outbox	facts_create_outbox	I2 (BKC201)	Creates database records in the outbox coming from FACTS. This sends a BOD from FACTS
pgs_facts_get_inbox	facts_get_inbox	I3 (BKC203)	Retrieves a database record at a time from

PostgreSQL syntax	SQL syntax	FACTS background process	Description
			the inbox for consumption by FACTS and the API system request. This is processing a BOD.
pgs_facts_clean_inbox	facts_clean_inbox	I4 (BKC204)	Cleans the inbox of processed database records. These are already processed BOD requests.

Use the Infor OS On-Boarding (SME925) program to push all ION-relevant FACTS data to Infor OS in a hierarchical manner. The process provides flexibility for the information that is sent. This program provides feedback of current status and provides access to historical push request data. The ION Initialization History (SME930) screen is displayed when you click History on Infor OS On-Boarding (SME925). ION Initialization History shows all of the records from SMPUSH for the current Ultimate Parent. This screen is display only, in alt-key 1 order (descending GUID), showing all companies.

Use the Infor OS Management FM (SMF951) program to manage all Infor OS-related settings and values. The SMOSFM file is used to store these values. The General tab contains global settings, such as the Tenant ID, Oagis release, and the connection type, Inbox/Outbox or REST/API. When modifying the connection method from Inbox/Outbox, a warning is displayed if there are any unprocessed records remaining in any database set up for use with Infor OS. Documents may be orphaned. The Inbox/Outbox and IMS tabs contain the necessary values for each integration connection type.

Note: To modify this program, you must check the Disable Background check box on the Settings tab of System Control FM (SMF950).

Push Tier, Push All, and Push Line processing

This is a workflow for push processing.

For Push processes a window is displayed showing the progress bar while processing, then all lines are re-displayed.

When a Push process is selected, a Push GUID is created for the line, a record is created in SMPUSH, and all records for the company requested in the Ult-P file are written to SMPUBQ with the Push GUID.

If a record already exists in SMPUBQ with a Push GUID, it is replaced with the current one. If a record already exists in SMPUBQ with an LID, then the SMPUBQ record is updated with the LID removed, effectively turning the old “show” request into a “sync”.

Write to SMXBLF as PUBQ_CLR_LID event

If creating a new record in SMPUBQ, write to SMXBLF as PUBQ_WRITE

Increment the # records count for this Ult-P

When all records for the Ult-P are processed update the SMPUSH record with the initial records count, who last received it (LID or All), and status change to “W”. The process the next line.

Inquiries

The System Administration inquiries enable administrators to analyze information in various views.

The Executive Inquiry provides, by branch and department, the current accounts payable and receivable balance, cash in bank, inventory valuation, open purchase and sales order balance and sales history for the next periods and the last six periods. In the Account F/M program in General Ledger, each GL account number is assigned a summary management type to be used in this inquiry. The types are: cash (used to calculate cash in bank), cost (used to calculate cost and gross margin % in sales history), inventory (used to calculate inventory valuation), payables (used to calculate open payables balance), receivables (used to calculate open receivables balance), and sales (used to calculate sales and gross margin % in sales history). Also in the Account F/M program, each GL account number is assigned an account type. Next period journal entries for GL account numbers assigned an account type of assets or liabilities are included in this inquiry. The open purchase orders are calculated from the purchase order file. The open sales orders are calculated from the sales order file. The figures displayed are calculated each time the program is used.

The Amortization Schedule allows users to enter a loan principle, interest rate and period of time for a loan and the loan payments will be listed on the screen. The schedules can be output to a viewer or a printer. You can enter a: Loan description, Loan principle, Interest rate, Life of loan and Starting month. The screen is divided into two portions. The upper portion of the screen is called the header portion where the user information is entered and the calculated monthly payment, total payment and total interest are displayed. The lower portion of the screen is called the line-item portion and consists of the information concerning the loan balance, etc., by month. Schedule information includes the following: one line per month of a year - year, month, total accumulated months, payment, principle, interest, total interest paid, and balance of the loan. The information entered, calculated, and displayed is not stored by the system.

The Terminal Inquiry displays all terminals logged into the system and the company and program being accessed by each user. The All company option is only available if the user

running User Management (SME900) has access to all companies on the Security tab of User Code F/M (SMF410). In the Refresh in Minutes field enter the interval in minutes for the information in the browser to be redisplayed. In the browser in the lower portion of the screen, the system displays the FACTS user count, user id, user name, TCPIP address, network id, operating system user id, the FID(0), the T number and Base ID. You can select: Update to update the user information display in the browser or Exit to return to the main Security menu.

The User Tracking Inquiry provides a list by user code itemizing which programs are accessed and the time used (if the user tracking flag is set to Y in the System Control F/M). (See the section on user tracking in the overview section.)

The Program Inquiry allows the user to view in list form all the programs and menus set up in the Program F/M on the screen along with their access codes and security codes.

The File Usage Inquiry provides a list by file name and by percentage used of all file specific information concerning file usage. The program can display files based on percentage used. Inquiry information includes the following: file name, file description, file type, key size, record size (i.e., total size of record), record number (i.e., number of records defined for this file), records used (i.e., number of allocated records), and percent of records used.

Use Audited Changes Inquiry to view changes to graphical maintenance files. This program is only available from graphical file maintenance programs for users who have the File Maintenance Audit checkbox in The Administrator Privileges section of the Security tab in User Code F/M.

Use System Error Inquiry (SMI650) to view and sort FACTS' program lines that have errors. You can filter and display using these values: company, user, program ID, line number, error number, user ID, exit status or date range. The browser lines include this information: date, tie, company name and number, user id and name, program name and number, line number, error code and description, status, screen guid and fid, and terminal description.

Reports and prints

The reports and prints programs provide lists of companies, programs, menus, users on the system and program changes.

The Company Listing provides a list of all companies, addresses and phone numbers set up in Company F/M (System Management-->File Maintenances-->Company F/M). Report information includes the following: company number, name, address, and phone number. Also included is the total number of companies listed.

The Program Name Listing to obtain a report of program names, descriptions, security codes, terminal validity and printer usage. The printout may be used as a worksheet to initially define security information and printer usage or as reference for users. Report information includes the following: program designation, name, security code and access code. For each of up to 999 terminal numbers, validity (Y or N) is printed along with the

printer-selection option number and the normal printer. Program descriptions, terminal validity and printer usage are defined in the Program F/M. Security codes are issued through the Program Security Maintenance.

The Program Usage Report provides a list of each program defined and lists the menus containing the program. The report may also print only programs that are not used on any menu. This printout is useful to purge the names of unused programs or to alert the user to place a program on a menu. Report information includes the following: program designation and the name of each menu on which the program appears. The total number of programs printed is also included. Program names are defined through the Program F/M. Menus are constructed through the Menu F/M.

The Menu Selections Print prints a range of menus (as determined by the user) which may be helpful in setting up security. This report is useful when you need to verify that selector-menus and security codes are defined properly. Report information includes the following: menu name, menu description, return program, and the names, descriptions and security codes of all programs called by the menu. The report format resembles the actual screen display. Menus are defined through the Menu F/M and security codes are maintained through the Program Security Maintenance.

The User Tracking Report prints a list of users using the system as to which programs are accessed and the time used (if the user Tracking Flag is set to Y in the System Control F/M). (See the section on the user tracking in the overview section.)

The Program Change Report prints a list of program changes from the Program Change F/M. The user (affiliate) enters program changes. If no program changes are entered, this report will not be used.

The F/M Audit Report prints a list of any changes made to the file information through file maintenance programs. This information is limited to file maintenance programs where an audit trail is being kept for changes (as set in the Program Name F/M). Report information includes the following: program designation, program name, date of changes, user code, user description, company and a list of the old record and new (changed) information as listed in the file.

The SM Code List prints a list of various SM codes including terminals, printers, banks, branches and files. Report information includes each code and the information stored with the code. The report also includes the total number of codes listed.

End of period

Use the two programs located on the System Management End-of-Period Checklist menu to help you organize and document how you will run the end-of-period procedures each period.

Initially, all standard end-of-period procedures are provided in the End-of-Period Checklist Entry program for each module. This is particularly useful for organizing month-end closeout procedures. If you need to change any of these procedures to better fit your company’s

needs, changes may be made through this program. For example, in the Accounts Receivable End-Of-Period checklist, there is a procedure to run the Service Charge Register.

This register is optional and may therefore be removed from the End-Of-Period checklist if a company does not charge service (finance) charges. The End-of-Period Checklist Print program prints a list of all end-of-period procedures (as set in the End-of-Period Checklist program). Report information includes the following: module code heading, and the descriptions in the order that they are entered in the entry program. The report also includes the total number of modules listed. The checklist should be used every period of the year as the period procedures are completed.

File maintenance and infrequent file maintenances

Use the System Management File Maintenance menu to access these programs.

Use System Control F/M (SMF950) to enter FACTS-related authorization code information, such as total number of terminals, modules purchased, and so on. You can also indicate whether alerts can be raised at the system level. Make sure you have your FACTS Authorization Code Sheet ready when you're setting up this program. When entering data, make sure answers you provide are accurate and consistent with what is printed on the Authorization Code Sheet. Every program in the FACTS system checks this record. Any inaccuracies will crash the system. DO NOT CHANGE the software level, serial number, modules purchased, main company name, ASCII Bit Set and maximum number of terminals after initial installation without contacting Infor. Unauthorized changes to these fields will crash the system.

Use Company F/M (SMF910) to create and maintain companies in the company control file. Users establish their own set of valid companies to be set up on the system. Companies should be numbered beginning with 01, 02, etc. The main company must be 01. IMPORTANT: Use the procedures outlined in the Installation Manual. There is no quick, easy way to set up a new company for processing.

Use Company Control F/M (SMF920) program to create and maintain control parameters for a company. You can also indicate whether alerts can be raised at the company level. CAUTION! Virtually every program in the system checks this control record during live processing. We seldom recommend that you make changes to this program after initial installation. Changes to certain fields, especially those dealing with GL numbers and number lengths, will adversely affect the system.

Use Location F/M (SMF965) to set up location codes that can be used to set default printers for any print or report program. Locations are not required to be set up. If the user has not set a default warehouse, department and/or branch in their active profile and there is a default set in the user's current location, those defaults will automatically be used.

Branch F/M (SMF955) allows FACTS system users to enter and maintain branches to be used throughout the system. The branch may be imbedded (inserted) in the GL account number and transaction from AP, AR, IC, JC, MC, PO, PR and SO may be posted to general ledger by branch. The branch is separate from the department. Branches may be set up as separate profit centers where departments may be set up within branches. Financial reports may be printed by branch; therefore, whenever a branch is entered or used for a warehouse, the branch defaults to the branch assigned to the terminal.

The warehouse branch (where applicable) takes precedence over the terminal branch. In Accounts Payable, a branch is assigned to each document; most AP reports print by branch. In Accounts Receivable a branch is assigned to each customer; each AR invoice document is assigned the branch assigned to the customer. In Sales Orders each invoice document is assigned the branch assigned to the warehouse (except the Statement Print). In all AR reports, the branch assigned to the document takes precedence over the branch assigned to the customer. The Statement Print sorts the documents assigned to the customer and prints the customers by branch. In Payroll a branch is assigned to each employee; most PR reports print by branch. In Inventory Control, sales orders, purchase orders and manufacturing control, a branch is assigned by the branch assigned to the warehouse.

Use Rounding Code F/M (SMF610) to enter rounding code information for contract pricing. This maintenance program allows you to establish rounding rules for contract prices, then indicate on the contract which rounding code (if any) to use. You can set rounding rules by several methods: the percentage change limit for action, and you can indicate the action to be taken when the percentage change limit is reached; the dollar minimum to met for action to be required and you can indicate the action to be taken when the percentage change limit is reached, the program or algorithm to use for the rounding rule, or how to round dollars and/or cents for contract pricing.

The information you enter in Country Code Entry (SME990) supports the Default Tax Code Entry program, which is used to enter the default tax table setup, if desired. This is used for B2C sales where the customer's tax code is not known. You must set up each country in which you plan to charge tax.

The information you enter in State Code Entry (SME991) supports the Default Tax Code Entry program, which is used to enter the default tax table setup, if desired. This is used for B2C sales where the customer's tax code is not known. You must enter each State and first indicate whether or not you should charge tax for orders delivered in that state. Typically, if a distributor has a business presence in a state, he or she must charge tax on orders delivered to that state.

Use the Storefront Initialization program to initially upload FACTS items to the eCatalog database. All requests for data are initiated from the eCatalog application. This program creates the initial add records in the eCatalog log file for when the request is made. When run, this program first removes any existing records of the selected types from the log file. You may need to clear information from the eCatalog database if they are trying to refresh the ERP data to the eCatalog.

Storefront Country Selection (SMU965) program allows the user to specify which countries are uploaded to Storefront. To access this program, choose System Management>File Maintenance>Storefront Initialization Program. You can 'Select' or 'Unselect' All Countries in

the line browser, as well as double-click any Country Code/ Name line in the browser to select (Yes in the Selected column) or un-select a single line.

Executive Inquiry Administrator users can access the Executive Inquiry Setting (SME600) screen to create chart settings by branch and department and enter caution and danger levels used in the Dashboard renderings. Using the Executive Inquiry Settings screen you can also restrict the chart code access in Executive Inquiry by setting security code and modify the update interval for the balance information displayed. Executive Inquiry Administrator privileges are designated in User Code F/M on the Security tab.

Use Note Entry to enter and maintain notes for AR documents, customers, items, IC transfer tickets (header and lines), and vendors.

Credit Card Control F/M (SMF957) enables you to activate, deactivate and manage various credit card handling features in the FACTS system. FACTS supports two types of credit card handling: manual and automatic A manual system collects no credit card processing information and accommodates users who are using imprint devices and settling credit card payments over the phone. The automatic system integrates credit card handling into FACTS with the use of CenPOS, a third-party credit card processing software package. If your company uses or plans to use CenPOS, the Credit Card Control F/M bridges that program to FACTS. Some of the flags in this program can be activated to turn on security features, or they can be deactivated to speed up credit card transactions. When you have completed the information on this screen, click Test beside the Base URL prompt to display the Test CenPOS Connectivity & Card Reader dialog box, where you can submit a 1-cent test transaction. The Credit Card Control F/M program reads the Company Control F/M (SMF920) file and displays only the fields appropriate for the credit card processor selected. If Manual-Do not collect Information is selected in Company Control F/M (SMF920), then the system displays a message indicating that a credit card processor has not been chosen. A Manual tab is available, so that the last credit card receipt number used can be viewed. Refer to *Infor Distribution FACTS Electronic Payments Guide for CenPOS* for credit card handling information.

Users with proper authorization set on the Security tab of User Code F/M (SMF410), can access CC Token Management to manage credit card tokens for use with CenPOS credit card processing. Credit card tokens can be created for the specified customer or by ship-to location for the customer. To access this screen, the CC Token Management prompt in Customer Defaults F/M (ARF840) must be set to Customer or Ship-to and CenPOS must be selected as the credit card processor. Refer to *Infor Distribution FACTS Electronic Payments Guide for CenPOS* for credit card handling information.

Use the Archiving Library Setup (SME631) program to maintain the list of UnForm library codes and their associated network and directory paths for UnForm Archiving. You can set the network/directory path for archiving for the following libraries: Accounts Payable, Banking, Inventory Control, Payroll, Purchase Orders, and Sales Orders.

Use the UnForm Archiving Setup (SME630) program to maintain the list of document codes and their associated UnForm libraries and document types in the FACTS SMUNFO data table. You can select the FACTS print, report or register to setup for archiving, associate the UnForm archive library and document type and indicate whether the archive should contain bar coding information. Note: For UnForm Archiving to function correctly with FACTS

(regardless of where the output is going - i.e. FaxLink, a printer, etc), there are two requirements of the ProvideX device driver being used. The letters "uf" must be in the device driver program name. This is case sensitive as lower case. If, for example, you setup a FaxLink printer which utilizes UnForm to format the output prior to faxing, the device driver program name could be "faxlink-uf". The device driver program name cannot be simply "faxlink", as the letters "uf", which identify it as an UnForm driver, are not present. Additionally, the device driver must declare the '*X' mnemonic the same way that the standard uf7ptr device driver defines it - e.g. 2190 mnemonic (chan)'*X'=pgn+";process". This likewise is case sensitive. If both of these conditions are true, the printer is recognized as an UnForm Archiving device, and FACTS adds the appropriate information to tell UnForm how to archive the document. If either of these conditions is not true, UnForm may still be used, but the document will not be archived.

Use the Resource Type F/M (SMF006) program to enter resource types for the SMRTYP table metadata. The type is used in the SMRLOC file. Any resource that does not specify how it is to be opened will use system help as a default. The target in the system_cmd line will be designated by {filename} and replaced at runtime.

Use the Launch Resource Manager (SMU610) program to start the Resource Manager feature to display supplemental resources tied to customers, documents, or items though out the system.

Use the System Management File Maintenance Utility sub-menu to access the following programs:

Terminal Type F/M (SMF880) allows you to specify the hex code command sequence for arrow and function keys to work correctly when you to TeleFACTS from WordPerfect. The file maintenance is supplied with two records for the Wyse 60 terminal. NOTE: Use this file maintenance only if you are using the WordPerfect interface for issuing letters, and your arrow keys and function keys get scrambled when you go to TeleFACTS. Therefore, you do not have to complete this file maintenance unless this problem arises. At that point, you should contact Technical Support to help you develop the hex codes for your terminal.

Terminal F/M (SMF930) is an administrative level program used to set up defaults for each terminal, especially screen colors and special key functions.

Use Printer F/M (SMF940) to set up printers that need to be accessed through FACTS. In the majority of printer configurations, you will only need to set the first three fields on this program’s main tab. For complete instructions on printer configuration in FACTS and ProvideX, refer to the Installation Manual.

Use Output Options F/M (SMF620) to set up output options for printing reports with multiple outputs. You can print a report to a printer, the viewer and to a file all in one process. After setting up output options and properly configuring reports, you can print reports to Excel, XML (Can print to TCP/IP port), ASCII Delimited (Can print to TCP/IP port) files, other (programmer defined files), or to an HTML file. Reports with multiple output options include: ICR710: Stock Status Report, GLR710: Trial Balance/Detail Ledger, ARR740: Customer Listing, APR750: Vendor Listing, Output options allow you to expand your reporting capabilities beyond defining a printer (in Printer F/M).

Use EMV Terminal FM (SMF460) to set up EMV (chip reader) credit card terminals in FACTS. For each terminal, specify the terminal ID, description and associated IP addresses. The IP address for each terminal is passed to the CenPOS credit card integration. When you process a credit card transaction, the EMV Terminal Search dialog box is displayed so you can select which terminal to use during credit card processing. You can also click **EMV Terminal** on the CenPOS Credit Card Entry screen to display the terminals for selection. Refer to *Infor Distribution FACTS Electronic Payments Guide for CenPOS* for credit card handling information.

Use Runtime Replacement F/M (SMF360) to define non-standard runtime replacement variables needed for FACTS Report Formatter processing. Runtime replacements are data elements that may change depending on when the report is run. For instance, if you run a report and want to save it to disk, you may always want the filename to consist of the program name and the date (for example: ICR71004012004.txt). You can define your output option to contain "Program Name"+"Date" and the filename will be created uniquely each time you run the report. Some common runtime replacements come with standard FACTS (company number, company name, time, user code, etc.). However, a technical person can define new ones if you have a need that is not met by the standard runtime replacements.

Module Code F/M (SMF980) allows FACTS system users to add module codes. The necessary information is included with your system. No entries are required initially. The module codes are used in the survey system.

File F/M (SMF970) FACTS system users to add or modify file names, if files are to be added or changed in the standard system. This information is used with the survey system. All necessary entries are included with your system when purchased.

System administrators can use Data Class Control Entry (SME640) to show all data classes and allow forcing to uppercase and/or use auto-complete for that data. Individual users are able to turn off Auto-Complete in User Preferences F/M (SMF440).

Prerequisite Setup

These prerequisites must be completed before using Data Class Control Entry.

1. For force uppercase to work, the Data Class must be setup in Data Class F/M (DOF950) and the Auto-Complete Prefix must be entered. All standard Data Classes are present, but if you have custom data that you want to force to uppercase, you should create a Data Class for it. It will be used to tie the Prompts to the correct Data Class, i.e. the SMPRMT record’s Auto-Complete Prefix field will be checked against the Data Class Auto-Complete Prefix when determining whether that prompt should force uppercase.
2. All DO entries in File Layout Entry (DOE120) must have been assigned the proper Data Class. Again, all standard data will be assigned, but if you have custom data files defined that include fields for existing or custom Data Classes, you should be sure that the entries have the Class assigned.

   Some fields in DO are comprised of elements, like the key to a file, that contain a Data Class value but the entire field is not that element. In these cases, a special Data Class should be assigned (Complex), and an entry added to SMC999.EXT to define how to find the data class value within the complex field.

Additionally, some fields in DO can be multiple elements based on the value of an alternate field (e.g. it is sometimes a Customer # and sometimes a Vendor number). In these cases, a special Data Class should be assigned (Multiple), and multiple entries added to SMC999.EXT to define when it is one data class vs. another.

Note that the assignment of the special data classes Complex and Multiple are not required. They are there to help a person looking at the DO entry to know something about that field.

3 Each SMPRMT record where the user will be entering one of the defined Data Classes (custom or standard) must have the Auto-Complete Prefix set to the same Auto-Complete Prefix defined in the corresponding Data Class in Prompt Entry (SMC002)-Prompt Characteristics tab.

If you have custom SMPRMT records for any of the defined Data Classes, you must be sure that the Auto-Complete Prefix is properly set or the force uppercase will not be enforced in your SMPRMT records.

The Auto-Complete field is ignored for all SMPRMT records whose Prefix is defined in a Data Class.

4 Some fields serve multiple purposes (e.g. Beginning and Ending values for a report can change based on the order selected). In these cases, the Update AC Prefix option should be set on the SMPRMT record, and the AC Prefix should use a tbl() function to set it correctly.

Note that no individual prefix value should be longer than 20 characters.

Use the Generic Data Changer (SMU940) program to modify one data class at a time. This program cannot be run until all users, except for the user performing the data class update, are locked out of the system via the User Management (SME900). Before will running, additional processing verifies this step has occurred. The user performing the data class update should give themselves a free pass in User Management before locking users out of the company in which the update is taking place. Display FACTS so you see your user code in User Management at all times during this process. Anytime you lock users out you should leave User Management running. If you sign out all users, no one can get back to the User Management to allow users back into FACTS (by clicking Comp In). Further it is recommended you perform these actions at the company level, using the Comp Out function instead of the All Out function and giving the data class update user a free pass at the company level instead a free pass for all companies. When all data class updates are complete, right click the user line in the browser and select Clear all users' free passes to clear the user's free-pass access. Only the data classes that are displayed in the Data Class Search box are eligible for the change. If it is not here you cannot change it. Special cases are explained are displayed on-screen for data classes with special circumstances for change. For example, the same ship-to code can be used for multiple customers. The data class, ship to, is changed for all customers who have the specified ship-to code. If you do not want to change the ship-to code for all customers do not use this program. Additionally you cannot modify a ship to code to a value that is already setup for any customer. Note: This

program is not available if Infor OS (Enable Inbox/Outbox check box) or EWMS (EW-Warehouse Management check box) is checked in Company Control F/M (SMF920).

You will probably only use the majority of these programs during installation and setup. Programs such as System Control F/M and Company Control F/M rarely require changes after live processing begins, and some changes could cause catastrophic system failure. You may also find that you use Company F/M, Printer F/M and Branch F/M somewhat more frequently to add companies, printers and branches to FACTS.

Use System Clean Up F/M (SMF993) to specify how long to retain information, such as closed alerts, F/M (file maintenance) audit records, old cost layers, as well as background processing history and XML background processing log, ION initialization, and error records, in the FACTS system before removal. The date program last ran is displayed at the top of the screen.

Details for each module tab are below:

System Management-Specify the number of months to keep closed alerts, background processing history, F/M audit records XML background processing logs, menu message, completed Infor OS initialization records and system error records.

Inventory Control-Specify the number of months to keep completed cost layers, item ledger cards, past transfers, usage and hits records. Cost Layers must be kept for at least 24 months. Only completed cost layers where the receipt and all disbursements against it were older than the number of months indicated will be removed. The system also displays the last number removed and the date removed through.

Accounts Payable-Specify the number of months to keep vendor ledger card transaction history detail.

Accounts Receivable-Specify the number of months to keep customer ledger card transaction history detail, paid document history, and check history.

General Ledger-Specify the number of months to retain the general ledger budget and ending balances. The system also displays the last run number removed and the date removed through.

Sales Orders-Specify the number of months to retain these types of sales order documents:

- quotes: converted or expired quotes from the system
- contracts: expired contracts entered the Contract Entry program
- CRS and SO Returns documents: completed customer return documents and SO returns documents
- MSDS history: historical information for MSDS sheets sent
- past sales: historical information for past sales
- inactive parent SO companion items or expired SO companion items: Any companion line item set as Persistent in SO Companion Item Entry (SOE150) cannot be removed, regardless of parent companion item active setting or companion line item expired value. Any SO companion line item set as Persistent also prohibits removal of the parent companion item.

Purchase Orders-Specify the number of months to retain:

- expired cost contracts and past purchase orders
- inactive parent PO companion items or expired companion items: Any PO companion line item set as Persistent in PO Companion Item Entry (POE150) cannot be removed, regardless of parent companion item active setting or companion line item expired value. Any companion line item set as Persistent also prohibits removal of the parent PO companion item.
- PO returns and VRS documents

Sales Analysis-Specify the number of months to retain sales information in each of these data files: branch, customer, salesperson, item, item class, customer/item, customer/item class, salesperson/item class, item/warehouse, item/invoice, temporary item, serial item, lot item, and invoice item master. Each SA data file can have a different number of periods to store the information.

Document Delivery-Specify the number of months to retain log records. The system also displays the last run number removed and the date removed through.

Manufacturing - Specify the number of months to retain manufacturing history.

Supplemental resource manager

Use the Supplemental Resource Manager (SMC910) program to manage and view supplemental resources for FACTS.

To access this program click System Management>File Maintenances>Launch Resource Manager. The Supplemental Resource Manager (SMC910) is displayed. The Supplemental Resource Manager may also be launched, when made available, from the Sales Order, Purchase Order, Accounts Payable and Accounts Receivable Entry programs. After you have entered or accessed record, click the Supplemental Resource Manager icon located at the header or line item area of the screen.

Select the entity type and entity to see the resources and associated resources linked to the entity. If the selected resource in line browser is an image type that is supported by PXPlus as one that can be viewed, it will show the image in a preview pane.

You can browse existing resources, add a single resource or multiple resources, delete, edit attributes, open, check in, and check out resources, depending on certain security restrictions.

The program can also operate in sync mode. When in sync mode, whenever a field in another program with the same entity type selected in the Resource Manager has focus and there are resources associated with that entity, the Resource Viewer will show the resources.

Supplemental Resource Manager User Security Settings

The security settings for user permissions for the Supplemental Resource Manager program are based on the following matrix:

	Add Resources	Delete Resources	Open Resource (ERF)	View Resource (ERF)	Edit Attributes	Check In (ERF)	Check Out (ERF)	Clear Check Out	Resource Type Manager	Drag and Drop	Edit security codes for	Edit security codes for
Resource Admin (SMZART)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Entity File Admin (SMRCTL)			Y	Y	Y	Y	Y					
Entity File Read Only (SMRCTL)				Y		Y						
Entity Admin (SMRECT)			Y	Y	Y	Y	Y					
Entity Read Only (SMRECT)				Y		Y						

Chapter 3 Transaction procedures

Messages procedures

Entering quick notes

1 Click System Management>Programs>Quick Note Entry.

2 Specify the **Note**/message.

3 You have these options:

Fax - Sends the information to fax a cover page and calls the Fax Information Entry program.

Create **O**A message - Allows you to create an OA message and calls the General Message Entry program from Office Automation.

Print - Allows you to print the message. Once printed the program returns to the action screen.

F1-Change Note - Use this option to return to the edit screen.

4 Press **F4** to exit the program.

Entering system messages

1 Click **System Management>Messages> Message Entry**.

2 Click **New**.

3 Specify the **Menu** name where the message will display.

4 Specify the **Date** to display the message.

5 Specify the **User Code** that must be in use for this message to be displayed.

6 Specify the **Message** (lines 1-6) (up to 65 characters per line).

7 Click **Save**.

8 Click **Exit**.

Inquiries procedures

Creating and maintaining Executive Management Inquiry settings for charts

1 Specify the **chart code**.
In Account F/M (GLF910), each GL account can be assigned an Executive Inquiry Type. Cash Inventory, Open POs, Open SOs, Accounts Payable, Accounts Receivables are the available chart codes.

2 Specify the **security codes** that the user may have to access this chart, if they are used. The entry must be a valid department. Department codes can be created and maintained in Department F/M (*General Ledger>File Maintenances>Infrequent File Maintenances>Department F/M*).

3 Specify the **Update Interval** (number of minutes between automatic updates) for the information displayed on the chart.

TIP: Different chart types lend themselves to longer or shorter time intervals. For example Open PO and Open SO chart types read directly from the PO and SO file and reflect real-time up-to-date transaction information. Cash, Inventory, Accounts Payable, and Accounts Receivables charts can have typically longer updates settings because their information is only updated when their respective register programs are run and posted.

For example, you can write check and collect payments but until Daily Sales Register program is updated the transaction is not reflected in the Executive Inquiry display. The same is true for Inventory, Sales Orders, Purchase Orders chart types; the transaction information in the General Ledger accounts is not updated until the appropriate register programs are run.

4 In the lower portion of the screen, you can enter branch and department and enter caution and danger levels used in the Dashboard renderings for the branch(es) and department(s) for the chart code.

Note that the Caution and Danger Levels are the values at which the dashboard rendering change color. The **Danger Level** and **Caution Level** field values allow you to precisely specify where the chart colors change from green (favorable) to yellow (caution) to red (danger) for each Dashboard panel you create. The color and chart illustrations on the dashboard panels are pre-set by category to indicate whether

favorable (indicated by green) information for a particular account is desirable to be a high number or low number. For example a favorable Accounts Payable balance would be a lower number.

5 You have these options:

Add or **Insert** a branch and department and enter caution and danger levels for the branch and department for the chart code.

Edit the branch, department, caution and danger levels for the highlighted chart code record.

Cancel line entry

Save the record.

Delete the highlighted line.

6 When you are finished entering chart code information for Executive Inquiry settings, click **Done** to exit the screen.

Displaying account balance information

1 Click **System Management>Inquiries>Summary Management Inquiry**.

2 Specify the **branch** code.

3 Specify the **department** code (if used).

4 The program calculates and displays the current Accounts Payable balance, Accounts Receivable balance, cash in bank, inventory valuation, open Purchase Order balance, and Open Sales Order balance and sales history information for the next period and the last six periods (includes sales, cost and gross margin %). It includes next period transactions from General Ledger to include the most current information available. .

5 (Optional) Press **Enter** to recalculate and redisplay the figures for the same branch and department.

6 You can enter another branch/department and display additional information or press F4 to exit the program.

Viewing program information

1 Click **System Management>Inquiries>Program Inquiry**.

2 In the **Beginning Search Characters** field, specify the search characters to be used in beginning the display (up to 6 characters). Press Enter (CR) to begin with the first program designation on file.

3 The system searches for a match to the entered characters and begins the display with those characters or the next name in alphabetical order. Display continues until the screen is full.

4 You can continue the display in alpha order or specify new search characters.

5 When you have finished reviewing program information, press **F4** to exit the program.

Viewing session information

1 Click **System Management>Inquiries>Terminal Inquiry**.

2 In the browser in the lower portion of the screen, the system displays the FACTS user count, user id, user name, TCPIP address, network id, operating system user id, the FID(0), the T number and Base ID.

3 You can click:

Update to update the user information display in the browser.

Exit to return to the main Security menu.

Creating an amortization schedule

1 Click **System Management>Inquiries> Amortization Schedule**.

2 (Optional) In the **Description** field, specify the loan description (up to 40 characters).

3 In the **Principle** field, specify the amount of the loan.

4 In the **Rate** field, specify the interest rate (.001-99.999).

5 In the **Months** field, specify the life of the loan in months (1-999).

6 In the **Start Month** field, specify the starting month of year of the loan (1-12).

7 The system now displays the calculated monthly payment, total payment, and total interest in the header portion. At the command prompt, the system displays the message: Print Schedule? Specify a T-terminal or one of the available printer numbers displayed at the bottom of the screen to determine where to print the calculated schedule. Press **Enter** to default to T.

8 In the lower portion of the screen, the system displays the following schedule information: one line per month of a year - year, month, total accumulated months, payment, principle, interest, total interest paid, and balance of the loan.

9 Click **End** to exit the program.

Notes procedures

Notes security

This screen is available to the Note Admin User defined on the Security view of User Code F/M to determine which users have Note Entry access by security code, whether users can create/edit categories for note types, and manage category creation by security code. From the Admin menu, you can access the Notes Security screen. You must specify a note type in Note Entry (SME710) before you can access this screen.

1 Use these fields to create information for notes

Notes Entry Security Code

The security codes that determine which users can access Note Entry (SME710). Security codes are assigned to users on the Security view of User Code F/M (SMF410). The system compares the code specified here with those assigned to users and determines whether a user has proper security to create notes.

User Can Create/Edit Categories

Indicate whether users can create or edit categories for the note type specified. You can select from Y-yes, N-no, or S-With Security Code. This setting determines which Category menu options (Creating Notes and Editing Notes) are available in Note Entry (SME710).

Create Category Security Code

The security codes that determine which users can access creating categories via the Category>Creating Categories menu option in Note Entry (SME710). This field is only available if you select S-With Security Code for the User Can Create/Edit Categories field (above).

Security codes are assigned to users on the Security view of User Code F/M (SMF410). The system compares the code specified here with those assigned to users and determines whether a user has proper security to create categories.

2 Save you work.

Entering and maintaining notes for AR documents, transfer tickets, PO documents, SO documents, customers, items, or vendors

1 Type SME710 at the Access Code menu prompt to directly access Note Entry (SME710).

2 In the **Note Type** field, specify the type of note you want to modify or create.

3 For the associated fields, specify the information for the fields that the system displays for the Note Type you specified. You can search for customers, items, vendors and documents.

4 In the **Category** field, specify the category for the note entry, such as General or Urgent. The system displays the category associated with the setting in the Note Type file or the user preference file as the default. If there is only one category on file for the note type, the system uses it as the default.

5 (Optional) Click the **Urgent Only** check box to indicate that you want to display only those notes that are designated as urgent for the Note Type, associated fields, and Category combination entered.

6 In the browser in the lower portion of the screen, the system displays a list of available notes for Note Type, associated fields, and Category combination entered. The Notes browser displays the note date and time, urgent flag, subject and user that created the note.

7 (Optional) If there are no notes available, click **Add** to add a note if you have the authority to create notes and the category has not been deactivated. If notes exist you can:

Click **Edit** to modify the highlighted note.

Click **Delete** to delete the highlighted note.

8 (Optional) If you add or modify a note, the system displays the Note Entry details screen. The Note Type, associated fields, and Category combination entered on the main screen display for reference.

9 Specify the following information for the note:

Subject--Specify or modify the subject for the note.

Urgent--Indicate the note should be classed as urgent. Notes marked urgent automatically display in Sales Order Entry programs for customers, document header records, document line records, and items.

Note--Specify or modify the text for the note.

Contact--Specify the contact person associated with the note.

Reason--Specify the reason for the note.

10 After completing the note fields, you can:

Click **OK** to complete the note entry and return to the main screen.

Click **Cancel** to return to the main screen without entering a note.

For Item Notes only, you can also click **Exports** to access the Export Selections from Items Notes (SME711) screen, which is used to export items notes to transfer document line notes.

11 When you have finished adding, modifying and deleting notes, you can click:

Print to access the Print Options screen that allows you to print a single note (highlighted in the browser). Select File>Print from the menu to access the Print Options screen that allows you to select of a date range of notes to print for the specified notes type and selected the associated fields and print them to the selected printer.

Lines (for Note types TRDH (transfer document header), POEH (Purchase Order Header Note), POPH (Purchase Order Receipt Header Note) SOEH (Sales Order Header Note), SOPH (Past Sales Order Header Note), SOQH (Quote Document Header Note) to access Note Entry for transfer document lines associated with the transfer document header.

Done to exit the Note Entry (SME710) screen.

Creating categories

1. Use the Creating Category screen to add categories for a note type. From the Category menu, you can access programs to edit, delete, and create note categories. Any note type can have an unlimited number of additional information fields associated with it, and any category of notes can have an unlimited number of additional information fields associated with it.
2. Notes are sorted and stored by note type and category. Notes processing comes with a standard category for each note type. For each note type: ARDC (AR document), CUST (customer), ITEM (item), POEH (Purchase Order Header Note), POEL (Purchase Order Line Note), POPH (Purchase Order Receipt Header Note), POPL (Purchase Order Receipt Line Note), SOEH (Sales Order Header Note), SOEL (Sales Order Line Note), SOPH (Past Sales Order Header Note), SOPL (Past Sales Order Line Note), SOEL (Sales Order Line Note), SOQH (Quote Document Header Note), SOQL (Quote Document Line Note), and VEND (vendor), the system provides a GENR-general note category. You can create additional categories using the Creating Category screen. User-created categories have a 3 character ID. System generated categories have only 3 characters.

   Screens from the Category menu are available to the Note Admin User set on the Security view of Company Control F/M and for general users based on setting on the Notes Security Setting for Customer/Item/Vendor Notes screen.
3. You can associate an unlimited number of categories depending on your system's Note Admin User setting on the Security view of Company Control F/M. You can define a specific user as the Notes Admin User or you can set this field to None so that note categories cannot be created for the specified company.

Editing categories

Use the Editing Category screen to edit categories for a note type. From the Category menu, you can access programs to edit, delete, and create note categories.

Your access to this screen is determined by the User Can Create/Edit Categories setting on the Notes Security for Customer/Item/Vendor Notes.

1 Use these fields to edit categories for notes.

1. Category ID

The category ID code that you are editing. The system defaults this value from the category entered on Note Entry (SME710).

2. Inactive

For user-defined categories only, indicates the category should be classed as inactive. Inactive categories cannot be used in creating notes. Inactive note categories do not automatically display notes.

3. Description

The category description. This field is modifiable for user-defined categories only.

4. Security Code Required to View Notes

The security codes that determine which users can view notes. Security codes are assigned to users on the Security view of User Code F/M (SMF410). The system compares the code entered here with those assigned to users and determines whether a user has proper security to view notes.

5. Security Code Required to Create Notes

The security codes that determine which users can create notes. The system compares the code entered here with those assigned to users and determines whether a user has proper security to create notes.

6. Allow Changing Notes

Indicate whether you allow notes in this category to be changed. You can select from: A—Always, U—Only Notes They Created, N—Never. Select A to indicate that you allow notes to be changed in this category with no restrictions, U to indicate that users can only change the notes they create, or N to never allow notes in this category to be modified.

7. Allow Deleting Notes

Indicate whether you allow notes in this category to be deleted. You can select from: A—Always, U—Only Notes They Created, N—Never. Select A to indicate that you allow notes to be deleted in this category with no restrictions, U to indicate that users can only delete the notes they create, or N to never allow notes in this category to be deleted.

8. Change/Delete Override Security Codes

Specify the security code to allow users to change and delete notes even when the category settings (that you specify above) don’t allow it. The security code you specify here overrides the Allow Deleting/Changing Notes settings. Users who have this security code assigned to them can still modify or delete notes in this category.

9. Defaults (button)

Click **Defaults** to access the Category Defaults for Notes screen where you can specify a default subject and default text to display for notes entered in this category.

2 Click **OK** to complete the category or **Cancel** to return to Note Entry (SME710) without creating a category.

System dashboards procedures

Changing the schedule for a background process

1 Click **System Management>System Dashboards Menus>Background Scheduler**.

2 Highlight the background process for which you want to modify the schedule.

3 Click **Edit**.

4 On the Background Process Schedule screen, the current schedule information is displayed on the left side of the screen.

5 On the right side of the screen you can modify the **Frequency Type** for the schedule: A-Manual, H-Hourly, D-Daily, W-Weekly, or M-Monthly.

6 For each Frequency Type, you can modify the number of minutes to wait before retrying when a process fails to start.

7 Based on the frequency type you specified you can enter additional scheduling information:

Frequency Type	Editable Information
Hourly	Minute of the Hour to run the process
Daily	Start Time for the process
Weekly	Day of the Week to start the process; Start Time for the process
Monthly	Day of the Month to start the process; Start Time for the process

8 Click **OK** to save your changes and return to the Background Scheduler Dashboard.

Viewing background process logs

1 Click **System Management>System Dashboards Menu>Background Process Log Viewer**.

2 Specify a specific transaction GUID or click **All**. The filter values are reset and the list box is reloaded.

3 Optionally in the Filters section, narrow your browser display by using the following check boxes and prompts available for specifying the browser results:

Destination: Directory, TCP/IP, Infor OS, Unspecified

Disposition: Incoming, Outgoing

Seq 0001: Indicate whether to display only records with a sequence number of 00001. This action displays only the first record of any possible record set, without showing all subsequent sequence number records for that first record. You can double click a record in the list box to display all subsequent sequence number records and uncheck the check box by default.

Events: Errors, Non-Errors

(The default for Destination, Disposition and Event Code filters is all options selected.)

4 Optionally further narrow your browser display by using the following prompts available for specifying the browser results:

Date/Time - Start Date, Start Time, End Date, End Time.
Date and Time Ranges can be specified to show a range of records. Blank entries indicate no specific starting date or time. The date format is shown in 24-hour format, or HH:MM:SS.sss, where “sss” indicates milliseconds. The time can be specified in either 24-hour time, 12-hour time (am/pm), and with or without the colon separators. For example you can specify “100”, for 1:00:00.000 or 1:00 am.) If you specify ‘14523.5p’, the time value is 13:45:23.000 or 1:45:23.500 pm. The time specified must have at least an hour and minute component; “10p” is invalid. If the end date is the same as the start date, the end time must be later than the start time.

API Name - the API name to use for the filter or click Search or All.

Entity Key - All or a specific entity key.
Note: This is a text search for the entered value in the Entity key column. If the specified text exists anywhere in the entity key of a record, the record is displayed. You cannot manually specify an entity key in this field, because the actual entity key may contain null characters that cannot be reproduced by typing. Null characters are masked with a space on the screen for readability. To filter on an entity key, you must select the entity from the records in the browser, then right-click to use the “Filter on this API Name and Entity Key” option for the line.

LID - All or a specific Logical ID.

1. Optionally click **Apply Filters** to reload the browser using the current filter selections. This is only available when the current filter options are different from the ones that were last applied.
2. In the line browser, this information is displayed for each record: Date/Time, Transaction GUID, Sequence number, Disposition (I-In, O-Out), Error Indicator('*' or blank), Event Code, Event Code Description, , API Name, Entity, CID In, CID Out, LID, Generation, Destination path, and Message Memo.
3. Optionally if you double click on a GUID line in the browser, all sequence numbers for the selected Transaction GUID are displayed.
4. Optionally click **Reset Filters** to reset all filter entries to the original filter values (all entries cleared and all check boxes checked). This is only available when the current filter options are different than the original filters.
5. You can repeat this process and specify additional transaction GUIDs for viewing records or click **Done** to exit the program.

Subscribing to alerts

1. Click System Managements> System Dashboards Menus> System Alerts Dashboard.
2. In the browser, highlight the alert to which you want to subscribe.
3. Click **Manage Subscriptions** to access the Manage Alerts Subscriptions screen.
4. The alert and user code are displayed at the top of the screen.
5. Click **Add** and specify the Available Subscription values. Refer to the Replenishment Alerts Matrix for an explanation of each alert and the Available Subscription values for each.
6. Click **OK** to return to the Manage Alerts Subscriptions screen.
7. (Optional) To add this alert again for another set of subscription values, select Add again and enter the additional subscription values, and click **OK**.
8. When you are finished adding alert subscriptions, click **Done** to return to the System Alerts Dashboard where you can select additional alerts to subscribe to.
9. When you are finished subscribing to alerts click **Done** to exit the program.

Responding to Alerts

1. Click SM>System Dashboards Menu>Alert Control Center.
2. Specify the user code for reviewing alerts.
3. Optionally, using the drop-down list, further limit the browser display of alerts by specifying an alert code.

4 Highlight an alert line in the browser and click:
Refresh to redisplay the alerts.
Alert Details to view detail information about the alert, including the alert name and extended description, alert delivery method and available subscription values and alert status. Click **OK** to return to the ACC.

5 For actionable alerts, click **Respond to Exception** to access the entry program for the alert to manage the alert.

6 When only the PreAuthExp alert is displayed, click **Re-Auth All** to attempt to re-auth all of the pre-auths currently displayed. If any pre-auth lines fail, a message is displayed.

7 Click **Close All** to close all Alert Detail and Respond to Alert windows.

8 Click Done to exit the screen.

Reviewing alert details

1 Click System Managements> System Dashboards Menus> System Alerts Dashboard.

2 In the browser, highlight the alert for which you want to review details.

3 Click **Alert Details** to access the Detail for System Alerts screen.

4 The alert, extended description, delivery method, and available subscription values are displayed.

5 When you have reviewed the alert information, click **OK** to return to the System Alerts Dashboard screen.

6 You can repeat this process to review more alert details or click **Done** to exit the program.

Editing alert subscriptions

1 Click System Managements> System Dashboards Menus> System Alerts Dashboard.

2 In the browser, highlight the alert subscription that you want to edit.

3 Click **Manage Subscriptions** to access the Manage Alerts Subscriptions screen.

4 The alert and user code are displayed at the top of the screen.

5 Click **Edit** and modify the Available Subscription values as needed. Refer to the Replenishment Alerts Matrix for an explanation of each alert and the Available Subscription values for each.

6 Click **OK** to return to the Manage Alerts Subscriptions screen.

7 (Optional) To edit this alert again for another set of subscription values, highlight the next subscription. Click **Edit** again and modify the additional subscription values, and click **OK**.

8 When you are finished editing alert subscriptions, click **Done** to return to the System Alerts Dashboard.

9 When you are finished editing to alerts click **Done** to exit the program.

Deleting alert subscriptions

1 Click System Managements> System Dashboards Menus> System Alerts Dashboard.

2 In the browser, highlight the alert from which you want to unsubscribe.

3 Click **Manage Subscriptions** to access the Manage Alerts Subscriptions screen.

4 The alert and user code are displayed at the top of the screen.

5 In the browser in the lower portion of the screen select the alert subscription you want to remove and click **Delete**.

6 (Optional) You can repeat this process to delete additional alert subscriptions.

7 When you are finished deleting alert subscriptions, click **Done** to return to the System Alerts Dashboard.

8 When you are finished subscribing to alerts click **Done** to exit the program.

Infor OS menu procedures

Managing Infor OS On-Boarding

1 Click System Management>Infor OS Menu>Infor OS On-Boarding.

2 Specify the company. It must be valid in Company Control F/M and the Enable Inbox/Outbox check box must selected.

3 In the browser each line displays this information.

- The processing tier for the Infor OS process
- API name and description
- The date the process was last pushed and the user initials of the push.
- The status of the last push process. The status indicates if it is in-process. Possible values are:

- Waiting – Status flag of SMPUSH = blank. Initial Records and Num Remaining are also blank – indicates that this Ult-P record has not been put into SMPUBQ yet.
- Processing – Status = “P”. Initial records are known, meaning the Ult-P file has been processed and all records were put in SMPUBQ, but there are still records being processed in SMPUBQ. Num Remaining will show # of records still in SMPUBQ and SMXOUH.
- Complete - Status = “C”
- The number of initial records and the records remaining during a process.
- The percentage complete for processing.
- Ultimate Parent (Ult-P), API Name, Description, Last Push Info (Date, Who, Initial Records, # Remaining, Status, % complete) from SMPUSH using alt-key 2

4 Use these options to manage records.

- Push Tier – Processes all records in the browser; refreshes when done; shows progress bar while processing
- Push All – Processes all records in the browser; refreshes when done; shows progress bar while processing
- Push Line – Processes selected line from the browser; shows warning that any dependencies are the responsibility of the user
- Refresh – Refreshes the line browser by updating the data and the SMPUSH record, but does not rebuild the list
- History – Shows history for the currently selected API Name (determined from Ult-P Name)

5 Click **Done** to exit the screen.

Supplemental resources procedures

Adding supplemental resources

1 Access the FACTS Entry program needed.

2 After you have entered or accessed record, select the Supplemental Resource Manager icon located at the header or line item area of the screen.

3 Click **Add** to launch the Resource Selector (SMC915) program or drag and drop a group of files and/or folders on to the line browser to launch the Resource Selector and pre-load the dropped files.

4 When new resources are added to the grid, the Defaults Settings are initially applied.

5 Complete the “Entity” fields for the entity you want to add resources to.

6 Specify the **File\Folder\URL** field by typing in the full path to a file, typing in a URL, typing in a directory, dragging and dropping files or folders onto the field, or browsing for a single file.

7 The browser has the option to filter results based on the “extension filter” field in the header and any extensions defined in the SMRTYP file if desired. If the type is a URL, you must type in the URL of the resource. If the type is a file, you can use the browse button to navigate to a file.

8 When your selections are made, click **Add to Grid** to begin the process of adding the resources to the grid. The resources will be added to the grid according the settings in the “Defaults” section. The default settings for “Internal”, “Encrypted”, “Security Code”, “Extension filters”, “Include Resource Type Extensions” and the setting for the resource type (file or link) will be kept in a user preference file.

9 The resources are added to the grid according the settings in the “Defaults” section. Each entry in the grid can be edited for further control of how each resource will be added. You can specify the following information using the fields in the grid:
Select check box – whether this line should be processed when you click the **Process Grid** button
Type –URL or File in the drop down.
Source Location –the directory name of resource for Files, enter the full URL name for URLs
Filename –the file name of the resource file, blank if URL.
Description – the description of resource
Internal check box –whether this resource will be an ISR (The setting is ESR, if unchecked)
Encrypted check box –whether this resource will be an ERF (must also be an ISR)
Delete check box – indicates whether the original source file will be deleted when the resource is successfully processed.
Entity Type - Entity type for this resource.
Entity – the entity for this resource.
Overwrite check box –whether the selected resource should replace any existing resource of the same name for the same entity, disabled if resource does not exist.
Security Code – the security code required for this resource to be visible in the Resource Manager.
Status – the status of current line in regards to validation and import results: “ready to import” - entries are valid for the line, “missing information – {missing info}” - some required fields are missing, or “failed import – {reason}” – failed to import for reason specified.

10 When all selections are made, click **Process Grid** to add the resources selected for import to FACTS. All lines are validated at this point. Any resources not successfully imported will remain in the grid and the status field in the grid will be updated to show the issue with the line.

11 (Optional) You can also delete the currently selected line in the grid, or clear the entire grid.

Viewing supplemental resources from entry programs

1 Access the FACTS Entry program needed.

2 After you have entered or accessed record, click the Supplemental Resource Manager icon located at the header or line item area of the screen.

3 The Supplemental Resource Manager screen displays with the resources for specified entity.

4 You have these options:

View to display the highlighted supplemental resource.

Scroll Arrows to view additional resources for the entity.

Sync to tie the Resource Manager Viewer display to the records in the calling program.

5 When you are finished viewing resources, click **File>Exit**.

Opening supplemental resources

1 Launch the Supplemental Resource Manager.

2 Specify the **Entity File type** and **Entity Key** as needed.

3 Highlight the resource line the in the browser.

4 Click **Open**.

Resources will be opened by the command line specified in the SMRTYP file, or by the SYSTEM HELP command if no entry exists in the SMRTYP file for a particular resource type. ERFs will be checked out automatically when they are opened, and they cannot be opened if they are checked out by someone other than the user trying to open the resource. The resource will be opened on the client to a temporary file in the user's home directory relative to the client. This home directory is found in the SMZART file. The file will be opened in a "tmp" directory created in the user's home directory. Any existing versions of the file in the tmp directory will be deleted first. The "tmp" directory will be created if needed. The name of the temp file will be the file name from the SMRLOC record. If the resource is an ERF, it must be checked out first, so you will be prompted to check it out.

Editing supplemental resources

1 Access the FACTS Entry program needed.

2 After you have entered or accessed record, click the Supplemental Resource Manager icon located at the header or line item area of the screen.

3 Specify the **Entity File type** and **Entity Key**.

4 Highlight the resource line the in the browser.

5 Click **Edit**.

6 You can modify:
a resource from one type to another (Internally Stored Resources, Internally Stored Resources, and Encrypted Resource Files). (URLs are always ESRs, and cannot be changed).
the file name for ISRs and ERFs, and the path for URLs.
the file path for ISRs and ERFs, which refers to the original location when files are internally stored. You cannot change location of ESRs.

7 **Save** your changes.

8 **Exit** the program.

Checking in/out encrypted resource files

1 Launch the Supplemental Resource Manager.

2 Specify the **Entity File type** and **Entity Key**.

3 Highlight the resource line the in the browser.

4 Click **Check In/Check Out**.
Note: You can edit any resource by opening up the resource using an external program, like a text or image editor. The only type of resource that FACTS can control access to is an Encrypted Resource File. In order to prevent multiple users editing the same Encrypted Resource File, an Encrypted Resource File must be checked out first by someone with proper permissions. This is done by clicking Check Out. When the resource is checked out, the user, date, and time of the checkout is stored in the SMRLOC file for this Encrypted Resource Files. A copy of the resource is placed in a “checkout” directory which is located either on the server or on the client, depending on the setting of the flag in the SMRTYP file for this type of resource. If there is no entry in the SMRTYP file for this resource, the resource is checked out on the client in the user’s home directory. When the file is checked back in (using the “Check In” button), the file is removed from the checkout directory. An Encrypted Resource File that is checked out may not be opened by another user, unless that user has “Resource Admin” rights, which is a flag available in the SMZART file. Users with Resource Admin rights can check out an ERF that is already checked out. An ERF does not have to be checked out to be overwritten.

Using the Generic Data Changer

1 Click **System Management>Security System>User Management**.

2 Specify the company.

3 Highlight your username in the browser.

4 Right-click and select **Update this user's free pass**.

5 In the Giver User a Free Pass dialog box, check the **Free pass for Company (xx)** check box and click **OK**.

6 Click Comp **Out**.

7 Click **Refresh** until the data class update user is the only user line in the browser. (Note the Pass column has 01 in it.)

8 Leave this program visible for this entire process.

9 Click **System Management>Maintenances>Generic Data Changer**.

10 Specify the data class to change at the **From** prompt and the new data class at the **New** prompt.
Note: If displayed, review any special case conditions that must be met for the data class selected.

11 Click **OK**.

12 When the process is complete, click **OK** at the end of update message.

13 Rerun the Generic Data Changer program as needed for additional data class changes.

14 Return to the User Management (SME900) program still displayed from step 8.

15 Click **Comp In**.

16 Right-click the browser line for the user performing the data class update.

17 Click **Clear all users' free passes**.

18 At the confirmation message, click **Yes**.

19 Click **Exit**.

Setting up the FACTS default allowed characters white list

The Default Allowed Characters white list contains the characters typically allowed in controlled fields, in addition to the standard alpha/numeric characters. In System Control F/M (SMF950), the Default Allowed Characters prompt is available to specify the default list of allowed characters for controlled fields, other than space, 0-9, A-Z, and a-z. The list applies to all data classes that are set using the prompts to Limit Characters and Use Defaults in Data Class Control Setup (SME640). (Non-controlled fields and data classes allow all characters.)

You can override this list using the new prompts in Data Class Control Setup.

Use these prompts in Data Class Control Setup (SME640).

Limit Characters If checked, all places in FACTS that allow entry of this data class will verify that only the indicated allowed characters are entered.

Allow All Alpha/Num Defaults to checked. This applies to the space, the digits from 0-9, and all upper-case and lower-case letters. When checked, all of those characters are allowed, and these values cannot be entered in the “Allowed” field because they are already known to be allowed. If Allow All Alpha/Num prompt is unchecked, you can enter any of these characters that are allowed in the “Allowed” field. For example, if you only want the digits 0-9 to be allowed, you can set Allow All Alpha/Num to unchecked (No), and enter ‘0123456789’ in the Allowed field.

Use Defaults The default list of allowed characters from System Control F/M is displayed next to this field. If that default list is adequate, check the box. The allowed characters will be that list in addition to all alpha/numeric characters if that option is selected.

Allowed If you are not using the default list from System Control F/M, this prompt is enabled. Specify the allowed characters for this data class. If Allow All Alpha/Num is checked, you cannot enter the standard alpha/numeric characters in this field because they are all allowed. If you leave this prompt blank, no special characters will be allowed in this data class.

In Data Class Control Setup, when editing a record and Limit Characters is checked, if you change any of the settings related to which characters are allowed, FACTS checks all of the existing data to ensure that no existing data violates the new settings.

If violations are not found in existing data, the changes are saved, and you can continue. If there are violations, they will be displayed. You must use the Generic Data Changer (SMU940) to change the offending data before you can make the requested change.

To resolve special characters issues

1. Copy the contents of the Special Characters Issues list to a document editor of your choice, such as Notepad.
2. Click SM>File Maintenaces> Generic Data Changer (SMU940)
3. Follow the instructions for the Generic Data Changer to change all of the entries in the list to acceptable values.
4. Then return to Data Class Control Setup to make the changes to allowed characters.